ВАЗОРАТИ МАОРИФ ВА ИЛМИ ҶУМҲУРИИ ТОҶИКИСТОН
ДОНИШГОҲИ МИЛЛИИ ТОҶИКИСТОН

КАФЕДРАИ ТЕХНОЛОГИЯИ ИТТИЛООТӢ ВА ИРТИБОТӢ

Арабов М.Қ.

Методҳои криптографии ҳифзи иттилоот

Душанбе - 2017

ББК 32.973+74.202.4+92Я2
А-73
ISBN: 978-99947-848-2-0

Аз тарафи Шӯрои илмию методии Донишгоҳи миллии Тоҷикистон аз 03.07.2017, суратмаҷлиси №09 ба чоп тавсия шудааст.

Арабов М.Қ. Методҳои криптографии ҳифзи итилоот. - Душанбе, 2017. -402 с.

Дар ин дастури таълимӣ методҳои ҳифзи итилоот, хусусан методҳои криптографӣ ба таври комил оварда шудааст. Бинобар ин, хонандагон метавонанд, бе ягон душворӣ ва доштани маълумоти иловагӣ, ба ғайр аз математика ва информатикаи мактабӣ, методҳои ҳифзи итилоотро ба таври пурра омӯзанд.

Дастури таълимӣ барои донишҷӯёни мактабҳои олӣ, миёна, миёнаи махсус, литсею коллеҷҳо ва умуман барои онҳое, ки хоҳиши омӯхтани методҳои ҳифзи итилоотро доранд, пешбинӣ шудааст.

Муқарризон:

Замонов Маликасрор Замонович
номзади илмҳои физикаю математика, мудири кафедраи информатика ва СИ, Донишгоҳи славянии Россия ва Тоҷикистон, факултети идоракунӣ ва технологияҳои иттилоотӣ, дотсент

Бобоёров Шавкат Кенҷабоевич
номзади илмҳои физикаю математика, дотсенти кафедраи алгебра ва назарияи ададҳо, факултети механика ва математика, ДМТ

Муҳаррирон:

Гулов Сангин Нурович
номзади илмҳои филология, мудири кафедраи телевизион ва радиошунавонӣ, факултети журналистика, ДМТ, дотсент

Қурбонов Кенҷа Юлчиевич
номзади илмҳои иқтисодӣ, дотсенти кафедраи ТИИ, факултети механика ва математика

Мундариҷа

Пешгуфтор

Агар ба масири таърих нигарем инсоният аз замонҳои қадим то ҳол роҳҳои бехатар равон кардани итилоотро ба нуқтаҳои лозимӣ хусусан дар вақти ҷангҳо ҷустуҷӯ мекард.

Қайд кардан ба маврид аст, ки масъалаи рамзгузорӣ – танҳо барои итилооте, ки ба ҳимоя ниёз доранд ба вуҷуд меояд. Одатан дар ин ҳолат мегӯянд, ки итилоот сирри махфӣ дошта, давлатӣ ё конфидентсиалӣ (махфӣ, пинҳонӣ) мебошад. Коркарди воситаҳо ва методҳои махфисозии тарзи (далели) равон кардани итилоотро стенография меомӯзад. Коркарди методҳои табдилдиҳии (рамзгузори ё шифрования) итилоот, бо мақсади ҳимоя аз истифодабарандагони ғайриқонуниро - криптография меомӯзад. Криптография илми татбиқӣ буда, дастовардҳои илмҳои дақиқ, алалхусус математикаро истифода мебарад.

Дар замони ҳозира техника ва технология дар ҳолату рушду густариш мебошад, бинобар ин, масъалаи ҳифзи итилоот низ ҳамчун як масъалаи мубрами рӯз ба ҳисоб меравад. Криптография асосан дар вақти ҷангҳои якум ва дуюми ҷаҳонӣ, алалхусус баъди ҷанги дуюми ҷаҳонӣ, хело рушту густариш ёфта, дар бисёр донишгоҳҳо ва донишкадаҳо ҳамчун предмети асосӣ хонда мешавад, ҳатто ихтисоҳои вобаста ба он низ таъсис дода, шудаанд. Масалан,дар ДМТ сар карда, аз соли 2011 ин ҷониб ихтисоси амнияти итилоот (98010101) дар факултети механика ва математика амал мекунад.

Дастури мазкур тарзе навишта шудааст, ки хонандагони он метавонанд бе ягон душворӣ ва доштани маълумоти иловагӣ методҳои ҳифзи итилоотро сар карда аз замонҳои қадим то замони муосир ба таври комил омӯзанд. Барои ин зарур аст, ки ҳар мавзӯъро бодиққат хонда, мисол ва барномаҳои дар он овардашударо таҳлил кунанд. Дар охири ҳар боб барои мустаҳкамкунӣ саволҳо оварда шудааст.

Дастур се фасл ва 11 бобро дарбар гирифта, ҳамчун як воситаи асосӣ барои худомӯзии методҳои рамзгузории итилоот ба ҳисоб меравад. Аз ин китоб хонандагон метавонанд, дар як муддати кӯтоҳ методҳои ҳифзи итилоотро омӯзанд.

Бояд қайд кард, ки ин китоб натанҳо ҳамчун як воситаи худомӯзӣ, балки воситаи методиву таълимӣ низ мебошад. Ҳамаи барномаҳои ин китоб дар компютер иҷро ва тест карда шудаанд.

Дар охири китоб феҳристи васеи адабиёт ҷой дода шудааст, ки барои пурратар омӯхтани метоҳои ҳифзи итилоот кӯмак мекунанд.

Аз баски ин китоб бори аввал чоп мешавад, бинобар ин метавонад аз нуқсону ғалатҳо орӣ набошад. Аз ин рӯ, муаллиф аз ҳамаи хонандагон эҳтиромона хоҳиш менамояд, ки фикру мулоҳизаи ҳэшро оид ба мазмуни китоб ба суроғаи (почтаи) электронии: cool.araby@mail.ru равон созанд.

Умед дорем ки фикру дархости беғаразонаи Шумо барои беҳтар шудани сифати дастур дар оянда кӯмак хоҳанд кард.

Муаллиф ба шахсоне, ки фикру мулоҳизаҳои худро оид ба мазмуни китоб беғаразона мерасонанд, қаблан изҳори миннатдорӣ мекунад.

Муаллиф ба муқарризон Замонов М.З., Бобоёров Ш.К., муҳаррирон Гулов С.Н., Курбонов К.Ю. ва дигар шахсоне, ки дар рафти навиштани ин китоб маслиҳатҳои муфид дода, таваҷҷуҳ зоҳир намуданд, миннатдории зиёди худро баён месозад.

ФАСЛИ 1. АСОСҲОИ МАТЕМАТИКИИ КРИПТОГРАФИЯ

Боби 1. Назарияи тақсимшавӣ. Мафҳум ва теоремаҳои асосӣ

1. Функсияи div ва mod

Оператори mod (remainder operator ё modulus operators) барои ҳисобкунии бақияи тақсими адади *a* ба адади b истифода бурда мешавад. Оператори div бошад, ҳангоми тақсим намудани адади *a* ба адади b, қисми бутуни ҳосили тақсимро муайян мекунад. Намунае аз мисолҳои амалҳои mod ва div чунин мебошад:

№	Қимати a	Қимати b	a mod b	a div b
1	7	4	3	1
2	5	9	5	0
3	25	7	4	3

Дар сурати қимати амалванди якум (тақсимшаванда) аз қимати амалванди дуюм (тақсимкунанда) хурд будан, натиҷаи a mod b ба амалванди якум (тақсимшаванда) баробар шуда, натиҷаи a div b ба 0 баробар мешавад.

Дар забонҳои барномависӣ мисли C++ ва Java барои муайянкунии бақияи ҳосили тақсим аз амали % истифода бурда мешавад. Қайд кардан ба маврид аст, ки дар забонҳои мазкур ҳангоми манфӣ ё мусбат будани тақсимшаванда амали % як хел натиҷа медиҳад, аммо дар назарияи ададҳо натиҷа шакли дигарро дорад. Дар

ҷадвали зерин намунаи ин амал дар барномасозӣ ва назарияи ададҳо оварда шудааст.

№	C++	Назарияи ададҳо
1	25%7=4	25 (mod 7)=4
2	8 %4=0	8(mod 4)=0
3	-6 % 10=-6	-6(mod 10)=4
4	-27%8=-3	-27(mod 8)=5

Дар криптография одатан аз mod-и назарияи ададҳо истифода бурда мешавад. Аз ин рӯ барои муайянкунии амали мазкур метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард.

```
int mod (int a, int b){
if (a<0)
        return (b-(a%b));
else
        return a%b;
}
```

2. Маълумоти умумӣ оиди ададҳои бутун

Дар криптография одатан аз ададҳои бутун истифода бурда мешавад, бинобар ин дар ин боб онҳоро мавриди баҳс қарор медиҳем. Барои ба хонанда фаҳмо шудан, баъзе таъриф ва теоремаҳои асосиро меорем.

Таърифи 1. Адади бутун гуфта, ададеро меноманд, ки дар навишти он аломати вергул дар барномависӣ нуқта (.)) иштирок намекунад.

Мисоли ададҳои бутун: 0, 1, 5, -10, 800, 768, 1989, 3478 ва ҳоказо.

Дар математика маҷмӯи ададҳои бутунро бо ҳарфи $\mathbb{Z}$ ишорат мекунанд.

Таърифи 2. Мегӯянд, ки ададн a ба ададн b бебақия тақсим мешавад, агар $a = b * q + 0$ $(a, b, q \in \mathbb{Z})$ шавад.
Дар ин ҷо ададн $a-$ро каратии ададн b ва ададн $b-$ро тақсимкунандаи ададн a ба меноманд.

Теоремаи 1. (теорема оиди тақсими бақиянок). Ҳар гуна ададн бутуни a ба воситаи ададн b бо тарзи ягона чунин

$$a = bq + r, \qquad 0 \le r < b \qquad (1)$$

ифода кардан мумкин аст.

Дар ин ҷо q-қисми нопурраи ҳосили тақсим ва r бақия аз тақсими ададн a ба ададн b номида мешавад.

Мисоли 1. Бигузор $a = 115$ ва b=27 бошад, он гоҳ 115=27*4+7 мешавад. Дар ин ҷо $q = 4$ ва $r = 7$ аст.

Мисоли 2. Бигузор $a = -31$ ва b=10 бошад, он гоҳ -31=10*(-4)+9 мешавад. Дар ин ҷо $q = -4$ ва $r = 9$ аст.

3. Калонтарин тақсимкунандаи умумӣ(КТУ)

Ҳар гуна ададе ки дар як вакт ададҳои a ва b-ро тақсим мекунад, тақсимкунандаи умумии ин ададҳо номида мешавад. Аз байни тақсимкунандаҳои умумии ададҳо калонтаринашро калонтарин тақсимкунандаи умумии ин ададҳо меноманд ва бо рамзи (a, b) ишора мекунанд.

Теорема 1. Агар $a = bq + c$ бошад, он гоҳ КТУ(a, b)=КТУ$(b,$ с) мешавад.

Барои ёфтани КТУ(a, b), дар ҳолати $a > b$ будан, аз алгоритми Евклид[1] истифода бурда мешавад, ки шакли зеринро дорад:

$$a = bq_0+r_1,\ 0< r_1<b$$
$$b =r_1q_1+r_2,\ 0<r_2<r_1$$
$$r_1=r_2q_2+r_3,\ 0<r_3<r_2$$
$$\ldots\ldots\ldots\ldots\ \ldots\ldots$$
$$r_{n-2}=r_{n-1}q_{n-1}+r_n,\ 0<r_n<r_{n-1}$$
$$r_{n-1}=r_nq_n.$$

Тавре ки аён, дар ин ҷо мо баробарии зеринро ҳосил мекунем:

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$$

Ҳамин тариқ, охирон бақияи ғайрисифрӣ, яъне r_n КТУ-и ададҳои a ва b ба ҳисоб меравад.

Мисоли 1. Бо ёрии алгоритми Евклид КТУ(2004,1941)-ро ёбед.

Ҳал:

2004=1941*1+63

1941=63*30+51

63=51*1+12

51=12*4+3

12=3*4

[1] Евклид **ё** Эвклид (юн. Εὐκλείδης) математики юнони қадим, тақрибан 300 п.м зиндагӣ карда, муаллифи нахустин асар оиди математик ба ҳисоб меравад.

Инак, КТУ(2004, 1941)=3 мешавад.

Барои ёфтани КТУ (a, b) метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст истифода кард:

```
long KTU(long a, long b){
 while (b!=0) {
          long t=a%b;
          a=b;
          b=t;
 }
 return a;
}
```

Барои муайянкунии КТУ ба ғайр аз алгоритми Евклид метавон аз алгоритми зерин низ истифода кард, ки аз нуқтаи назари компютер вақти камтарро мегирад.

$$\text{КТУ}(a,b)=\begin{cases}\text{КТУ}\left(\frac{a-b}{2},b\right), \text{агар } a,b-\text{тоқ бошанд;}\\ \text{КТУ}\left(\frac{a}{2},b\right), \text{агар } a-\text{ҷуфт ва } b-\text{тоқ бошад;}\\ \text{КТУ}\left(a,\frac{b}{2}\right), \text{агар } a-\text{тоқ ва } b-\text{ҷуфт бошад;}\end{cases}$$

Барои ёфтани КТУ (a, b) бо истифода аз ин метод метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст истифода кард:

```
long KTU(long a, long b){
        long g=1;
        //Аз КТУ муайян кардани дараҷаҳои 2
 while ((a%2==0) && (b%2==0)) {
          a=a/2;
          b=b/2;
```

```
            g=2*g;
 }
//Аққалан яке аз ададҳои a ва b тоқ будан
while (a!=0){
            while(a%2==0){ a=a/2;
      }
            while(b%2==0){ b=b/2;
            }
            //Дар ҳолати a ва b тоқ будан
            if (a>=b)
                        a=(a-b)/2;
            else
                        b=(b-a)/2;
 }
return g*b;
}
```

Таърифи 1. Ҳар гуна ададӣ натуралии аз 1 калон, ки танҳо ду тақсимкунда (яъне 1 ва худаш) дорад, ададӣ сода номида мешавад.

Таърифи 2. Ададҳои бутуни *a* ва b байнан сода номида мешаванд, агар КТУ(*a*, b)=1 бошад.

Таърифи 3. Ададҳои ғайрисодаро таркибӣ меноманд.

Мисоли 2. Дар байни 100 ададӣ натуралӣ (аз 1 то 100), ададӣ сода танҳо ададҳои зерин мебошанд: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Тавре ки аз математикаи элементарӣ медонем, барои ёфтани ададҳои сода метавон аз ғалбери Эратосфен[1] истифода кард. Моҳияти ин алгоритм чунин аст:

Дар аввал ададҳои натуралии аз 1 то N -ро пайдарпай менависем

$$1,2,\dots,N$$

Нахустин ададӣ аз 1 калони ин қатор ададӣ 2 аст. Ин адад танҳо ба 1 ва худаш тақсим мешавад, пас вай сода аст. Аз ин қатор ба ҷуз аз худи 2 ҳамаи ададҳои ба 2 каратиро (ҳамчун таркибӣ) хат мезанем. Баъди 2 нахустин ададӣ хатназада ададӣ 3 аст вай бо 2 тақсим намешавад (дар акси ҳол онро бояд хат мезадем). Бинобар ин ададӣ 3 танҳо ба 1 ва ба худаш тақсим мешавад, аз ин сабаб вай ҳам сода аст. Аз қатори (1) ба ғайр аз худи 3 ҳамаи ададҳои ба 3 каратиро хат мезанем. Аввалин ададӣ пас аз 3, ки хат зада нашудааст, ададӣ 5 аст. Вай ба 2 ва 3 тақсим намешавад (дар акси ҳол бояд онро хат мезадем). Бинобар он ададӣ 5 танҳо ба 1 ва ба худаш тақсим мешавад, аз ин сабаб вай ҳам ададӣ сода аст. Ҳамин тариқ ин равандро барои ададҳои дигар, ки аз $\sqrt{N}$ хурд мебошанд, иҷро мекунем. Дар натиҷа ҳамаи ададҳои хатназадаи аз N хурд, ададҳои сода мешаванд.

Барои муайянкунии ададҳои содаи аз 1 то N метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст истифода кард:

[1] Эратосфен математики юнонӣ асри III пеш аз мелод

```
void Soda(int n)
{
 int k;
 for (int i=1; i<=n; i++){
          k=0;
 for (int j=2; j<=(int) sqrt(i); j++){
          if (i % j==0)
            {
                  k++;
          break;
          }
 }
 if (k==0)
 cout<<i<<"\t";
 }
}
```

Теоремаи 2. Ҳаргуна ададӣ бутуни аз як калонро ба ҳосили зарби ададҳои сода бо тарзи ягона ҷудо кардан мумкин аст.

Хосияти 1. Ҳангоми ба зарбкунанандаҳои сода ҷудо намудани ададӣ a метавонанд, баъзе зарбкунандаҳо якчанд маротиба такрор шаванд. Бо ҳарфҳои $p_1, p_2, \dots, p_n$ ҳамаи зарбкунандаҳои содаи гуногуни ададӣ a ва бо $\alpha_1, \alpha_2, \dots, \alpha_n$ мувофиқан каратнокии онҳоро ишорат карда, ба сурати зерин формулаи ба зарбкунандаҳои сода ҷудо намудани ададӣ a-ро ҳосил мекунем:

$$a = {p_1}^{\alpha_1} \dots {p_n}^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$$

Мисоли 3. Ҷудокунии каноникии ададӣ 6791400 чунин шаклро дорад: $6791400 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11$

Барои ададӣ додашударо ба зарбкунандаҳои сода ҷудо кардан метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард.

```
void judokuni(int a, int b)
{
        if (a == 1)
                return;
        for (;; b++)
        if (a%b == 0)
        {
                cout << b << endl;
                rec(a / b, b);
                return;
        }
}
int main()
{
        int a;
        cin >> a;
        judokuni(a,2);
        return 0;
}
```

Мисоли 4. Муайян кунед, ки ададҳои 315 ва 78 байнан сода мебошанд?

Ҳал. Барои ёфтани КТУ(315, 78) аз алгоритми Евклид истифода бурда мешавад.

315=4*78+3

78=26*3+0

Тавре ки дида мешавад КТУ$(315, 78) = 3 \neq 1$. Бинобар ин, ададҳои 315 ва 78 байнан сода намебошанд.

Теорема 4. (тасвири хатии КТУ(a, b)). Агар ададиd КТУ(a, b) бошад, он гоҳ чунин ададҳои бутуни x ва y мавҷуданд, ки барои онҳо баробарии зерин ичро мешавад:

$$ax + by = d. \qquad (2)$$

Натиҷа. Агар ададҳои бутуни a ва b байнан сода бошанд, он гоҳ (2) шакли зеринро мегирад:

$$ax + by = 1 \qquad (3)$$

Дар формулаҳои (2) ва (3) ададҳои x ва y -ро коэффитсиентҳои Безу(Bezout Etienne 1739-1783) [1] меноманд.

Мисоли 5. Барои ададҳои 81 ва 26 коэффитсиентҳои Безуро ёбед.

Ҳал. Ибтидо КТУ(81, 26)-ро бо истифода аз алгоритми Евклид меёбем.

81=26·3+3

26=3·8+2

3=2·1+1

2=1·2+0

Аз ин ҷо КТУ(81,26)=1 мешавад.

[1] https://en.wikipedia.org/wiki/Bézout%27s_identity

Бо назардошти иҷроиши алгоритм, баробариҳои занҷирии зеринро ҳосил мекунем:

1=3-1·2=

3-1· (26-8·3)=9·3-1·26=

9· (81-3·26)-1·26=

9·81-28·26

Аз ин ҷо коэффитсиентҳои Безу $x = 9$ ва $y = -28$ мешавад.

Барои ёфтани коэффитсиентҳои Безу метавон аз барномаи зерин, ки дар забони C# навишта шудааст, истифода кард.

```
using System;
namespace BEZUKOEF
{
   class Program
   {
      public static Tuple<int, int> BEZU(int a, int b)
      {
         int x = 0;
         int lastx = 1;
         int y = 1;
         int lasty = 0;
         while (b != 0)
         {
            int quotient = a / b;
            b = a % (a = b);
            x = lastx - quotient * (lastx = x);
            y = lasty - quotient * (lasty = y);
```

```
            }
            return Tuple.Create(lastx, lasty);
        }
        static void Main(string[] args)
        {
            Tuple<int, int> z;
            int a, b;
            a = Convert.ToInt32(Console.ReadLine());
            b = Convert.ToInt32(Console.ReadLine());
            z = BEZU(81, 26);
            Console.WriteLine("x="+z.Item1+"  y="+z.Item2);
            Console.ReadKey();
        }
    }
}
```

4. Касрҳои бефосила ва алоқаи онҳо бо алгоритми Евклид

Бигузор α адади дилхоҳи ҳақиқӣ бошад. Бо ҳарфи q_1 адади бутуни калонтарини аз α калон набударо ишора мекунем. Дар вақти бутун набудани α маълум аст, ки $\alpha = q_1 + \frac{1}{\alpha_2};\ \alpha_2 > 1$ мешавад.

Айнан ҳамин тавр, дар ҳолати бутун набудани ададҳои $\alpha_2, \dots, \alpha_{s-1}$ ҳосил мекунем:

$$\alpha_2 = q_2 + \frac{1}{\alpha_3};\ \alpha_3 > 1,$$

$$\alpha_3 = q_3 + \frac{1}{\alpha_4};\ \alpha_4 > 1,$$
$$\dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots$$
$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s};\ \alpha_s > 1$$

Дар натиҷа ҷудокунии α – ро ба касрҳои бефосила (ё касрҳои занҷирӣ) пайдо мекунем:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots \\ \ddots \\ + \cfrac{1}{q_{s-1} + \cfrac{1}{q_s}}}} \qquad (1)$$

Барои ҳисоб намудани касрҳои бефосила метавон аз барномаи зерин истифода кард:

```
#include <iostream>
#include <string>
#include <sstream>
using namespace std;

 double solve(int n)
{
   if (n <= 0)
     return 0.0;
  double result = n;
  for (int i = n - 1; i >= 1; --i)
   result = i + 1.0 / result;
  return result;
```

```
}

string int_to_str(int value)
{
  ostringstream ostr;
  ostr << value;
  return ostr.str();
}

string build_formula(int n)
{
  if (n == 1)
      return "1";
  string formula = int_to_str(n);
   for (int i = n - 1; i > 1; --i)
      formula = "(" + int_to_str(i) + " + 1 / " + formula + ")";

  return "1 + 1 / " + formula;
}

int main(int argc, char** argv) {
  int m, n;
  cout<<"m="; cin>>m;
  cout<<"n="; cin>>n;
  cout << build_formula(m) << " = " << solve(n) <<endl;
 return 0;
}
```

Агар α ирратсионалӣ бошад, он гоҳ ҳар гуна α_1 ҳам ирратсионалӣ мешавад (дар ҳолати ратсионалӣ будани α_s дар асоси (1) α ҳам ратсионалӣ мешавад) ва протсесси нишондодашударо беохир давом додан мумкин аст .

Агар a ратсионалӣ бошад, онро ҳамчун касри ратсионалии ихтисоршавандаи $\alpha = \frac{a}{b}$, ки махраҷаш адади мусбат аст, ифода намудан мумкин аст, он гоҳ протсесси нишондодашуда ба охир мерасад ва онро бо ёрии алгоритми Евклид иҷро кардан мумкин аст. Дар ҳақиқат ҳосил мекунем:

$$a = bq_1 + r_2;\ \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = rq_2 + r_3;\ \frac{b}{r_3} = q_2 + \frac{1}{\frac{r_2}{r_3}},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n\ ;\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n\ ;\ \frac{r_{n-1}}{r_n} = q_n .$$

Аз ин ҷо ҳосил мекунем.

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} \qquad (2)$$

$$\ddots$$

$$+ \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}$$

Ададҳои q_1 , q_2 .... дар ҷудокунии α дар касри бефосила иштирок мекунанд, қисмҳои нопурраи ҳосили тақсим номида мешаванд. Касрҳои $\delta_1 = q_1$, $\delta_2 = q_1 + \frac{1}{q_2}$, $\delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}$ .....*ро* касрҳои мувофиқ меноманд.

Сурат ва махраҷи касрҳои мувофиқро бо ёрии ҷадвали

q		q_1	q_2	....	q_k	....	q_n
P	1	p_1	p_2	....	p_k	....	p_n
Q	0	1	Q_2	....	Q_k	....	Q_n

ва формулаҳои $\begin{cases} P_k = q_k P_{k-1} + P_{k-2} \\ Q_k = q_k Q_{k-1} + Q_{k-2} \end{cases}$ ҳисоб карданмумкин аст.

Намунаи мисолҳо:

$$\frac{25}{11} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}} = [2; 3; 1; 2]$$

$$-\frac{43}{15} = -2\frac{13}{15} = -3 + \frac{1}{7 + \frac{1}{2}} = [-3; 7; 2].$$

Барои ҳосил кардани натиҷаи ин навъ мисолҳо метавон аз зербарномаи зерин истифода кард, ки дар забони C++ навишта шудааст:

```
void pown(long int a, long int b){
  vector<int>q;
```

```
  int n=0;
  while(a%b!=0){
            int h=mod(a,b);
            q.push_back(a/b);
            a=b;
            b=h;
           }
  q.push_back(a/b);
  cout<<"[";
 n=q.size();
 for (int i=0; i<n; i++)
          if (i<n-1)
                    cout<<q[i]<<",";
          else
                    cout<<q[i];
 cout<<"]"<<endl;
}
```

Дар ин зербарнома аз зербарномаи mod истифода бурда шудааст.

5. Хурдтарин каратии умумӣ (ХКУ)

Ҳар гуна ададӣ бутуни ба ҳамаи ададҳои бутуни додашуда каратиро, каратии умумии ин ададҳо меноманд. Хурдтарин каратии мусбатро хурдтарин каратии умумии онҳо меноманд.

Дар ҳолати хусусӣ, агар ХКУ-и ададҳои a ва b ададӣ c бошад, онро чунин ишора мекунанд: ХКУ$(a, b) = c$.

Барои ёфтани ХКУ метавон аз формулаи зерин истифода кард:

$$\text{ХКУ}(a,b)=\frac{ab}{\text{КТУ}(a,b)}$$

КТУ(ХКУ) –и якчандто ададҳои $a_1,a_2,\dots,a_n$ – ро чунин муайян мекунанд:

Ибтидо барои ду адад КТУ(ХКУ)-ро ёфта, сипас ин усулро барои адади ёфташуда ва адади сеюми он давом медиҳанд ва ғайра.

6. Хосиятҳои асосии КТУ ва ХКУ

КТУ ва ХКУ дорои хосиятҳои зерин мебошанд:

Хосияти 1. КТУ(a,b,c)=КТУ(КТУ(a,b);c).

Хосияти 2. ХКУ(a,b,c)=ХКУ(ХКУ(a,b);c).

Хосияти 3. КТУ(ac, bc)=c·КТУ(a,b).

Хосияти 4. ХКУ(ac, bc)=c·ХКУ(a,b).

Хосияти 5. КТУ(n, n+1,n+2)=1.

Хосияти 6. Ададҳои $\frac{a}{\text{КТУ}(a,b)}$ ва $\frac{b}{\text{КТУ}(a,b)}$ байнан сода мебошанд.

Хосияти 7. Агар КТУ(n, k)=1 бошад, он гоҳ КТУ(n, n+k)=1 мешавад.

Мисоли 1: КТУ(3n,6n+3)=3·КТУ(n,2n+1)=3·КТУ(n, n+(n+1)) =3· КТУ(n, n+1) =3.

Мисоли 2: $\text{КТУ}(30n+25, 20n+15) = 5 \cdot \text{КТУ}(6n+5, 4n+3) = 5 \cdot \text{КТУ}(4n+3+(2n+2), 4n+3) = 5 \cdot \text{КТУ}(2n+2, 4n+3) = 5 \cdot \text{КТУ}(2n+2, 2n+2+(2n+1)) = 5 \cdot \text{КТУ}(2n+2, 2n+1) = 5.$

Хосияти 8. Агар КТУ $(a, b, \dots, l)$=1 бошад, он гоҳ $a, b, \dots, l$ байнан сода номида мешаванд. Агар ҳар яке аз ададҳои $a, b, \dots, l$ бо ҳар яки дигараш байнан сода бошанд, он гоҳ $a, b, \dots, l$ ҷуфт-ҷуфт сода мешаванд. Барои ду ададӣ додашуда мафҳуми ҷуфт-ҷуфт сода ва мафҳуми байнан сода ҳаммаъноянд.

Хосияти 9. Агар δ тақсимкунандаи умумии дилхоҳи a ва b бошад, он гоҳ $\text{КТУ}\left(\frac{a}{b}, \frac{b}{\delta}\right) = \frac{\text{КТУ}(a,b)}{\delta}$ аст. Дар ҳолати хусусӣ хосияти 6 ҷой дорад.

Хосияти 10. Агар ҳар яке аз ададҳои $a_1, a_2, \dots, a_m$ бо ҳар як ададҳои $b_1, b_2, \dots, b_m$ байнан сода бошанд, он гоҳ ҳосили зарби онҳо низ байнан сода мешавад.

Хосияти 11. Хурдтарин тақсимкунандаи аз як фарқкунандаи ададӣ таркибии a аз ададӣ $\sqrt{a}$ калон намебошад.

Хосияти 12. КТУ-и якчанд адад аз ҳосили зарби дараҷаҳои намуди p^{α} иборат аст, ки дар ин ҷо p— тақсимкунандаи содаи умумии ҳамаи ин ададҳо, α —нишондиҳандаи хурдтарине, ки p бо вай ба ҷудокунии каноникии он ададҳо дохил мешавад.

Мисоли 1. КТУ(6791400, 178500) ёфта шавад.

Ҳал. Аввал ададҳои 6791400, 178500-ро бо зарбкунандаҳои сода ҷудо мекунем, ки дар натиҷа шакли зеринро мегиранд:

$6791400 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11;\ 178500 = 2^2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 11.$

Аз ин ҷо КТУ(6791400, 178500)= $2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 =$

Хосияти 13. ХКУ-и якчанд адад аз ҳосили зарби дараҷаҳои намуди p^α иборат аст, ки дар ин ҷо p— тақсимкунандаи содаи умумии ҳамаи ин ададҳо, $\alpha -$ нишондиҳандаи калонтарине, ки p бо вай ба ҷудокунии каноникии он ададҳо дохил мешавад.

Мисоли 2. ХКУ(6791400, 178500) ёфта шавад.

Ҳал. Аввал ададҳои 6791400, 178500-ро бо зарбкунандаҳои сода ҷудо мекунем, ки дар натиҷа шакли зеринро мегиранд:

$6791400 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11;\ 178500 = 2^2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 11.$

Аз ин ҷо КТУ(6791400, 178500)= $2^3 \cdot 3^2 \cdot 5^3 \cdot 7^3 \cdot 11 =$ 33957 000 мешавад

Хосияти 14. Маҷмӯи каратиҳои умумии якчанд ададҳо бо маҷмӯи каратиҳои ХКУ-и он ададҳо баробар аст.

Хосияти 15. ХКУ-и якчанд ададҳои ҷуфт-ҷуфт байнан сода, ба ҳосили зарби он ададҳо баробар аст.

Саволҳо барои мустаҳкамкунӣ

1) Чӣ гуна ададҳоро адади бутун меноманд?
2) Чӣ гуна ададҳоро сода меноманд?
3) Барои муайянкунии ададҳои сода аз кадом алгоритм истифода бурда мешавад?

4) Алгоритми Евклид барои чӣ истифода бурда мешавад?
5) Чӣ тавр ХКУ(a,b) ва КТУ (a,b) ҳисоб карда мешаванд?
6) Чӣ тавр зарбкунандаҳои Безу ёфта мешаванд?
7) Чӣ гуна ададҳоро байнан сода меноманд?
8) Касрҳои бефосила бо алгоритми Евклид чи алоқаманди доранд?

Боби 2. Функсияҳои асосии назарияи ададҳо

1. Функсияҳои $[x]$ ва $\{x\}$

Ибтидо ду функсияҳои муайяни зеринро, ки барои ҳамаи қиматҳои ҳақиқӣ маълум мебошанд, дида мебароем.

1. Қисми бутуни x бо рамзи $[x]$ ишора карда мешавад ва ба калонтарин адади бутуни аз x калон набуда баробар мебошад. Дар забони C++ барои иҷрои ин амал аз функсияи floor(x) истифода бурда мешавад.
2. Қисми касрӣ аз x бо рамзи $\{x\}$ ишора карда мешавад ва ба фарқи байни x ва қисми бутуни вай, яъне $x-[x]$ баробар мебошад. Дар забони C++ барои иҷрои ин амал метавон аз ифодаи x-floor(x) истифода бурда мешавад.

Мисолҳо :

$[\pi]=3,\ [2{,}3]=2,\ [-3{,}75]=-4,$

$\{7\}=0, \{2{,}3\}=0{,}3,\ \{-5{,}75\}=0{,}25$.

3. Нишондиҳандае, ки бо он адади содаи $p\ (p\le n)$ ба ҳосили зарби n! дохил мешавад, баробар аст ба

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots \qquad (1)$$

Мисол. Адади 10!-ро ба зарбшавандаҳои сода ҷудо кунед.

Ҳал: Барои ҳалли ин мисол аз формулаи (1) истифода мебарем.

$$\left[\frac{10}{2}\right] + \left[\frac{10}{2^2}\right] + \left[\frac{10}{2^3}\right] = 5 + 2 + 1 = 8$$
$$\left[\frac{10}{3}\right] + \left[\frac{10}{3^2}\right] = 3 + 1 = 4$$
$$\left[\frac{10}{5}\right] = 2, \left[\frac{10}{7}\right] = 1.$$

Аз ин ҷо ҳосил мекунем: $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

2. Функсияҳои мултипликативӣ

Функсияи $\theta(a)$ мултипликативӣ номида мешавад, агар вай ду шарти зеринро қонеъ гардонад:

1. Ин функсия барои ҳамаи ададҳои бутуни мусбати a муайян буда, аққалан барои яке аз чунин a нобаробарӣ сифр аст.
2. Барои ҳаргуна ададҳои мусбати байнан соддаи a_1 ва a_2 баробарии зерин ичро гардад
$$\theta(a_1 a_2) = \theta(a_1)\theta(a_2)$$

Мисол. Бе душворӣ дидан мумкин аст, ки функсияи a^s, ки дар ин ҷо s −адади дилхоҳи ҳақиқӣ ё комплексӣ мебошад, мултипликативӣ аст.

Барои ҳар гуна функсияи мултипликативии $\theta(a), Q(1) = 1$ аст .

Дар ҳақиқат, бигузор $\theta(a_0) \neq 0$, бошад. он гоҳ $\theta(a_0) = \theta(a_0 \cdot 1) = = \theta(a_0)\theta(1)$, $1 = \theta(1)$ ҳосил мешавад.

Хосияти дуюми функсияи мултипликативии $Q(a)$ дар ҳолати k >2 будан барои k -то ададҳои ҷуфт-ҷуфт байниҳам содаи $a_1, a_2, \ldots, a_k$ низ ичро мешаванд. Дар ҳақиқат, ҳосил мекунем:

$\theta(a_1, a_2, \dots, a_k) =$
$\theta(a_1)\theta(a_2, \dots, a_k) = \theta(a_1)\theta(a_2)\theta(a_3, a_4, \dots, a_k) =$
$= \theta(a_1)\theta(a_2)\theta(a_3) \dots \theta(a_k).$

Дар ҳолати хусусӣ:

$$\theta(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}) = \theta\left(p_1^{\alpha_1}\right)\theta(p_2^{\alpha_2})\theta(p_3^{\alpha_3}) \cdots \theta\left(p_k^{\alpha_k}\right).$$

3. Миқдори тақсимкунандаҳо ва суммаи тақсимкунандаҳои адад

Функсияҳои $\tau(a)$ ва $S(a)$ барои ададҳои натуралии a муайян буда, мувофиқан миқдор ва суммаи тақсимкунандаҳои адади натуралии $a-$ро муайян мекунанд. Дар ҳолати $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ будан
$\tau(a) = (a_1 + 1) \cdots (a_k + 1)$ ва $S(a) =$
$\frac{p_1^{a_1+1}-1}{p_1-1} \cdots \frac{p_k^{a_k+1}-1}{p_k-1}$ мешавад. .

$S(\alpha)$ функсияи мултиплитикавӣ буда, дар ҳолати $\alpha > 0$ будан чунин ҳисоб карда мешавад:

$$S(p^{\alpha}) = \frac{p^{\alpha+1} - 1}{p - 1}$$

Мисол. Сумма ва миқдори тақсимкунандаҳои адади 45-ро ёбед.

Ҳал: Азбаски $45 = 3^2 \cdot 5$ аст, пас формулаҳои $S(a)$ ва $\tau(a)$ –ро истифода бурда, ҳосил мекунем:

$S(a) = S(45) = S(3^2 \cdot 5) = \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{8}{2} \cdot \frac{24}{4} = 2 \cdot 6 = 12.$

$\tau(a) = \tau(45) = \tau(3^2 \cdot 5) = (2 + 1)(1 + 1) = 3 \cdot 2 = 6.$

Барои муайян кардани сумма ва миқдори тақсимкунандаҳои ададӣ додашуда метавон аз зербарномаҳои зерин истифода кард.

```
#include <iostream>
using namespace std;
int sum(int n){
 int res=0;
 for (int i=1; i*i<=n; i++)
   if (!(n%i))
    {
     res+=i;
     if (i*i!=n)
       res+=n/i;
}
 return res;
}
int col(int n){
 int k=1;
 for (int i=1; i<=n/2;i++)
  if (n%i==0)
    k++;
  return k;
}
int main(int argc, char** argv) {
  int n,S, k;
  cout<<"n="; cin>>n;
  S=sum(n);     k=col(n);
```

```
 cout<<"S="<<S<<"  k="<<k;
 return 0;
}
```

4. Функсияи Эйлер

Функсияи Эйлер [1] $\varphi(a)$ – барои ҳамаи ададҳои мусбати a муайян карда мешавад ва миқдори ададҳои бо a байни ҳам содаи қатори ададҳои қатори $0,1,\cdots,a-1$ –ро ифода мекунад.

Бигузор $a=p_1^{a_1}\cdots p_k^{a_k}$ ҷудокунии каноникии ададии a бошад, он гоҳ

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) \qquad (*)$$

ё

$$\varphi(a)=\left(p_1^{a_1}-p_1^{a_1-1}\right)\left(p_1^{a_2}-p_1^{a_2-1}\right)\cdots\left(p_k^{a_k}-p_k^{a_k-1}\right),$$

мешавад. Дар ҳолати хусусӣ

$\varphi(a)=p^a-p^{a_1-1}$, $\varphi(p)=p-1$ баробар аст.

$\varphi(a)-$ функсияи мултиплитикативӣ буда, барои $a>0, \varphi(p^a)=p^a-p^{a-1}$ мебошад.

[1] Леонард Эйлер (нем. Leonhard Euler)-олими бузурги (швейтсариягӣ,, олмонӣ, рус) соҳаи математика 15-уми апрели соли 1707 дар шаҳри Базел (Швейтсария) ба дунё омадааст. 7-ум ё 18-уми сентябри соли 1783 дар шаҳри Санкт-Петербург (Империяи Рус) аз олам гузаштааст. Эйлер — муаллифи зиёда аз 850 кори илмӣ мебошад.

Мисол. Функсияи Эйлер барои ададӣ 45 ёфта шавад .

Ҳал. Ибтидо ададӣ 45-ро ба зарбкунандаҳои сода ҷудо мекунем, ки шакли $45= 3^2 \cdot 5$-ро мегирад. Пас аз ин формулаи (*)-ро истифода бурда ҳосил мекунем:

$$\varphi(45) = \varphi(3^2 \cdot 5) = 120\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot\cdot \frac{4}{5} = 4.$$

Барои ҳисобкунии қимати функсияи Эйлер метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст истифода кард.

```
long Eiler(long int a){
        int k=0;
        for (int i=1; i<a; i++){
                if (KTU(a,i)==1)
                        k++;
        }
        return k;
}
```

Саволҳо барои мустаҳкамкунӣ

1) Барои муайянкунии қисми бутун ва касрии ададӣ ҳақиқӣ додашуда аз кадом функсияҳо истифода бурда мешавад?
2) Функсияи мултипликативӣ гуфта, чӣ гуна функсияро меноманд?
3) Функсияи Эйлер барои чӣ истифода бурда мешавад?

4) Барои ёфтани сумма ва миқдори тақсимкунандаҳои адад аз кадом формулаҳо истифода бурда мешавад?
5) Чӣ тавр $n!$ −ро ба тақсимкунандаҳои сода ҷудо кардан мукин аст?

Боби 3. Муқоисаҳо. Синфи тафриқҳо

1. Мафҳуми муқоиса ва таърифҳои асосӣ

Таърифи 1. Ададҳои a ва b аз рӯйи модули m муқоисашаванда номида мешаванд, агар фарқи онҳо $(a-b)$ ба m бебақия тақсим шавад, яъне чунин адади бутуни к мавҷуд бошад, ки баробарии зерин иҷро гардад:

$$a-b=km$$

Мисоли 1. Ададҳои 5, 9, 13, 17, 21, -3, -7, -11,.... дар вақти тақсим ба адади $m=4$ дорои бақияҳои якхелаи $r=1$ мешаванд.

$-3=4(-1)+1;$
$5=4+1;$
$-11=4(-3)+1.$

Муқоисашавандагии ду ададди a ва b - ро аз рӯйи модули m чунин ишора мекунанд:

$$a\equiv b(mod\ m) \qquad (1)$$

Мисоли 2.

$$4\equiv -3(mod\ 7)$$
$$36\equiv 6(mod\ 5)$$
$$11\equiv 40(mod\ 17)\ .$$

Теоремаи 1. Муқоисаи (1) бо баробарии зерин баробарқувва мебошад:

$a=b+mt,$ t – ададди бутуни (2).

Исбот. Бигузор (1) ҷой дошта бошад. он гоҳ ҳосил мекунем:

$$a=mq+r \qquad (0\le r<m),$$
$$b=mq_1+r \qquad (0\le r<m).$$

Аз ин ҷо бармеояд:

$a - b = mq + r - mq_1 - r = m(q - q_1)$, $a = b + m(q - q_1)$.

Азбаски $q - q_1$ адади бутун аст, аз ин ҷо $a = b + mk$ мешавад. Дар ин ҷо исбот карда шуд, ки (2) ҳангоми иҷрошавии баробарии (1) ҷой доштааст.

2. Хосияти муқоисаҳо

Хосияти 1. Агар ду адад бо адади сеюм аз рӯйи модулҳои m муқоисашаванда бошанд, он гоҳ онҳо байнихуд низ аз рӯйи ҳамон модул муқоисашаванда мешаванд. Дар ҳақиқат, агар $a \equiv c\ (mod\ m)$, $b \equiv c\ (mod\ m)$ бошад, он гоҳ $a \equiv b\ (mod\ m)$ мешавад.

Хосияти 2. Ду ё якчанд муқоисаи аз рӯйи як модулро аъзо ба аъзо ҷамъ кардан мумкин аст.

Дар ҳақиқат

$$\begin{array}{l} a_1 \equiv b_1\ (mod\ m) \Leftrightarrow a_1 = b_1 + mt_1 \\ a_2 \equiv b_2\ (mod\ m) \Leftrightarrow a_2 = b_2 + mt_2 \end{array} \ +$$

$$a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2) \Longrightarrow a_1 + b_1 \equiv b_1 + b_2 (mod\ m).$$

Хосияти 3. Ду ё якчанд муқоисаи аз рӯйи як модулро аъзо ба аъзо зарб кардан мумкин аст.

Дар ҳақиқат:

$$\begin{array}{l} a_1 \equiv b_1\ (mod\ m) \Leftrightarrow a_1 = b_1 + mt_1 \\ a_2 \equiv b_2\ (mod\ m) \Leftrightarrow a_2 = b_2 + mt_2 \end{array} \ \times$$

$$a_1 \cdot a_2 = b_1 \cdot b_2 + m(b_1 \cdot t_2 + b_2 t_1 + mt_1 t_2) \Longrightarrow$$
$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 (mod\ m).$$

Хосияти 4. Ҳар ду тарафи муқоисаро ба дараҷаи натуралӣ бардоштан мумкин аст.

Исботи ин хосият аз хосияти 3 бармеояд.

Мисол. Дода шудааст:

$$4 \equiv -3\ (mod\ 7)$$

Ҳангоми $n = 2$: $16 \equiv 9(mod\ 7)$

Ҳангоми $n = 3$: $64 \equiv -27(mod\ 7)$

… … … … … … … … … … … … …

Хосияти 5. Ҳар ду тарафи муқоисаро ба ададиихтиёрии бутуни k зарб кардан мумкин аст .

Дар ҳақиқат:

$$\begin{array}{l} a \equiv b(mod\ m) \Leftrightarrow a = b + mt_1 \\ k \equiv k(mod\ m) \Leftrightarrow k = k + mt_2 \end{array} \times$$

$$a \cdot k = b \cdot k + m(bt_2 + kt_1 + mt_1t_2 \Rightarrow a \cdot k \equiv b \cdot k(mod\ m)$$

Мисол. Дода шуда аст.

$$4 \equiv -3\ (mod\ 7)$$

Ҳангоми $k = 2$: $8 \equiv -6(mod\ 7)$

Ҳангоми $k = -2$: $-8 \equiv 12(mod\ 7)$

Ҳангоми $k = 5$: $20 \equiv -157mod\ 5)$

Хосияти 7. Агар ададҳои a ва b аз рӯйи чанд модули гуногуни $m_1, m_2, \ldots, m_n$ муқоисашаванда бошанд, он гоҳ ин ададҳо аз рӯйи модуле, ки ба ХКУ-и ин модулҳо баробар аст, низ муқоисашаванда мешаванд.

Исбот. Бигузор баробарии зерин ҷой дошта бошад:

$$\left.\begin{array}{l} a \equiv b(mod\ m_1) \\ a \equiv b(mod\ m_2) \\ a \equiv b(mod\ m_3) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a \equiv b(mod\ m_n) \end{array}\right\} \qquad (1)$$

Аз (1) маълум мешавад, ки $a - b$ тақсимшавандаи умумии ададҳои $m_1, m_2, \ldots, m_n$ мебошад . Мо медонем, ки

тақсимшавандаи умумии ду ё чанд ададҳо ба ХКУ-и онҳо каратӣ мебошад, яъне

$$\frac{a-b}{[m_1, m_2, \dots, m_k]} \qquad (2)$$

Муносибати (2) нишон медиҳад, ки $a \equiv b(mod[m_1, m_2, \dots, m_k])$ мебошад.

Хосияти 7. Агар ададҳои a ва b аз рӯйи модули m муқоисашаванда бошанд, он гоҳ онҳо аз рӯйи ҳар гуна тақсимкунандаҳои он модул низ муқоисашаванда мешаванд.

Хосияти 8. Ҳарду тарафи муқоисаро бо тақсимкунандаи умумии онҳо тақсим кардан мумкин аст, агар охирон бо модул байнан сода бошад.

Дар ҳақиқат, аз $a \equiv b(mod\ m).\ a = a_1 d, b = b_1 d$ ва (d, m)=1 бармеояд, ки фарқи $a - b$, ки ба $(a_1 - b_1)d$ баробар аст, ба m тақсим мешавад. Бинобар ин $a_1 - b_1$ба m тақсим мешавад, яъне $a_1 \equiv b_1(mod\ m)$ аст.

Хосияти 9. Ҳарду тарафи муқоиса ва модулро ба як ададӣ бутун зарб кардан мумкин аст.

Хосияти 10. Ҳарду тарафи муқоиса ва модулро ба ҳар гуна тақсимкунандаи умумии онҳо тақсим кардан мумкин аст.

Хосияти 11. Агар як тарафи муқоиса ва модул ба ягон адад тақсим шавад, тарафи дигараш ҳам ба он тақсим мешавад.

Хосияти 12. Агар $a \equiv b(mod\ m)$ бошад, он гоҳ $(a, m) = (b, m)$ мешавад.

Хосияти 13. *Дилхоҳ ду адади бутун аз рӯйи модули* 1 муқоисашаванда мебошанд.

Хосияти 14. Ба *дилхоҳ* тарафи муқоиса метавон, адади ихтиёрии ба модул каратиро илова кард:

$$\begin{array}{l} a \equiv b\ (mod\ m) \ \Leftrightarrow a = b + mt_1 \\ mk \equiv 0\ (mod\ m) \ \Leftrightarrow mk = 0 + mt_2 \end{array} \quad + \qquad a + mk = b + 0 + m(t_1 + t_2) \Longrightarrow a + mk \equiv b(mod\ m)$$

Хосияти 15. Аъзое, ки дар як тарафи муқоиса ҷойгир аст, метавон онро ба аломати баръакс ба тарафи дигари муқоиса гузаронид.

Дар ҳақиқат,

$$\begin{array}{l} a + b \equiv c\ (mod\ m) \ \Leftrightarrow a + b = c + mt_1 \\ -b \equiv -b\ (mod\ m) \ \Leftrightarrow -b = -b + mt_2 \end{array} \quad + \qquad a + b + (-b) = c + (-b) + m(t_1 + t_2) \Longrightarrow a \equiv c - b(mod\ m)$$

Қайд кардан ба маврид аст, ки муқоисаҳо илова ба хосиятҳои овардашуда, инчунин дорои хосияти зерин мебошанд:

Рефлексивӣ: барои *дилхоҳ* адади a баробарии $a \equiv a\ (mod\ p)$.

Симметрӣ: агар $a \equiv b\ (mod\ p)$ бошад, $b \equiv a\ (mod\ p)$ мешавад.

Транзитивӣ: агар $a \equiv b\ (mod\ p)$ ва $b \equiv c\ (mod\ p)$ бошад, он гоҳ $a \equiv c\ (mod\ p)$ мешавад.

3. Системаи пурраи тафриқҳо

Таърифи 1. Синфи тафриқҳои адади x аз рӯйи модули натуралии n гуфта, маҷмӯи ҳамаи ададҳои бутунеро меноманд, ки бо адади x аз рӯйи модули

m муқоисашавандаанд. Синфи тафриқҳои адади x −ро бо $\bar{x}$ ё $[x]$ ишорат мекунанд, яъне:

$$\bar{x} = \{y \in Z : y = x \ (mod \ m)\}.$$

Қайд. Дар ин ҷо $[x]$ –синфи тафриқҳои адади x −ро ифода мекунад.

Мисол. Бигузор $n = 3$ бошад, он гоҳ ададҳои бутун ба се класси тафриқҳо ҷудо аст:

$\bar{0} = \{-6, -3, 0, 3, 6, ...\}$ - ададҳое, ки ҳангоми тақсим ба 3 бақияашон ба 0 баробар аст.

$\bar{1} = \{..., -8, -5, -2, 1, 4, 7, ...\}$ - ададҳое, ки ҳангоми тақсим ба 3 бақияашон ба 1 баробар аст.

$\bar{2} = \{..., -7, -3, -1, 2, 5, 8, ...\}$ - ададҳое, ки ҳангоми тақсим ба 3 бақияашон ба 2 баробар аст.

Азбаски, муқоисашавиҳо аз рӯйи модули m дар маҷмӯи ададҳои бутун $\mathbb{Z}$ дорои муносибати эквивалентӣ мебошанд, пас синфи тафриқҳо аз рӯйи модули m синфҳои эквивалентиро ифода мекунанд. Миқдори онҳо ба m баробар мебошад. Маҷмӯи ҳамаи синфи тафриқҳоро аз рӯйи модули m бо $\mathbb{Z}_m$ ё $\mathbb{Z}/m\mathbb{Z}$ ишора мекунанд.

Амалҳои ҷамъ ва зарб дар синфи тафриқҳо аз рӯйи формулаҳои зерин ҳисоб карда мешаванд:

$$[x] + [y] = [x+y], \ [x]\,[y] = [xy]$$

Теоремаи 1. Сумма ва ҳосили зарби синфи тафриқҳо аз интихоби намояндаи синфҳо вобастагӣ надорад.

Исбот. Бигузор $[x]=[x']$ ва $[y]=[y']$ бошад. Он гоҳ $x \equiv x' \pmod{m}$, $y = y'(mod\ m)$ мешавад. Хосияти муқоисаҳоро истифода бурда ҳосил мекунем:

$$x' + y' = x + y(mod\ m), x' \cdot y' = x \cdot y(mod\ m),$$

Ҳамин тариқ $[x' + y'] = [x + y]$ ва $[x' \cdot y'] = [x \cdot y](mod\ m)$.

Мисол. Маҷмӯи зеринро дида мебароем:

$$\mathbb{Z}_{12} = \{[0], [1], \dots, [11]\}$$

Аз ин маҷмӯъ якчанд мисоли ҷамъ ва тарҳро дида мебароем:

$$[5]+[8]=[1],\ [5]\cdot[8]=[4],\ [3]\cdot[8]=[0].$$

Қайд кардан мумкин аст, ки ададҳое, ки дохили як синфанд, аз рӯйи модули додашуда баробарбақия мебошанд:

$$-8 \equiv -2(mod\ 3),\ \ 5 \equiv 8(mod\ 3), \dots$$

Аз ҳар як синф фақат як намояндаро гирифта, системаи пурраи тафриқҳоро аз рӯйи модули m ҳосил мекунем.

Таъриф. Системаи ададҳое, ки аз ин гуна намояндаҳо иборат аст, системаи пурраи тафриқҳо номида мешавад .

Масалан, ададҳои −6, -2, 5 системаи пурраи тафриқҳоро аз рӯйи модули $m = 3$ ифода мекунанд.

Айнан ҳамин тавр системаи ададҳои зерин аз рӯйи модули $m = 4$ системаи пурраи тафриқҳоро ташкил мекунад: $5, 1, 17, 3, 13$.

Бо мақсади осон намудани баъзе ҳисобкуниҳо, одатан системаи пурраеро мегиранд, ки аз тафриқҳои ғайриманфии хурдтарин (ки онҳо ба худи бақияҳо

баробаранд) иборатанд. Ғайр аз ин баъзан системаи тафриқҳо мутлақан хурдтарин гирифта мешаванд. Барои мисоли мо ин система чунин аст: 0,1,2.

4. Хосияти тафриқҳо

Хосияти 1. Ҳар гуна m – то ададҳои бо модули m ҷуфт-ҷуфт ба ҳамдигар муқоисанашаванда, системаи пурраи тафриқҳоро аз рӯйи ин модул ташкил мекунанд.

Дар ҳақиқат, азбаски ададҳо бо ҳамдигар муқоисашаванда нестанд, пас онҳо ба синфҳои гуногун тааллуқ доранд ва аз сабаби он, ки миқдори онҳо ба миқдори синфҳо, яъне бо m баробар аст, пас албатта ба ҳар як синф яктогӣ адад рост меояд.

Хосияти 2. Агар КТУ$(a,m)=1$ бошад ва x системаи пурраи тафриқҳоро аз рӯйи модули m қабул намояд, он гоҳ барои ададӣ бутуни ихтиёрии b, $ax+b$ ҳам системаи пурраи тафриқҳоро аз рӯйи модули m ташкил медиҳад.

5. Системаи овардашудаи тафриқҳо

Синфе ки тафриқҳои он бо модул байнан содаанд, аз рӯйи ҳамон модул синфи сода номида мешавад.

Масалан, аз рӯйи модули $m=5$ синфҳои сода ин ададҳои зерин мебошанд:

$$\overline{1}\,\overline{2}\,\overline{3}\,\overline{4}$$

Аз рӯӣ модули $m=4$ синфҳои сода инҳоянд: $\overline{1},\overline{3}$. аз рӯйи модули $m=10$ бошад, ададҳои $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$ синфҳои сода мебошанд.

Барои тартиб додани системаи овардашудаи тафриқҳо аз системаи пурраи тафриқҳо ҳамон ададҳоро гирифтан лозим аст, ки бо $mod\ m$ байнан сода бошанд .

Масалан, аз рӯйи модули $m = 10$ ададҳои 1,3,7,9 системаи пурраи тафриқҳоро ифода мекунанд. Миқдори ададҳо дар системаи овардашудаи тафриқҳо аз рӯйи $mod\ m$ ба $\varphi(m)$ баробар аст, ки дар ин ҷо $\varphi(m)$-функсияи Эйлер аст.

Теоремаи 1. Агар x ҳамаи қиматҳои тафриқҳои системаи овардашударо аз рӯйи модули m қабул кунад, он гоҳ ададҳои $a \cdot x$ дар ҳолати $(a, x) = 1$ будан системаи овардашудаи тафриқҳоро аз рӯйи ҳамон модули m ташкил мекунанд.

6. Теоремаи Эйлер ва Ферма

Теоремаи хурди Ферма[1]**.** Агар p адади сода буда, a адади бутуни ба p тақсимнашаванда бошад, он гоҳ муқоисаи зерин иҷро мешавад.

$$a^{p-1} \equiv 1(mod\ p) \qquad (1)$$

Мисоли 1. Ҳисоб карда шавад. $31^{98}\ (mod\ 47)$.

Ҳал. $31^{98}\ (mod\ 47) = 31^{46 \cdot 2+6}\ (mod\ 47) = 31^{6}\ (mod\ 47)$.

[1] Пиер де Ферма (фр. Pierre de Fermat) математики бузурги фаронсавӣ, яке аз асосгузорини геометрияи аналитикӣ, таҳлили математика ва назарияи ададҳо ба ҳисоб рафта 17 августи соли 1601 дар шаҳри Бомон-де-Ломан (Beaumont-de-Lomagne, Франсия) ба дунё омадааст. 12-уми январи соли 1665 аз олам чашм пушидааст.

Теоремаи Эйлер. Дар вақти $m > 1$ ва $(a, m) = 1$ будан, баробарбақияи зерин ҳамавақт ҷой дорад:

$$a^{\varphi(m)} \equiv 1(mod\ m) \qquad (2)$$

Мисоли 2. Ҳисоб карда шавад. 21^{99} $(mod\ 38)$.

Ҳал. Ибтидо $\varphi(38)$ −ро ҳисоб мекунем, ки ба 18 баробар аст. Аз ин ҷост, ки $21^{18} = 1(mod\ 38)$ мешавад. Пас, 21^{99} $(mod\ 38) = 21^{18\cdot 5+9} = 21^{9}$ $(mod\ 38)$ мешавад.

Барои ҳисоб намудани натиҷаи охирон аз алгоритми зуд бадарачабардорӣ истифода карда мешавад. Баъдтар ин алгоритмро мавриди баҳс қарор медиҳем.

Теорема. Бигузор p ва q ададҳои сода буда, $p \neq q$ ва k-ададӣ ихтиёрӣ бошад. Он гоҳ баробарии зерин иҷро мешавад.

$$a^{k\varphi(pq)+1}\ mod\ (pq) = a.$$

Мисоли 3.

$$9^{49}\ mod\ 35\ = 9^{2\cdot 24+1}\ mod\ 35\ =\ 9$$
$$10^{49}\ mod\ 35\ = 10^{2\cdot 24+1}\ mod\ 35\ =\ 10$$

Таъриф. Бигузор ададҳои c ва m байниҳам сода бошанд. Ададӣ d аз рӯйи модули m ба ададӣ c баръакс номида мешавад, агар баробарии $cd\ mod\ m = 1$ иҷро гардад. Аз ин ҷо ҳосил мекунем: $d = c^{-1}\ mod\ m$.

7. Алгоритми зуд бадарачабардорӣ

Барои ҳисоб намудани қимати ифодаи $z = a^b mod\ p$ якчанд алгоритм мавҷуд аст, ҳоло мо алгоритми сода ва тез ҳисобкунии онро дида мебароем, чунин иҷро карда мешавад:

1) Ададди b - ро ба системаи ҳисоби дӯӣ мегардонем: b=($b_0, b_1, \dots, b_k$), $b_i \in \{0,1\}$.
2) Ҷадвали зеринро пур мекунем:

B	b_0	b_1	…	b_k
A	a_0	a_1	…	a_k

дар ин ҷо a_i чунин муайян карда мешавад:

$$a_0 = a, a_{i+1} = \begin{cases} {a_i}^2 \ mod\ n, b_{i+1} = 0, i \geq 0, \\ {a_i}^2 \cdot a \ mod\ n, b_{i+1} = 1, \end{cases}$$

Мисол. Қимати $2^{199}\ mod\ 1003$ ҳисоб карда шавад.

1) b=$199_{(10)} = (11000111)_2$;
2) Ҷадвали зеринро пур мекунем:

B	1	1	0	0	0	1	1	1
A	2	8	64	84	35	444	93	247

Ҷавоб. $2^{199}\ mod\ 1003$ =247

Варианти дигари ин алгоритм мавҷуд аст, ки дар он пешаки ба намуди дӯи табдил додани ададди b-ро талаб намекунад. Варианти мазкур ба намуди зербарнома (дар C++) дар поён оварда шудааст:

```
long int pown(long int a, long int b, long int n)
{
 long int c=1;
 while (b){
  if (b % 2==0)
{
            b/=2;
            a=(a*a)%n;
   }
 else  {
```

```
  b--;
  c=(c*a)%n;
 }
}
return c;
}
```

8. Муқоисаҳои номаълумдор

Шакли умумии муқоисаи номаълумдор чунин аст:

$$f(x) \equiv 0(mod\ m) \qquad (1)$$

дар ин ҷо $f(x) = a_0x^n + a_1x^{n-1} + \cdots a_n -$ бисёраъзогии дараҷаи n бо коэфисентҳои бутун мебошад.

Дар ҳолати a ба m каратӣ набудан, n –ро дараҷаи муқоиса меноманд. Ҳалли муқоисаи (1) гуфта, чунин ададӣ x_0 –ро меноманд, ки онро қаноат кунонад.

Агар ягон қимати $x = x_0$ муқоисаи (1)-ро қаноат кунонад, он гоҳ онро ҳамаи ададҳои аз рӯйи модули m муқоисашаванда низ қонеъ мегардонанд.

Таърифи 1. Ду муқоисае, ки онҳоро қиматҳои якхелаи x қонеъ мегардонад, баробарқувва номида мешаванд.

Масалан, муқоисаи $x^2 + 3x + 6 \equiv 1(mod\ 5) -$ ро ададӣ 2 қаноат мекунонад, пас $x \equiv 2(mod\ 5)$ мешавад, яъне онро ададҳои $2, 7, 12, 17, 22, \ldots$ низ қаноат мекунонанд.

Аз ҳамин сабаб, агар $f(x) \equiv 0(mod\ m)$ ҳал дошта бошад, он гоҳ ин ҳалҳоро дар байни ададҳои системаи тафриқҳои пурра кофтан лозим меояд.

9. Муқоисаи дараҷаи якум

Намуди умумии муқоисаи дараҷаи якум шакли зеринро дорад:

$$ax \equiv b(mod\ m) \qquad (1)$$

Агар КТУ $(a,m) = d > 1$ бошад ва b ба d тақсим шавад, он гоҳ муқоиса d-то ҳал дорад. Дар ҳолати хусусӣ ҳангоми $d = 1$ будан муқоисаи (1) ҳалли ягона дорад.

Агар b ба КТУ(a,m) каратӣ набошад муқоиса ҳал надорад.

Агар дар (1) КТУ$(a,m) = 1$ бошад, он гоҳ (1) бо ду усул ҳал карда мешавад:

1) $x = a^{\varphi(m)-1}b(mod\ m)$,

2) $x = (-1)^{n-1}p_{n-1}b(mod\ m)$,

дар ин ҷо $\varphi(m)$ – функсияи Эйлер, n -миқдори ҳосили тақсим дар алгоритми Евклид ва p_{n-1} - сурати касри муносиби пеш аз охир аст.

Агар $(a,m) = d$ буда, d ба b бебақия тақсим шавад, он гоҳ муқоисаро ба d ихтисор карда, ҳосил мекунем: $x \equiv x_0(mod\ m_1)$. Дар ин ҳолат ҳалҳои (1)-ро ададҳои додашудаи зерин ташкил мекунанд:

$$\begin{cases} x \equiv x_0(mod\ m), \\ x \equiv x_0 + m_1(mod\ m), \\ x \equiv x_0 + 2m_2(mod\ m), \\ \quad \dots\dots\dots\dots\dots\dots\dots\dots. \\ x \equiv x_0 + (d-1)(mod\ m). \end{cases}$$

мешаванд.

Қайд кардан ба маврид аст, ки муқоисаи $ax \equiv b(mod\ m)$ бо $ax \equiv b + my$ баробарқувва мебошад, аз ин ҷо

ҳар як муодилаи номуайяни дараҷаи якуми дуномаълумаро метавон ба муқоисаи дараҷаи якумии якномаълума табдил дод.

Мисоли 1. Муқоисаи $3x \equiv 2(mod\ 7)$ ҳал карда шавад:

Ҳал. Азбаски $(3,7) = 1$ аст, пас, ҳосил мекунем:
$x \equiv 3^{\varphi(7)-1} \cdot 2(mod\ 7) \Rightarrow x \equiv 3^5 \cdot 2(mod\ 7) \equiv 486(mod\ 7) \equiv 3(mod\ 7)$, азбаски $486 = 7 \cdot 69 + 3$ аст, пас ҳалли умуми шакли зеринро мегирад.

$$x = 3 + 7t;\ t = 0, \pm 1, \pm 2, \ldots.$$

Барои бо ин усул ҳал кардани муқоисаҳо метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард.

```
int mod (int a, int b){
  if (a<0)
        return (b+(a%b));
  else
        return a%b;
}
long KTU(long a, long b){
 while (b!=0) {
        long t=a%b;
        a=b;
        b=t;
 }
 return a;
}
 long Eiler(long int a){
```

```
        int k=0;
        for (int i=1; i<a; i++){
                if (KTU(a,i)==1)
                        k++;
        }
        return k;
}
 int resha(long int a, long int b, long int m){
        if (KTU(a,m)==1){
 int x=mod((int)(pow(a, (Eiler(m)-1))*b) ,m);
                return x;
        }
        else
                return 0;
}
```

Мисоли 2. Муқоисаро бо ёрии касрҳои муносиб ҳал кунед:

$$7x \equiv 4(mod\ 19)\ ;$$

Ҳал. Ҳалли муқоисаи намуди зеринро дорад:

$$x \equiv (-1)^n bp_{n-1}(mod\ m), a = 7, b = 4, m = 19.$$

ҳисоб мекунем:

$$19 = 7 * 2 + 5$$
$$7 = 5 * 1 + 2$$
$$5 = 2 * 2 + 1$$
$$2 = 2 * 1 + 0$$

Пас аз ин, ҷадвали касрҳои мувофиқро тартиб медиҳем, ки шакли зеринро мегирад:

q			2	1	2	2
p	0	1	2	3	8	19

$n = 3,\ \ p_{n-1} = 8$

Аз ин ҷо $x = (-1)^3 \cdot 4 \cdot 8 = -32 \equiv -13 \equiv 6(mod\ 19)$ мешавад.

Санҷиш : $7 \cdot 6 \equiv 4(mod\ 19)$.

Мисоли 3. Ҳисоб кунед: $2x \equiv 7(mod\ 8)$.

Ҳал. $a = 2, b = 7, m = 10,$ КТУ$(a, m) = (5,8) = 2.$

Аммо 7 ба 2 тақсим намешавад, пас муқоиса ҳал надорад.

Мисоли 4. Ҳалҳои бутуни муодилаи зерин ёфта шавад:

$$11x + 16y = 156$$

Ҳал. Аз $11x + 16y = 156$ ҳосил мекунем : $11x \equiv 156(mod\ 16)$

Барои 11 ва 16 КТУ-ро аз рӯйи алгоритми Евклид меёбем :

$$11 = 16 * 0 + 11$$
$$16 = 11 * 1 + 5$$
$$11 = 5 * 2 + 1$$
$$5 = 1 * 5 + 0$$

Аз ин ҷо (11,16)=1, n=2 ва d=156 мебошад. Ҷадвали касрҳои муносибро тартиб медиҳем :

q				1	2	5
p		0	1	1	3	16

Маълум мешавад, ки $p_{n-1} = 3$ аст. Бинобар ин:
$x \equiv (-1)^n b p_{n-1}(mod\ m) = (-1)^2 \cdot 156 \cdot 3 = 468 \equiv 4(mod\ 16)$, яъне $x = 4 + 16t$ мешавад. Қимати x -ро ба $11x + 16y = 156$ гузошта y-*ро* меёбем :

$$11(4 + 16t) + 16y = 156;$$

$44 + 11 \cdot 16t + 16y = 156$;

$16y = 112 - 11 \cdot 16t$;

$y = 7 - 11t$.

Ҷавоб: $x = 4 + 16t;\ y = 7 - 11t$.

Барои тавассути касрҳои бефосила ҳал кардани муодилаи (1) метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард:

```
int mod (int a, int b){
if (a<0)
        return (b+(a%b));
else
        return a%b;
}
 void pown(long int a, long int b, long int m){
  vector<int>q, p;
  int k=2, n=0, m1=m;
  q.push_back(0);
  q.push_back(0);
  p.push_back(0);
  p.push_back(1);
  while(m%a!=0){
          int h=m%a;
          q.push_back(m/a);
          m=a;
          a=h;
         }
 q.push_back(m/a);
 n=q.size();
```

```
 while (k<n){
          int t=q[k]*p[k-1]+p[k-2];
          p.push_back(t);
          k++;
 }
for (int i=0; i<n; i++){
        cout<<q[i]<<"   ";
 }
cout<<endl;
for (int i=0; i<n; i++){
        cout<<p[i]<<"   ";
 }
cout<<endl;
int x=mod((int)(pow(-1.0, n-3)*b*p[n-2] ),m1);
 cout<<"x="<<x;
}
```

10. Алгоритми васеъкардашудаи Евклид

Алгоритми васеъкардашудаи Евклид (АВЕ) дар аксар методҳои криптографӣ ва назарияи ададҳо истифода бурда мешавад. Алгоритми мазкур аз ду қисм иборат аст. Дар қисмати аввали он барои ададҳои додашудаи А ва В КТУ –и онҳо ҳисоб карда мешавад. Барои иҷрои ин амал метавон аз зербарномаи зерин истифода кард:

```
int Euclid (int A, int B){
 while (A%B !=0)
  {
```

```
  int C=A%B;
   A=B;
   B=C;
  }
return B;
}
```

Барои ҳал намудани муодилаи намуди $ax + by = d$, ки дар ин ҷо a ва b ададҳои додашуда буда, d КТУ –и онҳо мебошад, низ аз АВЕ истифода бурда мешавад. Қисми нахусти алгоритми АВЕ дар боло оварда шудааст. Қиматҳои a, b ва қисми бутуни ва бақияи тақсими a бар b дар ҷадвали зерин, ки дорои 4 сутун мебошад гирд оварда мешаванд:

I	A	B	A%B	[A/B]
1				
2				
3				
4				

Дар қисми дуюми алгоритм ба ҷадвал ду сутуни нав бо сарлавҳаҳои x ва y илова карда мешавад. Дар сатри охири сутунҳои мувофиқан 0 ва 1 навишта, бо истифода аз формулаҳои

$$x_i = y_{i+1}, y_i = x_{i+1} - y_{i+1} \cdot (a\ div\ b)_i$$

катакчаҳои боқимондаи ҷадвал пур карда мешаванд.

i	A	B	A%B	[A/B]	x	Y
1						
2						
⋮						
N					0	1

Мисоли 1. Муқоисаи $40x + 7y = 1$ ҳал карда шавад.

Ҳал. Аз АВЕ истифода бурда мешавад. Дар ин ҷо $A = 40, B = 7$ аст.

I	A	B	A%B	[A/B]	x	y
1	40	7	5	5	3	-17
2	7	5	2	1	-2	3
3	5	2	1	2	1	-2
4	2	1	0	20	0	1

Қимати $x = 3$ ва $y = -17$, ки дар сатри нахустини сутунҳои x ва y мехобанд ҳалли мисоли додашуда мебошанд. Дар ҳақиқат

$$40 \cdot 3 + 7 \cdot (-17) = 1$$ мешавад.

Қайд мекунем, ки муодилаи $40x + 7y = 1$ ба муқоисаи $40x \equiv 1(mod\ 7)$ баробарқуввa мебошад.

Барои ёфтани элементи баръакс аз рӯйи модули додашуда низ метавон аз АВЕ истифода кард.

Мисоли 2. Барои e=7 элементи баръакс аз рӯйи модули таркибии $\varphi(n) = 40$ ёфта шавад.

Ҳал. Аз АВЕ истифода бурда мешавад. Дар ин ҷо $A = \varphi(n) = 40, B = e = 7$ аст:

i	A	B	A%B	[A/B]	x	Y
1	40	7	5	5	3	-17
2	7	5	2	1	-2	3
3	5	2	1	2	1	-2
4	2	1	0	20	0	1

Қимати y=-17, ки дар сатри нахустини сутуни x мехобад, элементи баръакс ба ададӣ е мебошад. Дар ҳақиқат:

$d = y \ mod \ \varphi\ (n) = -17 \ mod \ 40 = 23$ мешавад.

Барои ҳисобкунии элементи баръакс аз рӯйи модули p низ метавон аз зербарномаи зерин истифода кард, ки дар забони C++ навишта шудааст.

```
int modInverse(int n, int p) {
        n = mod(n, p);
        for (int x = 1; x < p; x++) {
                if (mod(n*x, p) == 1) return x;
        }
        return 0;
}
```

Қайд. *Барои аз рӯи модули додашуда, ёфтани элементи баракс* ($a^{-1} mod\ p$) *метавон аз зербарномаи modInverse()ки дар класси BigInteger ҷойгир аст, истифода кард. Метои мазкур барои ададҳои кифоя калон низ кор мекунад. Тарзи истифодаи ин зербарнома чунин аст:*

java.math.BigInteger.modInverse(BigInteger m)-Java
public BigInteger modInverse(BigInteger *m* **)-C#**

Мисол.

```
import java.math.BigInteger;
import java.util.Scanner;
public class myModInverse {
public static void main(String[] args) {
    BigInteger a,p,S;
```

```
        Scanner sc=new Scanner(System.in);
        a=sc.nextBigInteger();
        p=sc.nextBigInteger();
        S=a.modInverse(p);
        System.out.println(S);
    }
}
```

11. Муқоисаҳои квадратӣ

Акнун ба омӯхтани муқоисаҳои квадратӣ оғоз мекунем, ки навишти стандартии онҳо чунин аст:

$$x^2 \equiv a(mod\ p) \qquad (1)$$

Агар (1) дорои ҳал бошад, он гоҳ a-ро тафриқи квадратии модули p номида, бо нишонаи $\frac{a}{p} = 1$, дар сурати акс a-ро тафриқи ғайриквадратӣ номида, бо $\frac{a}{p} = -1$ ишорат мекунанд.

Ишораи $(\frac{a}{p})$-ро "ададиа нисбатан ба p" мехонанд ва онро нишонаи Лежандр[1] меноманд. Ин нишона чунин муайян карда мешавад:

[1] Адриен Мари Лежандр математики бузурги фаронсавӣ 18-сентябри соли 1752 дар шаҳри Париж (шоҳигарии Франсия) ба дунё омадааст 10-уми январи 1833 дар зодгоҳаш вафот кардааст.

$$\left(\frac{a}{p}\right)=\begin{cases}1, \text{агар (1) ҳалшаванда бошад,}\\ 0, \text{агар } a \text{ ба } p \text{ бебақия тақсим шавад,}\\ -1, \text{агар (1) ҳалнашаванда бошад.}\end{cases}$$

Нишонаи *Лежандр* барои ададҳои *дилхоҳи* $a, b,$ ки бо адади содаи $p \neq 2$ тақсим намешаванд, дорои хосиятҳои зерин мебошад:

1. Агар $a \equiv b(mod\ p)$ бошад, он гоҳ $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.
2. $\left(\frac{a+kp}{p}\right)=\left(\frac{a}{p}\right), \forall k \in \mathbb{Z}$ (ададӣ бутун),
3. $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$,
4. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$. *Дар ҳолат хусусӣ* $\left(\frac{1}{p}\right)=1$ барои ададӣ содаи *дилхоҳи* $p \neq 2$, $\left(\frac{-1}{p}\right)=1$ ҳангоми $p \equiv 1\ (mod\ 4)$ ва $\left(\frac{-1}{p}\right)=-1$ ҳангоми $p \equiv 3\ (mod\ 4)$,
5. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
6. **Леммаи Гаусс** [1] : $\left(\frac{a}{p}\right)=(-1)^{\mu}$, дар ин ҷо $\mu-$ ададӣ тафриқҳои манфӣ дар байни тафриқи мутлақ хурдтарини ададҳои $a, 2\cdot a, \dots, \frac{p-1}{2}a$ ҷойгирбуда.

[1] Ҷоҳанн Карл Фридрих Гаусс (нем. Johann Carl Friedrich Gauß) – математик, механик, физик, астроном ва геодези немис 30 апрели соли 1777 дар шаҳри Брауншвейг (Олмон) ба дунё омадааст. Ӯ 23-юми феврали соли 1855 дар шаҳри Гёттинген (Олмон) аз олам чашм пушидааст.

7. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, яъне

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ ҳангоми } p \equiv \pm 1 \ (mod\ 8) \text{ будан,} \\ -1, \text{ҳангоми } p \equiv \pm 3 \ (mod\ 8) \text{ будан.} \end{cases}$$

8. Қонуни бо ҳам квадратӣ будани тафриқҳо (қонуни Гаусс). Бигузор p ва q ададҳои содаи гуногун ($p \neq 2, q \neq 2$) бошанд. Он гоҳ $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$ мешавад. Бо суханҳои дигар

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{-q}{p}\right), \text{ агар } p \equiv q \equiv 3 \ (mod\ 4) \text{ бошад,} \\ \left(\frac{q}{p}\right), \text{дар акси ҳал.} \end{cases}$$

9. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Қайд. Ба ёд меорем, ки системаи пурраи тафриқҳо аз рӯйи модули m гуфта, маҷмӯи иборат аз m ададро меноманд, ки аз ҳар як синфи тафриқҳо аз рӯйи модули m яктогӣ намоянда гирифта шудааст. Маҷмӯи ададҳои $0, 1, \dots, m-1$ системаи тафриқҳои ғайриманфии хурдтарин номида мешаванд. Маҷмӯи ададҳои

$$0, \pm 1, \dots, \frac{m-1}{2} \text{ ҳангоми тоқ будани } m,$$

$$-\frac{m}{2}+1, \dots, -1, 0, 1, \dots, \frac{m}{2}, \text{ҳангоми ҷуфт будани } m.$$

бошанд, системаи тафриқҳои мутлақ хурдтарин аз рӯйи модули m номида мешаванд. Ҳар яке аз тафриқҳои матлақ хурдтарин аз нисфи модул зиёд намешаванд.

Мисол. Муайян мекунем, ки $x^2 \equiv 88(mod\ 347)$ ҳал дорад ё не?

Ҳал. Нишонаи $\left(\frac{88}{347}\right)$ -ро гирифта, 88 –ро ба зарбшавандаҳои сода ҷудо карда, $88 = 2^3 \cdot 11$ – ро ҳосил мекунем. аз рӯйи хосияти 5)

$\left(\frac{88}{347}\right) = \left(\frac{2^3 \cdot 11}{347}\right) = \left(\frac{2^3}{347}\right) \cdot \left(\frac{11}{347}\right)$ мешавад. Мувофиқи хосияти 3) ҳосил мекунем.

$\left(\frac{2^3}{347}\right) = \left(\frac{2^2 \cdot 2}{347}\right) = \left(\frac{2}{347}\right)$. Азбаски $347 \equiv 3\ (mod\ 8)$ аст, пас мувофиқи хосияти 7) ҳосил мекунем. $\left(\frac{2}{347}\right) = -1$. Барои ҳисобкунии $\left(\frac{11}{347}\right)$ аз қонуни Гаусс истифода мебарем:

$$\left(\frac{11}{347}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{347-1}{2}}\left(\frac{347}{11}\right) = (-1)^{5\cdot 173}\left(\frac{347}{11}\right) = -\left(\frac{347}{11}\right).$$

Азбаски $347 = 11 \cdot 31 + 6$ аст, пас мувофиқи хосияти 2) ҳосил мекунем. $\left(\frac{347}{11}\right) = \left(\frac{6}{11}\right)$-ро ҳосил мекунем. Аз нав хосияти 5) ро татбиқ карда ҳосил мекунем.

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right) \cdot \left(\frac{3}{11}\right).$$

Аз рӯйи хосияти 7) ҳосил мекунем:

$\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$. Мувофиқи хосияти 4:

$$\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1\ (mod\ 11).$$

Ҳамин тариқ

$\left(\frac{11}{347}\right) = -(-1 \cdot 1) = 1$ ва $\left(\frac{88}{347}\right) = -1 \cdot 1 = -1$ мешавад, яъне муқоиса ҳал надорад.

Бигузор дар $x^2 \equiv a(mod\ p)$ адади p мураккаб бошад. Азбаски ҳар як муқоисаи модули мураккаб ба модули сода

мубаддал мегардад, пас омӯхтани ҳолати $p = p_1 p_2 \dots . p_k$ кифоя аст.

Дар ин маврид $\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_k}\right)$ нишонаи Якобӣ [1] номида шуда, дар он низ ҳамаи хосиятҳои нишонаи Лежандр ҷой дорад .

Мисол. Ҳал доштан ё надоштани муқоисаи $x^2 \equiv 21(mod\ 55)$ санҷида шавад.

Ҳал. Нишонаи Якобӣ $\left(\frac{21}{55}\right)$ -ро тартиб дода, бо назардошти зарбшавандаҳои $21 = 3 \cdot 7$ ва $55 = 5 \cdot 11$ ҳосил мекунем:

$\left(\frac{21}{55}\right) = \left(\frac{21}{5 \cdot 11}\right) = \left(\frac{21}{5}\right)\left(\frac{21}{11}\right) = \left(\frac{3 \cdot 7}{5}\right)\left(\frac{3 \cdot 7}{11}\right) = \left(\frac{3}{5}\right)\left(\frac{7}{5}\right)\left(\frac{3}{11}\right)\left(\frac{7}{11}\right) =$

$= (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\left(\frac{5}{3}\right)\left(\frac{2}{5}\right)(-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right)(-1)^{\frac{7-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{7}\right) =$

$= \left(\frac{2}{3}\right)(-1)^{\frac{3^2-1}{8}}\left(\frac{2}{3}\right)\left(\frac{4}{7}\right) = -(-1)^{\frac{3^2-1}{8}}(-1)^{\frac{3^2-1}{8}}\left(\frac{2^2}{7}\right) = -1$ яъне муқоиса ҳал надоштааст.

Агар дар муқоисаи квадратии $x^2 \equiv a(mod\ p)$ (дар ин ҷо p адади сода аст) $\left(\frac{a}{b}\right) = 1$ бошад,

[1] Карл Густав Якоб Якобӣ (нем. Carl Gustav Jacob Jacobi) -математик ва механики немис 10-уми декабри соли 1804 дар оилаи банкири яҳудӣ Симон Якобӣ дар шаҳри Потсдам (шоҳигарии Пруссия) ба дунё омадааст. Якобӣ дар таҳлили комплексӣ, алгебраи хаттӣ, динамика ва дигар бахшҳои математика саҳми босазое гузоштааст. Ӯ узви АИ Берлин, (1836) ҷамъияти шоҳигарии Лондон, (1833) узви вобастаи АИ Петербург (1830) узви Венск (1848) ва узви вобастаи академияи Мадрид (1848) буд. Якоби 18-уми феврали соли 1851 дар шаҳри Берлин аз олам гузоштааст.

барои ёфтани ҳал ададҳои $\left(1,2,\dots,\frac{p-1}{2}\right)$-ро тафтиш карда албатта, як ададиַ $x \equiv x_1 (mod\ p)$ -ро ёфтан мумкин аст. Ҳалли дуюми он $x \equiv p - x_1 (mod\ p)$ мешавад.

Қайд кардан мумкин аст, ки агар a аз рӯйи модули р тафриқи квадратӣ бошад, пас муқоисаи (2) дорои ду ҳал мебошад.

Дар ҳақиқат, агар a тафриқи квадратӣ бошад, он гоҳ муқоисаи (1) ақалан дорои як ҳалли $x \equiv x_1 (mod\ p)$ –ро дорад. Дар ин ҳолат, азбаски $(-x_1)^2 = x_1$ аст, он гоҳ худи ҳамон муқоиса ҳалли дуюми $x \equiv -x_1 (mod\ p)$ – –ро низ дорад. Ин ҳалли дуюм аз ҳалли якум фарқ мекунад, чунки агар $x \equiv -x_1 (mod\ p)$ бошад, он гоҳ $2x_1 = (mod\ p)$ мешавад, ки ин ба шарти $(2, p) = (x_1, p) = 1$ зид аст.

Бо ҳалли нишондодашуда ҳамаи ҳалли муқоисаи (1) ба охир мерасад, чунки миқдори ҳалҳои муқоисаи дараҷаи дуюм аз ду зиёд нест.

Барномаи ҳисобкунии нишонаи Якобӣ дар забони C++

```
#include <assert.h>
#include <iostream>
using namespace std;
  bool odd(int b){
        return b % 2 == 1;
 }
 int gcd(int a, int b){
        int c;
        while (a != 0) {
```

```
                c = a;
                a = b%a;
                b = c;
        }
        return b;
}
int jacobi(int a, int b) {
        int g;
        assert(odd(b));
        if (a >= b) a %= b;
            if (a == 0)
                return 0;
        if (a == 1)       /*  аз рӯйи хосияти 4 */
                return 1;
          if (a < 0)
           if ((b - 1) / 2 % 2 == 0)
                 return jacobi(-a, b);
        else
                return -jacobi(-a, b);
            if (a % 2 == 0)  /* дар ҳолати ҷуфт
будани a*/
              if (((b*b - 1) / 8) % 2 == 0)
                return +jacobi(a / 2, b);
        else
                return -jacobi(a / 2, b);
         g = gcd(a, b);
        assert(odd(a));
       if (g == a) /* агар b ба a тақсим
```

```
шавад */
                return 0;
            else if (g != 1)
        return jacobi(g, b)*jacobi(a / g, b);
            else if (((a - 1)*(b - 1) / 4) % 2 == 0)
                return +jacobi(b, a);
                else
                        return -jacobi(b, a);
}
```

Баъдтар усули ҳал кардани муқоисаи квадратиро меорем.

Саволҳо барои мустаҳкамкунӣ

1) Чӣ гуна ададҳоро аз рӯйи модули додашуда муқоисашаванда меноманд?
2) Алгоритми зуд бадарачабардорӣ чӣ гуна алгоритм аст?
3) Нишонаи Лежандр аз нишонаи Якобӣ чӣ фарқ мекунад?
4) Синфи овардашудаи тафриқҳо аз синфи пурраи тафриқҳо чӣ фарқият дорад?
5) Чӣ тавр муқоисаҳои тартиби як ҳал карда мешаванд?
6) Моҳияти теоремаи кучаки Эйлер аз чӣ иборат аст?
7) Теоремаи кучаки Эйлер аз теоремаи Ферма чӣ фарқ дорад?
8) Чанд усули ҳалли муқоисаҳои тартиби як мавҷуд аст?

Боби 4. Гурӯҳ, ҳалқа ва майдон. Ҳалқаи тафриқҳо

Гурӯҳ[1], ҳалқа[2] ва майдон[3] яке аз мафҳумҳои асосии алгебра ба шумор мераванд. Пеш аз дида баромадани ин мафҳумҳо ибтидо якчанд маълумоти ёрирасонро мавриди баҳс қарор медиҳем.

1. Амалҳои бинарӣ

Амали бинарӣ (аз лот. bi–ду)-амали математикиест, ки ду аргумент қабул карда, як натиҷа бармегардонад.

Таъриф. Дар маҷмӯи M амали бинарӣ (дӯӣ) гуфта, инъикоси $f: M \times M \to M$-ро меноманд, ки ҳар як ҷуфти ба тартиб гузошташудаи элементҳои $(x, y) \in M \times M$ – ро (ки амалванд номида мешаванд) ба ягон элементи ҳамин

[1] Мафҳуми гурӯҳро соли 1830 математики фаронсавӣ Эварист Галуа ҳангоми омӯхтани бисёраъзогиҳо дар математика дохил кардааст.

[2] Инкишофи алгебра ҳамчун илм дар асри XIX оғоз гардид. Яке аз масъалаҳои асосии назарияи ададҳо дар солҳои 60-70-ум назарияи тақсимшавӣ дар майдони умумии ададҳои алгебравӣ ба ҳисоб мерафт. Ҳалли ин масъалаҳоро Р. Дедикинд соли 1871 чоп намуд. Дар кори ӯ нахустин маротиба мафҳуми ҳалқаи бутуни майдони ададӣ истифода шудааст.

[3] Мафҳуми майдонро соли 1871 математики немис Р. Дедикинд (*Julius Wilhelm Richard Dedekind* – 6 октябри соли 1831 — 12 феврали соли 1916) дар илми математика дохил намудааст.

маҷмӯъ xfy (ки онро натиҷа меноманд) мувофиқат мегузорад.

Амалҳои бинарӣ метавонанд, дорои хосиятҳои зерин бошанд:

a) Комутативӣ: $x \circ y = y \circ x, \quad \forall x, y \in M$.

b) Ассотсиативӣ: (x∘ y) $\circ z = x \circ (y \circ z), \quad \forall x, y, z \in M$.

c) Алтернативӣ: $(x \circ x) \circ y = x \circ (x \circ y)$ ва $y \circ (x \circ x) = (y \circ x) \circ x, \forall x, y \in M$.

Мисоли амалҳои бинарӣ, дар маҷмӯи ададҳои ҳақиқӣ метавонанд, амалҳои ҷамъ, зарб ва тарҳ бошанд. Дар ин ҷо амалҳои ҷамъ ва зарб дорои хосияти комутативӣ буда, амали тарҳ дорои чунин хосият намебошад.

2. Хосияти амалҳои арифметикӣ аз рӯйи модули додашуда

Амалҳои ҷамъ ва зарб аз рӯйи модули N тақрибан ба амалҳои арифметикӣ бо ададҳои бутун ва ададҳои ҳақиқӣ якхел иҷро карда мешаванд. Онҳо қисман дорои хосиятҳои зерин мебошанд:

1) Ҷамъи маҳдуд: $\forall a, b \in \mathbb{Z}/N\mathbb{Z}: \ a + b \in \mathbb{Z}/N\mathbb{Z}$.
2) Қонуни ассотсиативии ҷамъ: $\forall a, b, c \in \mathbb{Z}/N\mathbb{Z}$:
$$(a + b) + c = a + (b + c).$$
3) Сифр (элементи нейтралӣ) элементи ягона аз рӯйи амали ҷамъ мебошад, ки барои он баробарии зерин иҷро мешавад:
$$\forall a \in \mathbb{Z}/N\mathbb{Z}: \ a + 0 = a.$$

4) Аз рӯйи мали ҷамъ ҳама вақт мавҷуд будани элементи баръакс: $\forall a \in \mathbb{Z}/N\mathbb{Z}$: $a + (-a) = 0$.
5) Қонуни комутативии ҷамъ: $\forall a, b \in \mathbb{Z}/N\mathbb{Z}$: $(a + b) = b + a$.
6) Амали зарби маҳдуд: $\forall a, b \in \mathbb{Z}/N\mathbb{Z}$: $a \cdot b \in \mathbb{Z}/N\mathbb{Z}$.
7) Қонуни ассотсиативии зарб: $\forall a, b, c \in \mathbb{Z}/N\mathbb{Z}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
8) Воҳид (элементи нейтралӣ) элементи ягона аз рӯйи амали зарб мебошад, ки барои он баробарии зерин иҷро мешавад:
$$\forall a \in \mathbb{Z}/N\mathbb{Z}: \ a \cdot 1 = a.$$
9) Қонуни дистрибутивии амали зарб нисбат ба амали ҷамъ:
$$\forall a, b, c \in \mathbb{Z}/N\mathbb{Z}: : (a + b) \cdot c = a \cdot c + b \cdot c.$$
10) Қонуни комутативии зарб: $\forall a, b \in \mathbb{Z}/N\mathbb{Z}$: а$\cdot b = b \cdot a$.
11) Ҳама вақт мавҷуд будани элементи баръакс аз рӯйи амали зарб аст:
$$\forall a \in \mathbb{Z}/N\mathbb{Z}: \ a \cdot a^{-1} = 1.$$

3. Мафҳум ва мисолҳои гурӯҳ

Таърифи 1. Маҷмӯи G бо амали бинарии $\circ$ гурӯҳ номида мешавад, агар амали $\circ$ дорои хосиятҳои зерин бошад.

- маҳдуд;
- дорои элементи нейтралӣ;
- ассотсиативӣ;

- вобаста ба он барои ҳар як элемент мавҷуд будани элементи баръакс.

Гурӯҳ бо амали комутативӣ гурӯҳи комутативӣ ё абелӣ[1] номида мешавад. Тақрибан ҳамаи гурӯҳҳои дар криптография истифодаша-ванда абелӣ мебошанд. Маҳз ин хосият сабаби истифодаи васеъи онҳо дар криптография гардидааст. Бо суханҳои дигар, дилхоҳ маҷмӯи бо амали бинарӣ хосиятҳои 1-4-ро қаноаткунанда гурӯҳ номида мешавад. Агар ин маҷмӯъ ба ғайр аз ин хосиятҳо, хосияти 5-ро низ доро бошад, гурӯҳи абелӣ номида мешавад. Гурӯҳи абелиро одатан бо рамзи $(G,+)$ ишорат мекунанд.

Мисолҳои стандартии гурӯҳ, ки ҳатто аз математикаи элементарӣ маълуманд инҳо мебошанд:

- Маҷмӯи ададҳои бутун-$\mathbb{Z}$, ҳақиқӣ-$\mathbb{R}$ ва комплексӣ-$\mathbb{C}$ аз рӯйи амали ҷамъ. Дар ин ҷо элементи нейтралӣ, 0 ва элементи муқобил барои ягон x элементи $-x$ мебошад.
- Ададҳои ғайринулии ратсионалӣ, ҳақиқӣ ва комплексӣ аз рӯйи амали зарб. Дар ин ҷо элементи нейтралӣ 1 ва элементи баръакс ба ягон x элементи x^{-1} мебошад.
- Маҷмӯи ададҳои ҷуфт $2\mathbb{Z}$.

Илова бар мисолҳои овардашуда, маҷмӯи ҳамаи қиматҳои решаи n-ум аз воҳид, маҷмӯи ҳамаи ададҳои

[1] Нилс Ҳенрик Абел (норв. Niels Henrik Abel; 5 августа 1802, Финнёй — 6 апрели 1829, Фроланн) — математики норвегиягӣ.

комплексӣ аз рӯйи модули ба 1 баробар, маҷмӯи векторҳои ҳамворӣ ва фазо аз рӯйи амали ҷамъ, маҷмӯи ададҳои шакли $\rho\left(cos\frac{2\pi k}{n}+i\,sin\frac{2\pi k}{n}\right)$ (дар ин ҷо $\rho>0, k=0,1,2,\dots,n-1$) дошта низ гӯруҳро ташкил медиҳанд.

Мисоли 1. Исбот карда шавад, ки маҷмӯи {0}, ки аз як сифр таркиб ёфтааст, гурӯҳи комутативиро аз рӯйи амали ҷамъ ташкил медиҳад.

Ҳал. Дар ҳақиқат, амали ҷамъ дар ин маҷмӯъ муайян гардидааст, чунки барои он баробарии зерин ҷой дорад:

$$0+0=0$$

Аз ин баробарӣ бармеояд, ки 0 - ин элементи ягонаи маҷмӯи додашуда, элементи нейтралӣ буда, инчунин барои худаш элементи муқобил ба ҳисоб меравад. Дар ин ҷо хосияти ассотсиативӣ аён мебошад:

$$(0+0)+0=0+(0+0)$$

Ҳамин тариқ дар ин ҷо ҳар се шарти муайянкунии гурӯҳ иҷро мегарданд. Бо назардошти хосияти комутативии ҷамъ хулоса мебарорем, ки маҷмӯи дидашуда гурӯҳи комутативӣ аст.

Мисоли 2. Исбот карда шавад, ки маҷмӯи {+1,−1} (ки аз ду элемент иборат аст) аз рӯйи амали зарб гурӯҳи комутативиро ифода мекунад.

Ҳал. Дар ҳақиқат амали комутативӣ дар ин маҷмуъ муайян гардидааст, чунки

$$(+1)\cdot(+1)=+1,\quad (+1)\cdot(-1)=(-1)\cdot(+1)=-1,\quad (-1)\cdot(-1)=+1$$ аст.

Ҳамин тариқ, ҳосили зарби элементҳо, низ дар ин маҷмӯъ мехобад. Аз баробарии охирон бармеояд, ки дар он элементи воҳидии e=+1 низ мавҷуд аст. Илова бар ин ҳар як элемент дорои элементи баръакс мебошад.

$$(+1)^{-1} = +1,\ (-1)^{-1} = -1,$$

Тавре ки дида мешавад, ҳар се шарти таърифи гурӯҳ иҷро мешаванд. Бо назардошти хосияти комутативии зарб хулоса мебарорем, ки маҷмӯи додашуда комутативӣ аст.

4. Ҳалқа. Теорема ва таърифҳои асосӣ

Таърифи 1. Маҷмӯи R бо ду амали бинарӣ (бо таври анъанави бо символҳои «+» ва «·» ишора карда мешаванд), ки хосиятҳои 1-9-қаноат мекунонанд, ҳалқа номида мешавад. Ҳалқаро бо рамзи $\langle R, \cdot, + \rangle$ ишорат мекунанд.

Агар дар ҳалқа амали зарб комутативӣ бошад, ҳалқаро ҳалқаи коммутативӣ меноманд.

Мисолҳои стандартии ҳалқа, ки ҳатто аз мактаби миёна маълуманд инҳо мебошанд:

- Маҷмӯи ададҳои бутун-$\mathbb{Z}$;
- Маҷмӯи ададҳои ҷуфт $2\mathbb{Z}$;
- Маҷмӯи ададҳои шакли $a + b\sqrt{2}$ ва $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ дошта, ки дар ин ҷо a, b, c – ададҳои бутун мебошанд.

Таърифи 2. Ҳалқа ҳалқаи бо воҳид номида мешавад, агар он дорои воҳиди мултипликативӣ бошад, яъне дар он чунин элементи e мавҷуд бошад, ки $ae = ea = 1$ $(\forall a \in \mathbb{R})$ шавад.

Теоремаи 1. Маҷмӯи $\mathbb{Z}_m$ (синфи тафриқҳо аз рӯйи модули m) бо амалҳои ҷамъ ва зарб ҳалқаи тафриқҳоро бо воҳид ташкил мекунад.

Исбот. Иҷроиши ҳамаи хосиятҳои ҳалқаи комутативӣ бо воҳидро барои $\mathbb{Z}_m$ месанҷем:

1. Ҷамъи ассотсиативӣ

$$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]=[a+(b+c)]$$
$$=[a]+[b+c]=[a]+([b]+[c]).$$

2. Ҷамъи комутативӣ

$$[a]+[b]=[a+b]=[b+a]=[b]+[a].$$

Қайд. *Барои тафтиши хосиятҳои 1-2 аз хосияти комутативӣ ва ассотсиативии амали ҷамъ истифода бурда шудааст.*

3. Мавҷудияти элементи баръакс.

$$[a]+[0]=[a+0]=[a].$$

Қайд. *Ба сифати элементи нейтралӣ дар ин хосият аз маҷмӯи ададҳои каратии m истифода бурдан мумкин аст.*

4. Мавҷудияти элементи баръакс:

Дар класси $[a]$ элементи баръакс $[-a]$ ба ҳисоб меравад.

$$[a]+[-a]=[a+(-a)]=[0].$$

5. Зарби ассотсиативӣ:

$$([a]\cdot[b])\cdot[c]=[a\cdot b]\cdot[c]=[(a\cdot b)\cdot c]=[a\cdot(b\cdot c)]$$
$$=[a]\cdot[b\cdot c]=[a]\cdot([b]\cdot[c]).$$

6. Зарби комутативӣ:

$$[a]\cdot[b]=[a\cdot b]=[b\cdot a]=[b]\cdot[a].$$

7. Қонуни дистрибутивии зарб аз рӯйи ҷамъ:

$$([a]+[b])\cdot[c]=[a+b]\cdot[c]=[(a+b)\cdot c]=[a\cdot c+b\cdot c]=$$
$$=[a\cdot c]+[b\cdot c]=[a]\cdot[c]+[b]\cdot[c].$$

Қайд. *Ҳангоми тафтиши хосиятҳои 5-7 аз хосияти ассотсиативӣ, комутативӣ ва дистрибутивии ададҳои бутун истифода карда шудааст.*

8. Мавҷудияти элементи нейтралӣ:

$$[a] \cdot [1] = [a \cdot 1] = [a].$$

Тавре ки аён гашт, барои синфи $\mathbb{Z}_m$ ҳамаи хосиятҳои ҳалқаи комутативӣ бо воҳид иҷро мегарданд.

Ҳалқаи $\mathbb{Z}_m$ ҳалқаи класси тафриқҳо номида мешавад. Иҷроиши шартҳои 1-4 маънои абелӣ будани маҷмӯи $\mathbb{Z}_m$-ро аз рӯйи амали ҷамъ ифода мекунанд. Ин маҷмӯъ гӯрӯҳи аддитивии ҳалқаи $\mathbb{Z}_m$ номида мешавад. Дар ҳолати хусусӣ метавон барои синфи $\mathbb{Z}_m$ амали тарҳи синфҳоро муайян кард.

$$[a] - [b] = [a] + [(-b)]$$

Қайд кардан ба маврид аст, ки дар ҳалқа метавон амали зарби синф ба ададӣ бутун ва ба дараҷаи бутуни ғайриманфӣ бардоштани синфро иҷро кард:

$$n \cdot [a] = \underbrace{[a] + [a] + \cdots + [a]}_{n}, \quad -n \cdot [a] = n \cdot [(-a)], \quad 0 \cdot [a] = [0];$$

$$[a]^n = \underbrace{[a] \cdot [a] \cdot \ldots \cdot [a]}_{n}, \quad [a]^0 = [1];$$

Барои дилхоҳ синфи $[a] \in \mathbb{Z}_m$ баробариҳои зерин ҷой доранд:

$$\mathrm{c} \cdot [a] = [c \cdot a], \quad [a]^n = [a^n]$$

дар ин ҷо a ва c – ададҳои бутун буда, $n \geq 0$ аст.

Қайд кардан ба маврид аст, ки ҳангоми m=5 будан элементҳои класси $\mathbb{Z}_m$ ададҳои $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ буда, амали ҷамъ аз рӯйи модули m=5 чунин муайян карда мешавад:

$\bar{0}+\bar{1}=\bar{1},\ \bar{1}+\bar{2}=\bar{3},\bar{2}+\bar{3}=\bar{0},\ \bar{2}+\bar{4}=\bar{1}$ ва ҳоказо. Моҳияти амали ҷамъ дар синфи $\mathbb{Z}_5$ чунин муайян карда мешавад: Ибтидо ду элемент бо ҳамдигар ҷамъ карда шуда, сипас натиҷа аз рӯйи модули m=5 навишта мешавад. Ба ҳамин монанд барои синфи тафриқҳои $\mathbb{Z}_m$ низ амали ҷамъ муайян карда мешавад.

Усули мувофиқи тартибдиҳии гурӯҳҳои охирнок ба шакли ҷадвал мавҷуд аст, ки онро ҷадвали Кэли мегӯянд. Дар сатр ва сутуни нахустини ҷадвали мазкур мувофиқан ададҳои a ва b навишта шуда, сипас, дар катакчаҳои буриши сатру сутунҳо мувофиқан элементҳои $a \circ b$ навишта мешаванд.

Мисоли 3. Амали ҷамъ ва зарб барои синфи $\mathbb{Z}_5$ навишта шавад.

Ҳал. Тавре, ки қайд кардем, дар ин ҷо панҷ синфи тафриқҳоро аз рӯйи модули 5 дорем: $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$. Ҷадвали ҷамъ ва зарб мувофиқан чунин шаклро мегиранд:

«+»	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

« · »	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Мисол: $\bar{3}+\bar{4}=\overline{3+4}=\bar{7}=\bar{2}$; $\bar{3}\cdot\bar{4}=\overline{3\cdot 4}=\overline{12}=\bar{2}$.

Тавре ки дида мешавад, дар ҳар сатри ҷадвали зарб ба ғайр аз нахустин воҳид мавҷуд аст. Ин маънои онро дорад, ки барои ҳар як элементи ғайринулии $x \in \mathbb{Z}_5$ чунин элементи у мавҷуд аст, ки барои он $xy = 1$ мешавад.

Таърифи 1. Элементи $x \in \mathbb{Z}_m$ баргарданда номида мешавад, агар чунин элементи у$\in \mathbb{Z}_m$ мавҷуд бошад, ки барои он дар ҳалқаи $\mathbb{Z}_m$ баробарии зерин иҷро гардад:

$$[x][y] = 1.$$

Агар элементи x баргарданда бошад, он гоҳ чунин элементи y ягона мебошад ва тавассути рамзи x^{-1} ишора карда мешавад.

Таърифи 2. Элементи $x \in \mathbb{Z}_m$ тақсимкунандаи сифр номида мешавад, агар чунин элементи ғайрисифрии у $\in \mathbb{Z}_m$ мавҷуд бошад, ки барои он дар ҳалқаи $\mathbb{Z}_m$ баробарии зерин иҷро гардад:

$$[x][y] = 0.$$

Теоремаи 3. (Критерияи мавҷудияти элементи баргарданда) Элементи $x \in \mathbb{Z}_m$ фақат ва фақат ҳамон вақт баргарданда мебошад, агар КТУ$(x, m) = 1$ шавад.

Барои ёфтани элементи баргарданда (баръакс) метавон аз алгоритми васеъкардашудаи Евклид, ки қаблан дар боби 3 мавриди баҳс қарор гирифта буд истифода кард.

Мисоли 4. Ҳисоб карда шавад. $3^{-2}(\ mod\ 5)$

Ҳал. Ибтидо мисоли додашударо ба шакли $3^{-2}(\ mod\ 5) = (3^{-1})^2(\ mod\ 5)$ табдил дода, сипас аз алгоритми васеъкардашудаи Евклид ва формулаи зерин истифода мебарем:

$$x_i = y_{i+1}, \quad y_i = x_{i+1} - y_{i+1} \cdot (a \; div \; b)_i$$

I	A	B	A%B	[A/B]	X	y
1	5	3	2	1	-1	2
2	3	2	1	1	1	-1
3	2	1	0	2	0	1

Ҷавоб. Қимати y=2, ки дар сатри нахустини сутуни y мехобад, элементи баръакс ба ададu 3 мебошад. Дар ҳақиқат $(2 * 3)^2 \; (mod \; 5) = 1$ мешавад.

Қайд мекунем, ки ба ғайр аз ABE барои муайянкунии элементи баръакс метавон аз формулаи зерин низ истифода кард:

$$[a]^{-1} = \left[a^{\varphi(m)-1}\right].$$

Ҳангоми КТУ($[a], m) = 1$ будан, миқдори умумии классҳо ба $\varphi(m)$ баробар буда, маҷмӯи онҳо ба $\mathbb{Z}_m^*$ ишорат карда мешавад.

Аз ин ҷо бармеояд, ки $\mathbb{Z}_m^*$ гурӯҳи элементҳои баръакси синфи $\mathbb{Z}_m$ −ро ташкил карда, дар сурати ададu содаи р будани m гурӯҳи дорои элементи баръакс будаи $\mathbb{Z}_p^*$ ҳамаи синфҳои ғайрисифриро ташкил медиҳад $(\varphi(p) = p - 1)$.

Мисоли 5. Се рақами охирони ададu $A = 1997^{1997}$ ёфта шавад.

Ҳал. Дар ин ҷо гап дар бораи ҳисобкунии $[1997]^{1997}$ дар гурӯҳи $\mathbb{Z}_{1000}^*$ меравад. Ҳосил мекунем:

$$[1997]^{1997} = [-3]^{1997} = [-3]^{5 \cdot 400 - 3} = [-3]^{-3} = ([-3]^{-1})^3$$
$$= [333]^3 = [333^3] = [(333 \cdot 3)^2 \cdot 37]$$
$$= [(-1)^2 \cdot 37] = [37].$$

Дар ин ҷо мо аз теоремаи Эйлер $[-3]^{\varphi(1000)} = [-3]^{400} = [1]$ ва $333^3 = (333 \cdot 3)^2 \cdot 37$ истифода карда шудааст.

Дар натиҷа $A = \cdots 037$ ба даст меояд.

Мисоли 6. Ҳалқаи $\mathbb{Z}_{10}^*$- ро дида мебароем.

Ҳал. Ҳосил мекунем, $\mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}$, $\varphi(10) = 4$. Бо истифода аз формулаи (2) ҳосил мекунем:

$$[1]^{-1} = [1], \quad [3]^{-1} = 7, \quad [7]^{-1} = [3], \quad [9]^{-1} = [9].$$

Тавре ки аён аст, маҷмӯи $\mathbb{Z}_{10}^*$ аз рӯйи зарб гурӯҳро ташкил медиҳад.

Қайд кардан ба маврид аст, ки дар байни ҳамаи классҳои $[a] \in \mathbb{Z}_m$ танҳо ду синф ба худашон баръакс мебошанд: [1] ва $[p-1] = -[1]$.

Теоремаи 4. Дар ҳалқаи $\mathbb{Z}_m$ танҳо ба таври ягона имконияти тақсим ба синфи $[a] \in \mathbb{Z}_m^*$ мавҷуд аст. Ҳосили тақсими синфи $[a]$ бар синфи [b] аз рӯйи формулаи зерин муайян карда мешавад:

$$[c] = [b] \cdot [a]^{-1}.$$

Мисоли 7. Дар ҳалқаи $\mathbb{Z}_{24}$ ҳосили тақсими синфи [18] бар синфи [7] ёфта шавад.

Ҳал. Азбаски $[7] \in \mathbb{Z}_{24}^*$ аст, бинобар ин $[7]^{-1} = [7]$ мешавад. Аз ин ҷо

$$[18] \cdot [7]^{-1} = [18] \cdot [7] = [6].$$

Теоремаи Эйлерро ба шакли зерин дида мебароем.

Теорема 5. Агар $[a] \in \mathbb{Z}_m^*$ - синфи баргарданда (обратимий) бошад, он гоҳ формулаи зерин ҷой дорад.

$$[a]^{\varphi(m)} = [1].$$

Таърифи 3. Тартиби синфи тафриқҳо $[a] \in \mathbb{Z}_m^*$ гуфта чунин ададӣ хурдтарини δ −ро меноманд, ки барои он баробарии зерин иҷро мешавад:

$$[a]^\delta = [1].$$

Мисоли 8. Тартиби синфи тафриқҳои $[7] \in \mathbb{Z}_{18}^*$ ёфта шавад.

Ҳал. Ҳосил мекунем

$[7]^1 = [7]$, $[7]^2 = [13]$, $[7]^3 = [1]$, аз ин ҷо аён аст, ки δ=3 мешавад.

Теоремаи 6. Бигузор δ тартиби синфи тафриқҳои $[a] \in \mathbb{Z}_m^*$ бошад. Баробарии

$$[a]^k = [1] \qquad (7)$$

фақат ва фақат ҳамон вақт ҷой дорад, агар $k = 0(mod\ \delta)$ шавад.

Исбот. Ададӣ k-ро бо δ тақсими бақиянок карда, ҳосил мекунем:

$$k = \delta q + r, \qquad 0 \le r < \delta.$$

Аз ин ҷо ҳосил мекунем. $[a]^k = ([a]^\delta)^q [a]^r = [a]^r$. Ҳамин тариқ баробарии (7) ба баробарии зерин баробарқувва мебошад.

$$[a]^r = [1].$$

Агар фарз карда шавад, ки $r > 0$ аст, он гоҳ ба таърифи он ки δ ҳамчун ададӣ хурдтарини натуралиест, ки барои он $[a]^\delta = [1]$ мешавад, ба зидият дучор мешавем.

Аз ин теорема натиҷаҳои зерин бар меоянд:

Натиҷаи 1. Тартиби дилхоҳ синфи тафриқҳо аз $\mathbb{Z}_m^*$ тақсимкунандаи $\varphi(m)$ мебошад.

Натиҷаи 2. Баробарии $[a]^k = [a]^r$ ба муқоисаи $k = l(mod\ \delta)$ баробарқувва мебошад.

Натиҷаи 3. Ҳамаи синфи тафриқҳои $[a]^k$, k=0, 1, …, $\delta - 1$, ҷуфт-ҷуфт гуногун мебошанд.

Таърифи 7. Бигузор КТУ(g, m) = 1 бошад. Агар тартиби синфи тафриқҳо $[g] \in \mathbb{Z}_m^*$ ба $\varphi(m)$ баробар бошад, он гоҳ ададди g решаи ибтидоии аз рӯйи модули m номида мешавад.

Мисоли 9. Ададди 3 аз рӯйи модули 4 ва ададди 5 аз рӯйи модули 7 решаи ибтидоӣ мебошад. Аммо аз рӯйи модули 8 решаи ибтидоӣ тамоман мавҷуд нест.

Барномаи ёфтани решаи ибтидоӣ аз рӯйи модули додашуда шакли зеринро дорад:

```
int powmod (int a, int b, int p) {
        int res = 1;
        while (b)
                if (b & 1)
                        res = int (res * 1ll * a % p),  --b;
                else
                a = int (a * 1ll * a % p),  b >>= 1;
        return res;
}
int generator (int p) {
        vector<int> fact;
        int phi = p-1,  n = phi;
        for (int i=2; i*i<=n; ++i)
                if (n % i == 0) {
                        fact.push_back (i);
```

```
                while (n % i == 0)
                        n /= i;
        }
    if (n > 1)
        fact.push_back (n);
    for (int res=2; res<=p; ++res) {
        bool ok = true;
        for (size_t i=0; i<fact.size() && ok; ++i)
    ok &= powmod (res, phi / fact[i], p) != 1;
        if (ok)  return res;
    }
    return -1;
}
```

Дар ин ҷо функсияи powmod() – амали ба дарачабардориро аз рӯйи модул ва функсияи generator – решаи ибтидоиро аз рӯйи модули сода муайян мекунад.

Теоремаи 8 (Гаусс). Агар модули m адади содаи р бошад, он гоҳ решаи ибтидои ҳамавақт вуҷуд дорад.

5. Майдон. Мисолҳои асосӣ

Таърифи 1. Маҷмӯи $(F,\cdot,+)$ бо ду амал, ки дорои хосиятҳои зерин мебошанд, майдон номида мешавад

- $(F,+)$ –гурӯҳи абелӣ бо элементи воҳидии 0;
- $(F\backslash\{0\},\cdot)$ –гурӯҳи абелӣ бо элементи воҳидии 1;
- $(F,\cdot,+)$ –қонуни дистрибутивиро қаноат мекунонад.

Аз ин ҷо чунин хулоса баровардан мумкин аст, ки майдон - ин ҳалқаи комутативиест, ки ҳар як элементи он дорои элементи баръакс мебошад.

Қайд мекунем, ки маҷмӯи элементҳое, ки дар $\mathbb{Z}_m$ дорои элементи баръакс мебошанд, ба таври математикӣ чунин навишта мешаванд:

$$\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | \text{КТУ}(x, N) = 1\}.$$

Мисолҳои стандартии майдон - ин маҷмӯи ададҳои ратсионалӣ, ҳақиқӣ ва комплексӣ мебошанд. Дар ҳолати сода будани m маҷмӯи $\mathbb{Z}_m$ майдони охирнокро ташкил карда, майдони тафриққо аз рӯйи модули р номида мешавад. Чунин майдонро бо рамзи $\mathbb{Z}_p$ ишорат мекунанд.

Илова бар мисолҳои стандартӣ маҷмӯи ададҳои намуди $a + b\sqrt{2}$ ва $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, ки дар ин ҷо ададҳои $a, b, c -$ ададҳои ратсионалӣ мебошанд, низ гурӯҳро ташкил медиҳанд. Системаи алгебравии $\langle B, \oplus, \& \rangle$ бо амалҳои бинории & (конъюнксия) ва $\oplus$ (ҷамъ аз рӯйи модули 2) дар маҷмӯи $B = \{0,1\}$, низ майдонро ташкил мекунанд.

Агар миқдори элементҳои майдон охирнок бошанд, майдонро охирнок меноманд. Миқдори элементҳои майдонро тартиби он меноманд. Ҳалқаи тафриққои: Z_{18}={0, 1, 2, 3 ,4 , 5, …, 17}-ро дида мебароем. Дар ин мисол танҳо барои элементҳои ғайринулие, ки бо модул байнан содаанд (яъне, 1, 5, 7, 11, 13, 17) элементи баръакс мавҷуд аст. Бинобар ин, гурӯҳи мултипликативии $Z_{18}^* = \{1, 5, 7, 11, 13, 17\}$ майдонро ташкил медиҳад. Агар модул ададди содаи p бошад, он гоҳ дилхоҳ элементҳои $1, 2, \ldots, p - 1$ дорои элементи баръакс мебошанд, аз ин рӯ гурӯҳи мултипликативии $Z_p^* = \{1, 2, \ldots, p - 1\}$ майдонро ташкил

медиҳад. Масалан, $Z_5 = \{0, 1, 2, 3, 4\}$ мисоли содаи гурӯҳи охирнок мебошад, ки дорои 5 элемент аст.

Майдони охирнокро майдони Галуа[1] низ меноманд. Аз ин рӯ барои майдони охирноки аз q элемент иборат метавон яке аз ишораҳои F_q ва $GF(q)$-ро истифода кард. Дар ин ҷо GF -"майдони Галуа" хонда мешавад.

Соли 1893 математики амрикоӣ Мур[2] исбот кард, ки ба таври ягона то изоморфизм барои дилхоҳ адади содаи p ва адади мусбати n майдони охирноки аз $q = p^n$ элемент иборат мавҷуд аст.

Таърифи 2. Адади хурдтарини p , ки барои он баробарии $p \cdot 1 = 0$ иҷро мегардад, характеристикаи майдон F_q номида мешавад.

Характеристикаи майдон бо $charF = p$ ишорат карда мешавад. Масалан, майдони $Z_5 = \{0, 1, 2, 3, 4\}$ дорои характеристикаи $p = 5$ мебошад, чунки баробарии $p \cdot 1 \equiv 0$ танҳо ҳангоми $p = 5$ будан иҷро мегардад.

---

[1] Эварист Галуа (фр. Évariste Galois) математики фаронсавӣ асосгузори алгебраи олиии муосир, 25-уми октябри соли 1811 дар шаҳр Бур-ля-Рене (Франсия) ба дунё омада, 31-уми майи соли 1832 дар шаҳри Париж (Франсия) аз дунё чашм пушидааст.

2 Элиаким Гастингс Мур (англ. Eliakim Hastings Moore) –математики амрикоӣ 26-уми январи соли 1862 дар шаҳри Мариетта (Огайо) ба дунё омадааст. Кори нахустини Мур ба асосҳои алгебра ва геометрияи алгебравӣ бахшида шудааст. Ӯ нахустин маротиба соли 1893 теорема оиди класификатсияи майдонҳои охирнокро исбот кард. 30-уми декабри соли 1932 дар Чикаго (ИМА) аз олам чашм пушидааст.

6. Мафҳумҳои асосии назарияи гурӯҳҳо

Таърифи 1. Гурӯҳи G даврӣ номида мешавад, агар дар он чунин элементи g мавҷуд бошад, ки дилхоҳ элементи G −ро ҳамчун дараҷаи он тасвир кардан мукин бошад.

$$\forall x \in G \quad \exists n \in \mathbb{Z}: \ x = g^n.$$

Дар ин ҳолат $G = \langle g \rangle$ навишта, мегӯянд, ки G тавлидшудаи элементи g мебошад ва худи $g-$ ро элементи тавлидкунанда меноманд.

Мисол.

1. $Z_6^+ = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 5 \rangle$.
2. $Z_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle = \langle 5 \rangle$.

Дар ҳақиқат, $Z_9^* = \{1, 2, 4, 5, 7, 8\}$ буда, танҳо барои ин элементҳо элементи баръакс мавҷуд мебошад (мувофиқан, 1, 5, 7 2, 4, 8). Илова бар ин, тафтишҳо нишон медиҳанд, ки $Z_9^* = \{2^0, 2^1, 2^2, 2^3, \ 2^4, 2^5\}$ (ба ёд меорем, ки тартиби элементҳо дар маҷмӯъ шарт намебошад). Ин имкон медиҳад, ки дар байни гурӯҳи Z_6^+ ва Z_9^* аз рӯйи қонуни $i \longmapsto 2^i$ изоморфизм барқарор кард, яъне $Z_6^+ \to Z_9^*$

3. $Z_7^* = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$.

Айнан ҳамин тавр дар байни гурӯҳи Z_6^+ ва Z_7^* аз рӯйи қонуни $i \longmapsto 3^i$ метавон изоморфизм барқарор кард, яъне $Z_6^+ \to Z_7^*$.

4. $Z_8^* = \{1, 3, 5, 7\}$ −даврӣ намебошад.

Таърифи 2. Гурӯҳ охирнок номида мешавад, агар миқдори элементҳои он охирнок бошанд. Миқдори элементҳои гурӯҳро тартиби он меноманд ва бо $|G|$ ё $\#G$ ишорат мекунанд.

Таърифи 3. Тартиби элементи g-и гурӯҳи G гуфта, чунин ададӣ натуралии хурдтарини $n \geq 0$ −ро (дар гурӯҳи G) меноманд, ки барои он баробарии зерин иҷро мешавад:

$$g^n = e. \qquad (1)$$

Ба шарти он, ки чунин n мавҷуд бошад, дар сурати акс тартиби элементи g ба ∞ баробар мешавад. Тартиби g −ро бо $ord(g)$ низ ишорат мекунанд.

Дар (1) e −ро элементи нейтралӣ меноманд, яъне аз рӯйи ҷамъ 0 ва аз рӯйи зарб 1.

Мисолҳо.

1) Гурӯҳи $\mathbb{Z}^+$ − ҳамаи ададҳои бутун аз рӯйи амали ҷамъ даврӣ мебошанд, $\mathbb{Z}^+ = \langle 1 \rangle$ ва $ord(g) = \infty$ барои дилхоҳ аз сифр фарқкунандаи $n \in \mathbb{Z}$.
2) Тартиби элементҳои гурӯҳҳои Z_6^+, Z_9^* ва Z_8^* мувофиқан чунин мебошад:

G	0	1	2	3	4	5
ord(g)	1	6	3	2	3	6

G	1	2	4	5	7	8
ord(g)	1	6	3	6	3	2

g	1	3	5	7
ord(g)	1	2	2	2

5. Тасдиқотҳои асосӣ оиди тартиби элементҳои гурӯҳ.

1) Агар $g \in G$ бошад, он гоҳ баробарии (1) фақат ва фақат ҳамон вақт иҷро мешавад, ки агар n ба $ord(g)$ тақсим шавад.
2) Агар G гурӯҳи абелӣ буда, $a, b \in G$ −элементҳои тартибашон байнан сода бошанд, он гоҳ $ord(ab) = ord(a)ord(b)$ мешавад.
3) Агар $G = \langle g \rangle$ гурӯҳи охирноки даврӣ бошад, он гоҳ $G = \{e, g, g^2, \dots, g^{ord(g)-1}\}$ буда, ҳамаи элементҳои овардашуда гуногун мебошанд.

Исбот.

1) Агар n ба $ord(g)$ тақсим шавад, он гоҳ $g^n = (g^{ord(g)})^{\frac{n}{ord(g)}} = e$ мешавад. Баръакс, агар баробарии (1) ҷой дошта бошад, n-ро ба $ord(g)$ тақсими бақиянок карда, ҳосил мекунем: $n = k \cdot ord(g) + r$ $(0 \le r < ord(g))$. Аз ин ҷо $g^n = e = (g^{ord(g)})^k g^r = g^r$ мешавад. Барои ба хосияти элементи минималӣ будани $ord(g)$ зидият нашудан, зарур аст, ки $r = 0$ шавад. Ҳамин тариқ, n ба $ord(g)$ тақсим мешавад.
2) Ишораҳои $k = ord(ab), n = ord(a),\ m = ord(b)$ −ро дохил карда бо назардошти абелӣ будани гурӯҳи G ҳосил мекунем:

$$e = (ab)^{km} = a^{km}(b^m)^k = a^{km}.$$

Бо назардошти банди якуми тасдиқот km ба n тақсим мешавад. Азбаски n ва m байнан сода мебошанд, k ба n низ тақсим мешавад. Ба ҳамин

монанд k ба m низ тақсим мешавад, яъне ба $n \cdot m$ тақсим мешавад. Аз дигар тараф, аён аст, ки $(ab)^{nm} = e$ аст. Азбаски, k ин адади минималӣ аз рӯйи хосияти $(ab)^k = e$ мебошад, пас, $k = mn$ мешавад.

3) Ҳамаи элеметҳои овардашуда гуногун мебошанд. Дар ҳақиқат, агар ҳангоми $0 \leq i < j \leq ord(g) - 1$ будан $g^i = g^j$ бошад, пас, баробарии $g^{j-i} = e$ иҷро мешавад, ки ба хосияти минималностӣ ord(g) зид мебошад. Акнун нишон медиҳем, ки элементи дилхоҳӣ $x \in G$ дар маҷмӯи мазкур мехобад. Барои ягон $n \in G$ ҳосил мекунем $x = g^n$. Ададӣ n-ро ба ord(g) тақсими бақиянок карда ҳосил мекунем $n = k \cdot ord(g) + r\ (0 \leq r < ord(g))$. Ҳамин тариқ $x = (g^{ord(g)})^k g^r = g^r$ мешавад.

Таърифи 4. Зермаҷмӯи H −и гурӯҳи G зергурӯҳи ин гурӯҳ номида мешавад, агар H нисбат ба амалҳои гурӯҳи G худаш гурӯҳ бошад.

Теорема 1. Зермаҷмӯи H −и гурӯҳи G фақат ва фақат ҳамон вақт зергурӯҳи G мешавад, агар баробариҳои зерин иҷро гарданд:

1) $a, b \in H => a \cdot b \in H$;
2) $a \in H => a^{-1} \in H$.

Мисол. Ҳамаи зергурӯҳҳои гурӯҳи Z_6^+ ин $\{0\}, \{0, 3\}, \{0, 2, 4\}$ ва худи гурӯҳӣ Z_6^+ мебошанд.

Яке аз теоремаҳои муҳими назарияи гурӯҳро бе исбот меорем.

Теоремаи Лагранҷ[1]**.** Тартиби зергурӯҳҳои гурӯҳи охирнок тартиби ин гурӯҳро тақсим мекунад.

Саволҳо барои мустаҳкамкунӣ

1) Чӣ гуна амалро амали бинарӣ мегуянд?
2) Кадом амалҳои бинориро медонед?
3) Чӣ гуна маҷмӯъ гурӯҳ номида мешавад?
4) Синфи тафриқҳо бо гӯрӯҳ чӣ алоқамандӣ дорад?
5) Ҳалқа гуфта чиро меноманд?
6) Майдон чист?
7) Кадом мисолҳои гурӯҳ, ҳалқа ва майдонро медонед?
8) Тақсимкунандаи сифр гуфта, чиро дар назар доранд?
9) Зергурӯҳи гурӯҳ чист?

[1] Ҷозеф Луи Лагранҷ (фр. *Joseph Louis Lagrange*, итал. *Giuseppe Lodovico Lagrangia*; 25 января 1736, Турин (Италия)— 10 апреля 1813, Париж) — математик, астрономи ва механики фаронсавӣ зодаи Итолиё мебошад.

Боби 5. Логарифмирониии дискретӣ ва масъалаи факторизатсия

1. Теоремаи чинӣ оиди бақияҳо

Теоремаи чинӣ оиди бақияҳо (ТЧБ) яке аз теоремаҳои қадимаи математика ба ҳисоб меравад, ки тақрибан таърихи 2000-сола дорад. Дар оянда аз теоремаи ТЧБ чандин маротиба истифода бурда мешавад, масалан барои беҳтаркунии ҷараёни рамзкушоӣ дар алгоритми RSA ва дигар протоколҳо. ТЧБ тасдиқ мекунад, ки системаи муодилаҳои

$$\begin{cases} x = a(mod\ N), \\ x = b(mod\ M). \end{cases}$$

аз рӯйи модули $N \cdot M$ фақат ва фақат ҳамон вақт решаи ягона дорад, агар КТУ$(N, M) = 1$ бошад.

Мисоли 1. Системаҳои муодилаҳои

$$\begin{cases} x = 4(mod\ 7), \\ x = 3(mod\ 5). \end{cases}$$

дорои решаи $x_0 = 18$ мебошад. Бе душворӣ дурустии ин ҳалро санҷидан мумкин аст, зеро 18 (mod 7)=4 ва 18 (mod 5)=3 мебошад.

Акнун тарзи ёфтани ин ҳалро дида мебароем. Ибтидо тарзи ёфтани ҳалро ба шакли схематикӣ дида мебароем. Агар x ҳарду муодилаи системаро қаноат кунонад, он гоҳ чунин адади бутуни u ёфт мешавад, ки барои он баробариҳои зерин иҷро мегарданд:

$$\begin{cases} x = 4 + 7u, \\ x = 3(mod\ 5). \end{cases}$$

Аз муодилаи якуми ин система қимати ёфташудаи $x-$ ро ба муодилаи дуюми система гузошта ҳосил мекунем.

$$4 + 7u = 3\ (mod\ 5)$$

Баробарии охирон табдил дода ба шакли зерин меорем:

$$2u = 7u = 3 - 4 = 4\ (mod\ 5)$$

Азбаски КТУ(2,5) = КТУ(7,5) = 1 аст, пас метавон муодилаи охиронро нисбат ба u ҳал кард. Пеш аз ҳама аз рӯйи модули 5 барои ададӣ 2 ададӣ (элементи) баръаксро меёбем. Ададӣ мавриди назар ба 3 баробар аст, чунки $2 \cdot 3 = 6 = 1(mod\ 5)$ мешавад. Пас қимати ифодаи зеринро ҳисоб мекунем:

$$u = 2^{-1} \cdot 4(mod\ 5) = 3 \cdot 4(mod\ 5) = 2(mod\ 5).$$

Қимати ёфташудаи u-ро ба ифодаи $x = 4 + 7u$ гузошта ҳосил мекунем:

$$x = 4 + 7u = 4 + 7 \cdot 2 = 18.$$

гузошта ҳосил мекунем.

Системаи ду муодила аз нуқтаи назари амалӣ хеле ҷолиб мебошанд, бинобар ин, ибтидо алгоритми ҳалли онҳоро меорем. Бигузор ададҳои N ва M байнан сода буда, системаи муодилаҳои зерин дода шуда бошанд.

$$\begin{cases} x = a(mod\ N), \\ x = b(mod\ M). \end{cases} \qquad (1)$$

Алгоритми ҳалли системаи (1) чунин шаклро дорад:

1) Ҳисобкунии қимати $T = M^{-1}\ (mod\ N)$. (Бо назардошти байнан сода будани N ва M ҳисобкунии қимати T ҳамавақт имкон дорад).
2) Ҳисобкунии қимати $u = (b - a)T\ (mod\ N)$.

3) Аз рӯй модули $N \cdot M$ ҳал шакли зеринро мегирад:

$$x = a + uM.$$

Барои бовари ҳосил кардан ба дурустии ҳалли ёфташуда санҷиш мегузаронем.

$x(mod\ M) = a + uM(mod\ M) = a,$

$$x(mod\ N) = a + uM\ (mod\ N) = a + (b - a)TM(mod\ N)$$
$$== a + (b - a)M^{-1}M(mod\ N) = b.$$

Акнун ҳолати умумии ТЧБ-ро мавриди баҳс қарор медиҳем. Бигузор $m_1, m_2, \dots, m_r$ ва $a_1, a_2, \dots, a_r$ ададҳои бутуни байнан ҷуфт-ҷуфт сода бошанд. Талаб карда мешавад, ки чунин элементи x аз рӯйи модули $M = m_1, m_2, \dots, m_r$ барои системаи муодилаҳои зерин ёфта шавад:

$x = a_i\ (mod\ m_i)$ барои ҳамаи $i -$ ҳо.

ТЧБ мавҷудият ва ягонагии ҳалро кафолат дода, чунин натиҷа медиҳад:

$$x = \sum_{i=1}^{r} a_i M_i y_i (mod\ M), \qquad (2)$$

дар ин ҷо $M_i = \frac{M}{m_i}$, $y_i = M_i^{-1}(mod\ m_i)$ мебошад.

Мисоли 2. аз рӯйи модули $M = 1001 = 7 \cdot 11 \cdot 13$, ҳалли системаи зерин ёфта шавад:

$$\begin{cases} x = 5(mod\ 7), \\ x = 3(mod\ 11), \\ x = 10(mod\ 13). \end{cases}$$

Ибтидо қимати M_i ва y_i –ҳои дар формулаи (2) истифодашударо ҳисоб мекунем.

$M_1 = 143,$ $y_1 = 5,$

$M_2 = 91,$ $y_2 = 4,$

$$M_3 = 77, \qquad y_3 = 12.$$

Пас аз ёфтани M_i ва y_i −ҳо бо истифода аз формулаи (2) ҳосил мекунем.

$$x = \sum_{i=1}^{3} a_i M_i y_i (mod\ M)$$

$$= 715 \cdot 5 + 364 \cdot 3 + 924 \cdot 10 (mod\ 1001) = 894.$$

Инак, натиҷа $x = 894$ мешавад.

2. Алгоритми Горнер (The Garner' algorithm)

Барои ҳалли системаи муқоисаҳо метавон аз алгоритми Горнер[1] низ истифода кард. Мувофиқи алгоритми мазкур x ҳамчун аъзои n-уми пайдарпайии $\{x_i\}$ ҳисоб карда мешавад. Пайдарпайиҳои $\{x_i\}$ ва $\{y_i\}$ аз рӯйи формулаи зерин сохта мешаванд:

$$\begin{cases} y_i = x_1 = r_1, \\ y_{i+1} = \frac{r_{i+1} - x_i}{m_1 \cdot m_2 \cdot \ldots \cdot m_i} \ mod\ m_{i+1}, \\ x_{i+1} = x_i + y_{i+1} \cdot m_1 \cdot m_2 \cdot \ldots \cdot m_i. \end{cases}$$

Бартарии ин алгоритм дар он аст, ки барои ҳисобкунии аъзоҳои ояндаи (x_{i+1}, y_{i+1}) танҳо як қимати пешинаи (x_i, y_i) истифода бурда мешавад.

Мисол. Қимати хурдтарини x, ки муодилаи зеринро қаноат мекунонад ёфта шавад:

[1] Вилям Ҷорҷ Горнер (англ. William George Horner) математики англис соли 1786 дар шаҳри Бристол (Англия) ба дунё омадааст. 22-юми сентябри соли 1837 дар шаҳри Бат (Англия) аз дунё чашм пушидааст.

$$\begin{cases} x \equiv 2(mod\ 3), \\ x \equiv 5(mod\ 7), \\ x \equiv 4(mod\ 11). \end{cases}$$

Ҳал. Дар системаи додашуда, $m_1 = 3,\ m_2 = 7, m_3 = 11,\ r_1 = 2, r_2 = 5, r_3 = 4$ аст. Акнун қимати пайдарпайиҳои y_i ва $x_i (i = 1,2,3)$ −ро ҳисоб мекунем:

$$y_1 = x_1 = 2,$$
$$y_2 = (r_2 - x_1) \cdot (m_1)^{-1}\ mod\ m_2 = (5-2) \cdot 3^{-1} mod\ 7 = 1,$$
$$x_2 = x_1 + (y_2 \cdot m_1 mod\ m_2) = 2 + (1 \cdot 3\ mod\ 7) = 5,$$
$$y_3 = (r_3 - x_2) \cdot (m_1 \cdot m_2)^{-1}\ mod\ m_3 = (4-5) \cdot 21^{-1} mod\ 11 = 1,$$
$$x_2 = x_2 + (y_3 \cdot m_1 \cdot\ m_2) = 5 + 1 \cdot 3 \cdot 7 = 26.$$

Ҷавоб: $x = x_2 = 26$.

3. Логарифмирониидискретӣ

Дар майдони охирноки F_q барои ададҳои ихтиёрии $a, b \in F_q$ логарифми дискретӣ аз рӯйи асоси a гуфта, чунин ададиn-ро меноманд, ки барои он баробарии зерин иҷро гардад:

$$a^n = b \text{ (дар майдони } F_q) \qquad (1)$$

Масъалаи ҳисобкунии логарифми дискретии ададҳои додашудаи a, b, p − ро дар майдони охирнок масъалаи логарифмиронии дискретӣ меноманд.

Бо суханҳои дигар барои g ва a −и додашуда ҳали x −и муодилаи $g^x = a$ логарифми дискретии[1] элементи a аз рӯйи асоси g номида мешавад. Дар ҳолати гурӯҳи

[1] https://en.wikipedia.org/wiki/Discrete_logarithm

мултипликативии ҳалқаи тафриқҳо аз рӯйи модули m будани G ҳал инчунин индекси адади a аз рӯйи асоси g номида мешавад. Агар g решаи ибтидои аз рӯйи модули m бошад, он гоҳ мавҷудияти индекси адади a аз рӯйи асоси g кафолат дода мешавад.

Бигузор p адади содаи тоқ буда, a ташкилкунандаи гурӯҳи Z_p^* (ҳамин тариқ $ord(a) = p - 1$) ва b адади ба p тақсимнашаванда бошад, он гоҳ ёфтани чунин аади n – ро, ки баробарии зеринро қаноат мекунонад логарифмирониидискретӣ меноманд.

$$a^n \equiv b(mod\ p). \qquad (2)$$

Дар ин ҳолат $n = log_a b$ навишта мешавад. Ҳоло алгоритмеро дида мебароем, ки дар сурати суфта (гладкий) будани адади p, (яъне ҳангоме, ки адади $p - 1$ ба зарбкунандаҳои хурд тақсим шавад) хело тез кор мекунад.

Барои ёфтани b ҳангоми маълум будани a,n,p метавон зербарномаи (методи) modInverse()дар класси BigInteger ҷойгир аст, истифода кард. Тарзи истифодаи ин зербарнома чунин аст:

```
BigInteger S=BigInteger.modPow(BigInteger exponent,
BigInteger m)
```

Мисол.

```
import java.math.BigInteger;
import java.util.Scanner;
public class modPow{
public static void main(String[] args) {
    BigInteger a,n,p,b;
    Scanner sc=new Scanner(System.in);
```

```
        a=sc.nextBigInteger();
        n=sc.nextBigInteger();
        p=sc.nextBigInteger();
        b=a.modPow(n, p);
        System.out.println(S);
    }
}
```

Дар сурати акс, ҳангоми маълум будани a, b, p барои ёфтани n метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард.

```
#include <iostream>
#include <cmath>
#include <map>
using namespace std;
int solve (int a, int b, int m) {
        int n = (int) sqrt (m + .0) + 1;
        int an = 1;
        for (int i=0; i<n; ++i)
                an = (an * a) % m;
        map<int,int> vals;
        for (int i=1, cur=an; i<=n; ++i) {
                if (!vals.count(cur))
                        vals[cur] = i;
                cur = (cur * an) % m;
        }
        for (int i=0, cur=b; i<=n; ++i) {
                if (vals.count(cur)) {
                        int ans = vals[cur] * n - i;
```

```
                    if (ans < m)
                        return ans;
                }
                cur = (cur * a) % m;
            }
            return -1;
}
int main(int argc, char** argv) {
  cout<<solve(20,7,23);
 return 0;
}
```

Қайд. *Дар назарияи ададҳо адади суфта гуфта, чунин адади бутунро меноманд, ки ҳамаи тақсимкунандаҳои содаи он хурд бошанд.*

Ададии натуралӣ B-суфта номида мешавад, агар тақсимкунандаҳои он аз B калон набошанд.

Масалан, ададии 2000 бо чунин шакл $2^4 \times 5^3$ ба зарбкунандаҳои сода ҷудо карда мешавад, аз ин ҷо 2000 — ин ададии 5-суфта, инчунин 6-суфта мебошад, ва ғайра, аммо 4-суфта намебошад.

Алгоритми LOGSmooth. Бигузор q – ададии содаи тақсимкунандаи $p-1$ бошад. Он гоҳ маҷмӯи ҳалҳои муодилаи $x^q = 1$ (дар майдони F_p) аз элементҳои $1, c, c^2$, …, c^{q-1} иборат мебошанд, ки дар ин ҷо $c \equiv a^{\frac{p-1}{q}} \ (mod\ p)$ аст. Агар d чунин ададии додашудаи муодилаи $x^q = 1$ –ро қаноат кунонанда бошад, пас тавассути методи азназаргузаронӣ (перебор) метавон чунин ададии t- ро ёфт,

ки барои он $d = c^t$ $(0 \le t \le q-1)$ шавад. Дар ин ҷо беохир хурд будани q фарз карда мешавад.

Бигузор $p-1 = q^k l$ бошад (дар ин ҷо l ва d байнан сода мебошанд), он гоҳ пай дар пай чунин ададҳои $u_i (i = 0, 1, \dots, k)$ −ро меёбем, ки барои онҳо баробарии зерин иҷро шавад:

$$(ba^{-u_i})^{lq^{k-i}} \equiv 1 \ (mod\ p). \qquad (3)$$

Ҳангоми $i = k$ будан муқоисаи зеринро ҳосил мекунем:

$$(ba^{-u_k})^l \equiv 1 \ (mod\ p).$$

Бо назардошти (2) муқоисаи ҳосилшуда ба муқоисаи зерин баробарқуввa мебошад:

$$a^{(n-u_k)l} \equiv 1 \ (mod\ p).$$

Азбаски $ord(a) = p-1$ аст, он гоҳ муқоисаи охирон маънои онро дорад, ки $(n-u_k)l$ ба $p-1$ тақсим мешавад, яъне

$$n \equiv u_k (mod\ q^k).$$

Барои ҳамаи тақсимкунандаҳои содаи q–и адади $p-1$ чунин муқоисаҳоро навишта, баъдан тавассути ТЧБ қимати $n (mod\ p-1)$ −ро ҳисоб мекунем.

Акнун тарзи ёфтани ададҳои u_i −ро, ки муқоисаи (3)-ро қаноат мекунонад, дида мебароем. Метавон $u_0 = 1$ гузошт. Агар ягонто $u_i -$ҳо аллакай маълум бошанд, он гоҳ аз (3) бармеояд, ки $(ba^{-u_i})^{lq^{k-i-1}}$ муодилаи $x^q \equiv 1 (mod\ p) -$ро қаноат мекунонад. Акнун метавон чунин t −ро ёфт, ки барои он баробарии зерин иҷро гардад:

$$(ba^{-u_i})^{lq^{k-i-1}} \equiv c^t (mod\ p).$$

Гузориши $u_{i+1} = u_i + tq^i$ – ро дохил мекунем. Пас баробарии зерин иҷро мегардад, ки ҳангоми $i + 1$ будан маънои иҷроиши баробарии (3)-ро дорад:

$$(ba^{-u_{i+1}})^{lq^{k-i-1}} \equiv c^t a^{-tlq^{k-1}} \equiv 1(mod\ p).$$

Ҳамин тариқ аз рӯйи схемаи зерин u_k –ҳо ёфта мешаванд:

$$u_0 = 1, \quad r_i = (ba^{-u_i})^{lq^{k-i-1}}\ (mod\ p), t_i = log_c r_i,\ u_{i+1} = u_i + t_i q^i.$$

Мисол. Чунин n -ро меёбем, ки муқоисаи $2^n \equiv 74(mod\ 163)$ –ро қаноат кунонад.

Ҳал. Дар ин ҷо $a = 2, b = 74,\ p = 163$ ва $p - 1 = 2 \cdot 3^4$ мебошад. Ибтидо $q = 3$ мегузорем, он гоҳ $k = 4$ ва $l = 2$ мешавад. Илова бар ин, $c \equiv 2^{\frac{p-1}{3}} = 2^{54} \equiv 104(mod\ 163)$, $c^2 \equiv 58(mod\ 163)$ мебошад. Акнун ҷадвали зеринро пур мекунем:

i	0	1	2	3
r_i	1	58	1	104
t_i	0	2	0	1
u_{i+1}	1	7	7	34

Аз ин ҷо ҳосил мекунем:

$$n \equiv 34\ (mod\ 81). \qquad (4)$$

Акнун $q = 2$ мегузорем. Он гоҳ $k = 1$ ва $l = 81$ ва $c \equiv 2^{\frac{p-1}{2}} \equiv -1(mod\ 163)$ буда, ҷадвали зеринро пур мекунем:

i	0
r_i	-1
t_i	1
u_{i+1}	2

Аз ин ҷо ҳосил мекунем:

$$n \equiv 2 \ (mod\ 2). \qquad (5)$$

Аз (4) ва (5) бармеояд, ки $n \equiv 34 \ (mod\ 81)$ аст.

4. Масъалаи факторизатсия. Методи Ферма

Яке аз масъалаи асосӣ дар назарияи криптография бо калидҳои кушода масъалаи факторизатсия ба ҳисоб меравад. Ҳоло масъалаи мазкурро мавриди баҳс қарор медиҳем.

Бигузор ададиn ки ҳосили зарби ду адади содаи p ва q −ро ифода мекунад, ададиn тоқ бошад. Ҳангоми дода шудани n барои ёфтани зарбшавандаҳои p ва q метавон аз методи Ферма истифода кард. Чунин масъаларо (яъне аз рӯйи n муайянкунии p ва q) − масъалаи факторизатсия меноманд. Моҳияти методи Ферма - ин ёфтани чунин ададҳои A ва B аст, ки барои онҳо баробарии зерин иҷро мегардад:

$$n = A^2 - B^2.$$

Методи Фермаро метавон ба намуди алгоритмӣ чунин навишт:

1) Қисми бутуни решаи квадрати аз ададиn ҳисоб карда мешавад:

$$m = \left[\sqrt{n}\right].$$

2) Барои $x_i = m + i \ (i = 0,1,2, \dots)$ қимати функсияи зеринро

$$q(x_i) = x_i^2 - n,$$

то замоне, ки $q(x_i)$ ба квадрати пурра баробар шудан, ҳисоб мекунем.

3) Бигузор $q(x_i)$ квадрати пураи ягон адад, масалан B-ро ифода кунад, яъне $q(x_i) = B^2$, он гоҳ чунин адади $A = x_i -$ро муайян карда, аз баробарии $A^2 - n = B^2$ қимати $n = (A^2 - B^2) = (A - B)(A + B) -$ро ва аз ин ҷо қимати p ва q муайян карда мешаванд: $p = A + B$, $q = (A - B)$.

Мисол. Адади $n = 19\,691 -$ро факторизатсия мекунем. Ибтидо қимати $m = [\sqrt{n}] = 141 -$ро ҳисоб мекунем. Ҷараёни ҳисобкунии тақсимкунандаҳои n-ро бошад, ба намуди ҷадвал менависем:

x	$q(x)$	$\sqrt{q(x)}$
141	190	13,78
142	473	21,75
143	758	27,53
144	1045	32,33
145	1334	36,52
146	1625	40,31
147	1918	43,79
148	2213	47,04
149	2510	50,10
150	2809	53

Аз катакчаи охирони сутуни сеюми ҷадвал ҳосил мекунем: $(140 + 10)^2 - n = 53^2$, аз ин ҷо $n = 150^2 - 53^2 = 203 \cdot 97$ мешавад. Ҳамин тариқ, ҳосил мекунем: $19691 = 203 \cdot 97$, яъне $p = 203$ ва $q = 97$. Тавре, ки аз ҷадвал маълум аст, дар ин ҷо барои ёфтани қиматҳо 10 итератсия, як амали ба дараҷабардорӣ, як амали тарҳ ва як амали аз

решаи квадратӣ баровардан истифода шудааст, яъне миқдори доимии амалҳо иҷро гардидааст.

5. Қимати функсияи Эйлер $\varphi(N)$ ва масъалаи факторизатсия

Барои аз рӯйи n ($n = p \cdot q$) ёфтани қиматҳои p ва q (яъне масъалаи факторизатсия метавон) аз усули дигар низ истифода кард. Ин усулро бо исботи тасдиқоти зерин меорем.

Лемма. Қимати функсияи Эйлер $\Phi = \varphi(N)$ имконияти ба зарбкунандаҳои сода ҷудо намудани адади N-ро фароҳам меорад.

Исбот. Ҳосил мекунем

$$\Phi = \varphi(N) = (p-1) \cdot (q-1) = N - (p+q) + 1.$$

Аз ин ҷо $S = N + 1 - \Phi$ гузошта ҳосил мекунем:

$$S = p + q.$$

Мақсади мо ёфтани p ва q мебошад, ки суммаи онҳо S ва ҳосили зарбашон ба N баробар аст. Бисёраъзогии зеринро дида мебароем:

$$f(X) = (X-p) \cdot (X-q) = X^2 - SX + N.$$

Муодилаи $f(X) = 0$ –ро ҳал карда метавон p ва q-ро ба даст оварад.

$$p = \frac{S+\sqrt{S^2-4N}}{2}, \quad q = \frac{S-\sqrt{S^2-4N}}{2}.$$

Ба сифати мисол модули кушодаи $N = 18923$ –ро дида мебароем: Фарз мекунем, ки $\Phi = \varphi(N) = 18648$ мебошад. Ҳисоб мекунем.

$$S = p + q = N + 1 - \Phi = 276.$$

Бисёраъзогии мувофиқи он шакли зеринро мегирад:

$$f(X) = X^2 - SX + N = X^2 - 276X + 18923.$$

Решаҳои ин бисёраъзогӣ: $p = 149, q = 127$ мешаванд.

6. Ҳисобкунии решаи квадратӣ дар майдонҳои охирнок

Майдони охирноки $GF(p)$ ва ададиҳои $a-$ро, ки тафриқи квадратӣ аз рӯйи модули p аст, дида мебароем. Талаб карда мешавад, ки чунин x –ро ёбед, ки баробарии зеринро қаноат кунонад.

$$a = x^2 (mod\ p)$$

Ададиҳои $(p-1)$ –ро ба шакли $2^r \cdot s$ (дар ин ҷо s–ададиҳои тоқ аст) тасвир мекунем. Аён аст, ки $p-1$ ададиҳои тоқ аст, пас $r \geq 1$ мешавад. Бигузор z ягон тафриқи ғайриквадратӣ аз рӯйи модули p бошад (яъне нишонаи Лежандри он $\left(\frac{z}{p}\right)$ аз -1 фарқ кунад).

Ду ҳолатро дида мебароем:

1) $p \equiv 3(mod\ 4)$. Дар ин ҳолат метавон дар ҳол ҳалро пайдо кард.

$$x = a^{\frac{p+1}{4}} (mod\ p)$$

2) $p \equiv 1(mod\ 4)$.

Ибтидо қимати $y = z^s\ (mod\ p)$ –ро ҳисоб мекунем. Азбаски тартиби дилхоҳ элемент тақсимкунандаи ададиҳои $2^r \cdot s$ мебошад, бинобар ин, тартиби y низ тақсимкунандаи 2^r аст, аз ин ҷо $y^{2^r} \equiv 1(mod\ p)$ мешавад. Инчунин метавон нишон дод, ки $y^{2^{r-1}} \equiv -1(mod\ p)$ аст, яъне тартиби

элементи y дақиқан ба 2^r баробар аст. Акнун элементҳои зеринро ҳисоб мекунем:

$$\lambda_0 = a^s (mod\ p), \quad \omega_0 = a^{\frac{s+1}{2}} (mod\ p) \qquad (1)$$

Бе душворӣ пай бурдан мумкин аст, ки баробариҳои зерин ҷой доранд:

$$\omega_0^2 \equiv a \cdot \lambda_0\ (mod\ p) \ \text{ ва } \ x^2 \equiv a(mod\ p) \to x^{2s} \equiv a^s = \lambda_0\ (mod\ p) \quad (2)$$

Азбаски тартиби элементи x^s тақсимкунандаи 2^r мебошад, пас тартиби λ_0 низ тақсимкунандаи 2^r аст. Ғояи методи Шенкс-Тоннел аз сохтани ҷуфти пайдарпайиҳои (λ_i, ω_i) иборат аст, ки шарти зеринро қаноат мекунонанд:

$$\omega_i^2 \equiv a \cdot \lambda_i (mod\ p), i = 0,1,2, \ldots \qquad (3)$$

Ба ғайр аз ин (зимнан) тартиби λ_{i+1} тақсимкунанди хоси λ_i то замоне, ки тартиби λ_i –и навбатӣ ба сифр баробар нашудан, мебошад. Дар он сурат барои i –и ёфташуда шартҳои $\lambda_i = 1$ ва $\omega_0^2 \equiv a\ (mod\ p)$ иҷро мегарданд. Аз ин ҷо $x = \omega_i -$ решаи ҷустуҷӯшаванда ба ҳисоб меравад.

Азбаски қимати ибтидоии (λ_0, ω_0) бо назардошти шарти (2) баробарии (3)-ро қаноат мекунонад, аллакай маълуманд, пас формулаи умумии муайянкунии қиматҳои $(\lambda_{i+1}, \omega_{i+1})$ –ро менависем:

$$\lambda_{i+1} = \lambda_i \cdot y^{2^{r-m}}, \quad \omega_{i+1} = \omega_i \cdot y^{2^{r-m-1}}, \qquad (4)$$

дар ин ҷо 2^m–тартиби элементи λ_i мебошад

Мисол. Дар майдони $GF(p)$ ҳангоми $p = 41$ будан решаи квадратӣ аз адади $a = 2$ ёфта шавад.

1) Ҳосил мекунем: $p-1=40=2^3\cdot 5$, аз ин ҷо $s=5$ ва $r=3$ мешавад.
2) Аз рӯӣ формулаи (1) қиматҳои ибтидоии (λ_0,ω_0) −ро ҳисоб мекунем:
$$\lambda_0=a^s(mod\ p)=2^5\ (mod\ 41)=32,$$
$$\omega_0=a^{\frac{s+1}{2}}(mod\ p)=2^3(mod\ 41)=8.$$
3) Тартиби элементи λ_0 −ро меёбем:
$\lambda_0^2\ (mod\ p)=32^2\ mod\ 41=40\equiv -1(mod\ 41)$, $\lambda_0^4\equiv 1\ (mod\ p)$.
Аз ин ҷо $ord(\lambda_0)=2^m=4$ буда, қимати $m=2$ мешавад.
4) Тафриқи ғайриквадратиро меёбем. Ҳангоми $z=3$ будан нишонаи Лежандро ҳисоб мекунем:
$$\left(\frac{z}{p}\right)=\left(\frac{3}{41}\right)=\left(\frac{41\ mod\ 3}{3}\right)(-1)^{\frac{(41-1)\cdot(3-1)}{2}}=\left(\frac{2}{3}\right)=-1.$$
Аз ин ҷо аён аст, ки $z=3$ тафриқи ғайриквадратӣ буда, метавонад барои ҳисобкунии ҷуфти $(\lambda_{i+1},\omega_{i+1})$ истифода шавад.
5) Қимати у-ро ҳисоб мекунем. $y=z^s(mod\ p)=3^5(mod\ p)=38$.
6) Дарачаеро, ки бояд $y-$ро бо m бардорем муайян мекунем:
$$d=2^{r-m}=2^{3-2}=2,\ \ y^d=3^2=9.$$
7) Ҳисоб мекунем:
$$\lambda_1=\lambda_0\cdot y^d(mod\ p)=32\cdot 9(mod\ 41)=1,$$
$$\omega_1=\omega_0\cdot y^{d-1}(mod\ p)=8\cdot 3(mod\ 41)=24.$$
Азбаски λ_i–и навбатӣ ба 1 баробар шуд, пас амали ҷустуҷӯи реша ба охир мерасад, яъне решаи матлуб

$x = \omega_1 = 24$ мебошад. Дурустии решаи ёфташударо тафтиш мекунем:

$$x^2 \; mod \; p = 24^2 (mod \; 41) = 2 = a.$$

Саволҳо барои мустаҳкамкунӣ

1) Моҳияти асосии ТЧБ аз чӣ иборат аст?
2) Моҳияти методи Горнер аз чӣ иборат аст?
3) Чӣ тавр метавон тавассути схемаи Горнер системаи муқоисаҳои тартиби се ё чорро ҳал кард?
4) Масъалаи факторизатсия чӣ гуна масъала мебошад?
5) Моҳияти методи Ферма аз чӣ иборат аст?
6) Тавассути қимати функсияи Эйлер чӣ тавр масъалаи факторизатсия ҳал карда мешавад?
7) Чӣ тавр решаи квадрати аз рӯйи модули додашуда ёфта мешавад?

ФАСЛИ 2. МЕТОДҲОИ КЛАССИКИИ РАМЗГУЗОРӢ

Боби 6.Марҳалаҳои ибтидоии рамзгузорӣ

1. Назардошт умуми оиди рамзгузорӣ

Чӣ тавр метавон итилооти муҳимро ба шахси (канали) лозими тавре равон кард, ки дигарон аз сирри он огоҳ нагарданд? Ҳар як инсон дар ҳар давру замон бо мақсадҳои гуногун кӯшиш мекунад, ки ин масъалаи татбиқиро барои худ ҳал кунад. Инсоният аз рӯзи пайдоиши хат бо барои ҳалли масъалаи мазкур методҳои зиёдеро эҷод кардааст. Умуман се усули маъмули ҳалли ин масъала вуҷуд дорад:

1) Сохтани канали алоқаи боваринок (муътабар) байни муштариён ба сурате, ки барои дигарон дастнорас бошад;
2) Истифодаи канали алоқаи умумӣ, вале ба таври махфиёни равон кардани итилоот;
3) Истифодаи канали алоқаи умумӣ, вале равон кардани итилооти лозимӣ тавассути он ба сурате, ки танҳо қабулкунандаи асосӣ онро барои хондан барқарор карда тавонаду халос.

Дар замони ҳозира техника ва технология дар ҳолату рушду ғустариш аст, сохтани канали алоқаи бовариноке, ки тавассути он чандин маротиба равон кардани итилооти ҳаҷмаш зиёд ба таври амн имкон дошта бошад, номумкин аст. Коркарди воситаҳо ва методҳои махфисозии тарзи (далели) равон кардани итилоотро стенография меомузад. Мафҳуми стенография (аз ду калимаи юнонии στενός «маҳдуд» (узкое, тесний) ва γράφειν «мактуб») – гирифта шуда, усули навиштест, ки ба мақсади кӯтоҳнависии нутқи ғуфтугӯӣ аз аломатҳои махсус истифода мебарад. Методҳои стенографӣ таърихи тулонӣ доранд. Масалан, аз замонҳои қадим чунин усули стенографии равон кардани итилоот маъмул буд: Дар аввал сари ғуломонро тарошида, пайғоми лозимиро дар он менавиштанд. Пас аз баромадани мӯи сар ғуломро ба адреси лозими равон мекарданд.

Коркарди методҳои табдилдиҳии (рамзгузорӣ ё шифрования) итилоот, бо мақсади ҳимоя аз истифодабарандагони ғайриқонуниро - криптография меомӯзад.

Криптография (аз юнонӣ: κρυπτός — пӯшида ва γράφω — менависам) — илмест, ки методҳои кофидентсиалӣ (номумкин будани хондани маълумот барои одамони бегона), якпорчагии итилоот (ғайриимкон гардонидани ноаён иваз кунии итилоот), аутентификатсия (тафтиши соҳибияти муаллиф ё дигар хосияти объект) ва ғайриимкон гардонидани дасткаши аз муаллифият (имзои электронӣ)-ро меомӯзад. Чунин методҳо ва

усулҳои табдилдиҳии итилоотро шифр (рамз) меноманд. Рамзгузорӣ (шифрования)- бо истифодаи қоидаҳои муайяни рамз (шифр) матни додашударо ба матни рамзгузошташуда (шифротекст, криптограмм) табдил медиҳад. Рамзкушоӣ амали ба рамзгузорӣ баръакс мебошад, яъне матни рамзгузошташударо бо истифода аз қоидаҳои рамз (шифр) рамзкушоӣ мекунад.

Бояд қайд кард, ки криптография аз стенография фарқи калон доранд.

Масъалаи рамзгузорӣ танҳо барои итилооте, ки ба ҳимоя ниёз доранд ба вуҷуд меояд. Одатан дар ин ҳолат мегӯянд, ки итилоот сирри махфӣ дошта, давлатӣ ё конфидентсиалӣ (махфӣ, пинҳонӣ) мебошад. Криптография илми татбиқӣ буда, даствардҳои илмҳои дақиқ, алалхусус математикаро истифода мебарад. Қайд кардан ба маврид аст, ки ҳамаи масъалаҳои криптография аз дараҷаи инкишофи илму технология, аз татбиқи воситаҳои алоқа ва усулҳои равон кардани итилоот вобастагии калон доранд. Одатан итилоотҳои, ки онҳоро рамзгузорӣ кардан лозим аст, дорои сири

- ✓ давлатӣ;
- ✓ ҳарбӣ;
- ✓ соҳибкорӣ;

ва ғайра мебошанд.

Се усули маъмули ҳимояи итилоотро мавҷуд аст:

1. физикӣ;
2. стенографӣ;

3. криптографӣ.

Усули физикӣ - ҳимояи барандагони итилоот аз дастёбӣ (перехвата), нест кардани барандагони итилоот ҳангоми хавфи бадаст оварӣ (самолётҳои Америка) ва ғайраро меомӯзад.

Усули стенография – махфи гардонидани барандагони итилоот (сари ғуломан, ранги ноаён ва ғайра) ро меомӯзад.

Усули криптография – ин усулҳои ҳимоя дар замони ҳозира нисбатан маъмул ва машҳуртар мебошанд.

Криптография таъмин мекунад:

1) махфикунонии итилоот;
2) аутентификатсияи итилоот, яъне тасдиққунии соҳибияти итилоот, соҳибияти тарафҳо, вақти сохтан ва ғайра;
3) ғайриимкон гардонидани дасткашӣ аз соҳибият, яъне имзоҳои электронӣ;
4) якпорчагии итилоот;

ва ғайра.

Методҳои криптографӣ дар масъалаҳои татбиқии зерин истифода бурда мешаванд:

1) имзоҳои электронии рақамӣ (ИЭР);
2) пулҳои электронӣ;
3) қуръакашии электронӣ;
4) шартномаҳои дар як вақт имзогузошташуда;

5) ҳимояи коғазҳои қиматнок;
6) овоздиҳии электронӣ;

ва ғайра.

2. Таърихи криптография

Криптография илмест, ки тақрибан ҳангоми пайдоиши хат ба вуҷуд омада, таърихи 8 ҳазор соларо доро мебошад. Таърихи криптографияро метавон ба 5 марҳила тақсим кард:

1) Марҳилаи якум тақрибан аз асри VI-и пеш аз милод оғоз гардидааст. Принсипи асосӣ дар ин марҳила иваз намудани як ҳарф бо ҳарфи дигар ва ё ивази ягон символ ба символи дигар мебошад. Методҳо ва воситаҳои ин давра: рамзи Атбаш, таҷҳизоти Скитал (а. V), диски ва ҷадвали Энея (а. IV), квадрати Полибия (а. II) , Рамзи Сезар (I) ва ғайра.
2) Марҳилаи дуюм аз асри IX мелодӣ оғоз гардида то ибтидои асри XX давом кардааст. Дар ин давра метавон ибтидо дар Шарқи наздик корҳои Ал-Фараҳидӣ (718-791), Ал-Киндӣ (801-847), Ал-Қалкашандӣ (1355-1412) ва баъдан сар карда аз асри 15 дар Аврупо корҳои Леон Баттист Алберт (1466), Кардано (1550), Блез де Виженер (1585), Плейфер (1854 Англия) ва ғайраро номбар кард.

3) Марҳилаи сеюм аз ибтидои асри 20 сар карда то нимаи он давом кардааст. Дар ин давра воситаҳои электромеханикии рамзгузорӣ ва рамзкушоӣ пайдо шудаанд. Дар ин давра корҳои Вернам (1917), Энигма (1920), Хилл (1929) ва ғайраро метавон номбар кард.
4) Марҳилаи чорум аз миёнаи асри 20 оғоз гардида то солҳои 70-уми ин аср давом кардааст. Ин марҳила марҳилаи гузариш ба криптографияи математикӣ ба ҳисоб меравад. Дар корҳои Шеннон мафҳумҳои миқдори итилоот, интиқоли итилоот, энтропия (дар назарияи ахборӣ дараҷаи ҳолате ё вазъияте итилоотро ифода мекунад), функсияи рамзгузорӣ ва ғайра пайдо шудаанд.
5) Марҳилаи муосир аз охирҳои соли 1970 оғоз гардида то ҳол идома дорад. Дар ин давра равиши нави криптография, яъне криптография бо калидҳои кушода пайдо шуд. Дар ин давра метавон корҳои Деффи-Ҳеллман (1976), Шамир, Тоҳир Ал-Ҷамол, методҳои DES (23.11.1976), RSA (1977), ГОСТ 28147-89 (1989), ГОСТ Р 34.10.2001 (ГОСТ дар ХКЭ) ва ғайраро номбар кард.

Қайд кардан ба маврид аст, ки дар криптографияи муосир истифодабарии алгоритмҳои рамзгузории бо калидҳои кушод хос мебошад, ки истифодабарии воситаҳои ҳисобарорро талаб мекунад. Зиёда аз

даҳҳо алгоритмҳои рамзгузории санҷидашуда маълум аст, ки ин алгоритмҳо калиди кифоя калон (дароз) ва саҳеҳро истифода мебаранд. Дар ин алгоритмҳо устувории криптографӣ низ ба назар гирифта мешавад. Алгоритмҳои маъмули марҳилаи ҳозира:

- ✓ Симметрӣ ҳамаи рамзҳои ҷараёнӣ (поточный), блокӣ, DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC2, RC4, RC5 ва ғайраҳо;
- ✓ Ассиметрӣ RSA, Elgamal (Ал-Ҷамол), ECDSA (Elliptic Curve Digital Signature Algorithm), Rabin, Luc, Диффи-Ҳеллман DH (Diffie, Hellman), DSA (Digital Signature Algorithm), ГОСТ Р 34.10-2001, McEliece, Williams System;
- ✓ Ҳэш-функсия MD4, MD5, MD6, SHA (Secure Hash Algorithm), SHA-1, ГОСТ Р 34.11-94.

Қайд. *Дар оянда мафҳумҳои симметрӣ, асимметрӣ, ҳэш-функсия ва алгоритмҳои овардашударо шарҳу эзоҳ медиҳем.*

Дар бисёр мамлакатҳо стандарти миллии рамзгузориро қабул кардаанд. Масалан, соли 2001 дар ИМА стандарти рамзгузории симетрӣ AES дар асоси алгоритми Rijndael бо дарозии калиди 128, 192 ва 256 бит сохта шуда, қабул гардид. Алгоритми AES ба ҷои алгоритми пешинаи DES омад, ки ҳоло барои истифода фақат дар режими Triple DES тавсия карда шудааст. Дар Федератсияи Русия бошад, стандарти ГОСТ 28147-89, ки алгоритми блокии рамзгузорӣ бо калиди 256 битро дар

бар мегирад ва ичунин алгоритми имзои рақамӣ ГОСТ Р 34.10-2001 вуҷуд дорад.

3. Мафҳумҳои асосӣ

Матни ошкор — додаҳое (шарт нест, ки матнӣ бошанд), ки бе истифодаи криптография равон карда мешаванд. Бо суханҳои дигар, матни ошкор – ин итилооти додашуда пеш аз рамзгузорӣ мебошад.

Шифротекст ё матни рамзгузошташуда – додаҳое, ки пас аз татбиқи криптосистема ба даст меояд. (одатан - бо истифода ягон калид).

Калид - ин параметри рамз (шифр) мебошад, ки барои рамзгузорӣ ва рамзкушоии итилоот истифода бурда мешавад.

Рамз (Шифр, криптосистема) — системаи (семейство) табдилдиҳии матни кушод ба матни рамзгузошташуда.

Рамзгузорӣ (Шифрования) — ҷараёни татбиқи табдилдиҳии криптографии матни кушод дар асоси алгоритм ва калид, ки дар натиҷа матни рамзгузошташуда ба вуҷуд меояд.

Рамзкушоӣ (Расшифровывания) — ҷараёни татбиқи табдилдиҳии криптографӣ, ки матни рамзгузоштаро ба матни ошкор табдил медиҳад.

Рамзи ассиметрӣ (Асимметричный шифр) - рамзи ду калида ё рамзи бо калиди кушода, рамзест, ки дорои ду калид, калиди рамзгузорӣ ва калиди рамзкушоӣ мебошад. Барои чунин намуди рамзгузорӣ бо донистани калиди рамзгузорӣ наметавон матнро рамзкушоӣ кард ва баръакс.

Калиди кушод - яке аз ду калидҳои криптографии ассиметрӣ, ки ба ҳар ду тараф дастрас аст ва ё дар шабака ба таври озодона паҳн карда мешавад.

Калиди махфӣ - яке аз ду калидҳои криптографии ассиметрӣ, ки махфӣ нигоҳ дошта мешавад.

Криптоаналитик — олиме, ки методҳои криптографиро сохта ва истифода мекунад.

Илме, ки бо ҳифзи иттилоот машғул аст, криптология ном дорад.

Криптология аз ду калимаи юнонӣ гирифта шуда, маънояш cryptos- махфӣ, logos-илм мебошад.

Криптология ба ду самт ҷудо мешавад:

- ✓ криптография;
- ✓ криптоанализ.

Криптография – ҷустуҷӯ ва тадқиқи усулҳои математикии табдилдиҳии иттилоотро меомӯзад.

Криптоанализ — илмест, ки методҳои математикии халалдоркунии конфиденсиалӣ ва ягонагии иттилоотро барои рамзкушоӣ кардан истифода мебарад.

Алифбо гуфта, маҷмӯи ба тартибоварда шудаи элементҳои алифборо меноманд. Бо сифати алифбоҳо дар системаҳои иттилооти ҳозиразамон чунин алифбоҳоро истифода мебаранд:

- ✓ русӣ 32-ҳарф;
- ✓ лотинӣ 26-ҳарф;
- ✓ бинарӣ 0,1;

ва ғайра

Ҳамлаҳои криптографӣ – кӯшиши криптоанализ, ки ба системаи ҳимоякардашуда мубодилаи итилооти ба мақсади ба даст овардани итилоот равона карда шудааст.

Ҳамлаи бо муваффақият анҷомёфтаи криптоанализро шикастан (взлом) ё ошкоркунӣ меноманд.

Дешифрование (дешифровка) — ҷараёни табдилдиҳии ё кушодани матни рамзгузошташуда бе донистани калид дар асоси маълумотҳои маъмули рамзгузорӣ.

Ҳэш-функсия — функсияест, ки пайғомҳои дарозиашон гуногунро ба пайғомҳои дарозиашон қайдкардашуда табдил медиҳанд.

4. Рамзи Атбаш

Рамзи Атбаш (калимаи яҳудӣ. אתב"ש) яке аз рамзҳои кадимтарини яҳудиҳо мебошад, ки тақрибан асри VI – и п.м. аз тарафи Ессея (иудейкой сектой

повтанцев) сохта шудааст. Усули рамзгузории методи мазкур чунин аст: Ҳарфи аввали алифбо бо ҳарфи охир, ҳарфи дуюм ба ҳарфи пеш аз охир ва ҳоказо иваз карда мешавад. Бо суханҳои дигар, дар як сатр алифбое, ки тавассути он пайғом навишта мешавад, менависем. Дар сатри дуюм бошад, алифборо ба таври баръакс тавре менависем, ки ҳар як ҳарф дар зери ҳарфи дигар қарор гирад. Пас, барои рамзгузорӣ ҳар як ҳарфи матни пайғомро мувофиқан бо ҳарфи сатри дуюм иваз мекунем. Масалан, тарзи навиштани алифбои лотинӣ чунин аст.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Мисол:

Матни ошкор:WORD .

Матни рамзгузошташуда: DMJW

Бо суханҳои дигар агар сар карда аз як ҳарфҳои алифборо рақамгузорӣ кунем. Он гоҳ усули рамзгузории методи мазкурро метавон чунин баён кард: Ҳарфи i – юми алифбо бо ҳарфи (n+1-i) mod n иваз карда мешавад. Дар ин ҷо i –рақами тартибии ҳарф дар алифбо буда, n – миқдори ҳарфҳои алифбо мебошад.

Калимаи Атбаш аз чор ҳарф: Алеф, Тае, Бет ва Шит гирифта шудааст, ки ҳарфи якум, охирон, ҳарфи дуюм, ҳарфи пеш аз охирони алифбои Рими Қадим мебошанд.

Барномаи рамзгузории методи Атбаш дар забони C++ барои ҳарфҳои калони алифбои лотинӣ.

```
#include <iostream>
#include <string>
using namespace std;
int main(int argc, char** argv) {
 string S;
 cin>>S;
 for (int i = 1; i <= S.size(); i++){
        int T = (int)S[i] - 65;
        T = 25 - T;
                S[i] = (char)T + 65;
        }
        cout<<S;
return 0;
```

5. Асбоби скитал

Дар криптография скитал (ё сцитал аз калимаи юнонии σκυτάλη- шашпар, гурз, амуд, чӯбдасти махсуси идора кардани ҳаракати кӯча) ҳамчун рамзи Спартаи Қадим маълум буда, барои иҷрои рамзгузории

ҷойивазкуни истифода бурда мешавад. Асбоби мазкур аз силиндри борик ва тасмачаи пергаментие (пӯсти хайвонот, ки ба таври махсус кор карда шуда, то пайдоиши коғаз барои хатнависӣ

истифода мешуд), ки дар атрофи силиндр ба сурати спиралӣ печонида шудааст, иборат буда, ҳангоми рамзгузорӣ (рамзкушоӣ) пайғоми лозимӣ дар он навишта мешавад. Юниҳои қадим ва спартаҳо асбоби мазкурро баъзан дар вақти ҷангҳо истифода мебурданд.

Рамзгузорӣ

Барои рамзгузорӣ аввал тасмачаи пергамен-тиро дар атрофи найча(силинд) ба сурати спиралӣ печонида, сипас, матни лозимиро дар болои он ба шакли уфуқӣ менависем. Пас аз навиштани матни лозимӣ тасмачаро мекушоем, ки дар он матни рамзгузошташуда пайдо мешавад. Барои рамзкушоӣ найчаи андозааш ба андозаи найчае, ки тавассути он рамзгузорӣ карда будем, лозим меояд.

Ҳангоми рамзгузорӣ ду параметри асосӣ нақши (роли) калон мебозанд: миқдори ҳарфҳои дар як сатр (силинд) навишташуда ба шакли уфуқӣ – n ва миқдори символҳои дар як даври силинд навишташуда – m. Масалан, бигузор силиндре, ки дар як даври он навиштани 4 рамз ва ба дарозии он навиштани 8 рамз имкон дорад, дода шуда бошад. Ҳангоми рамзгузории пайғоми “Ин рамзи Спартаи қадим аст!” шакли «И_ _ енсқб_паорадшариамтмдза _!ним» - ро мегирад.

Ба таври схематикӣ ин амал чуниин шакл дорад:

и	н	_	р	а	м	з	и
_	с	п	а	р	т	а	и

_	қ	а	д	и	м	_	м
е	б	о	ш	а	д	!	.

Тавре ки аз ин мисол дида мешавад, ҳангоми рамзгузорӣ ҷадвале сохта мешавад, ки дорои 4 сатр ва 8 сутун мебошад. Аз баски ҳангоми мубодилаи итилоот, итилооте мавҷуданд, ки дорои дарозиҳои гуногун мебошанд, бинобар ин, бо назардошти ҳар ду тарафҳо яке аз ин параметрҳо, яъне миқдори сатрҳо ё сутунҳо интихоб карда мешавад (одатан m). Параметри дуюм бошад, тавассути формулаи $n = \left[\frac{k-1}{m}\right] + 1$ ҳисоб карда мешавад. Дар ин ҷо k – миқдори символҳои мактуб ва $[x]$ - қисми бутуни ададии х мебошад.

Алгоритми рамзгузорӣ

1) Ибтидо матн ба қисмҳои иборат аз n – символ ҷудо карда мешавад;
2) Дар ҳар як сатри ҷадвал n символ (як қисми ҷудокардашуда) навишта мешавад;
3) Пас аз навиштани ҳамаи символҳо, агар ягон катакча холӣ монад, он бо ҷойи холӣ ё ягон символи дигар пур карда мешавад.
4) Агар ҷадвал (тасмача) пеш аз баохиррасии пайғом пур шавад, маънои онро дорад, ки андозаҳо нодуруст интихоб карда шудаанд.
5) Дар охир матни дар ҷадвал навишташударо ба намуди амудӣ пайиҳам навишта, пайғоми рамзгузошташуда ҳосил мекунем.

Рамзкушоӣ

Барои рамзкушоӣ силиндри диаметраш ба силиндре, ки тавассути он пайғом рамзгузорӣ карда шуда буд, лозим аст, ки дар он тасмача ба сурати спиралӣ барои рамзкушоӣ печонида мешавад. Бартарияти рамзи мазкур аз он иборат аст, ки ҳангоми рамзгузорӣ хатогӣ кам ба амал меояд. Аммо чунин рамзро метавон зуд шикаст. Масалан, усули рамзшиканиии рамзи мазкурро Эдгар Аллан По дар кори худ «A Few Words on Secret Writing[1]» пешниҳод кардааст. Моҳияти ин усул аз он иборат аст, ки ҳангоми надонистани диаметри силиндр конуси диаметраш тағйирёбанда гирифта мешавад. Пас аз ин лента дар атрофи он печонида шуда, ба ин тараф ва ба он тарафи конус то барқарор кардани пайғом ҳаракат дода шуда, пайғом рамзкушоӣ карда мешавад.

Алгоритми рамзкушоӣ

Талаб карда мешавад, ки матни «И_ _енсқб_паорадшариамтмдза_!ним.» рамзкушоӣ карда шавад.

Барои рамзкушоӣ ҷадвали дорои 4 сатр ва 8 сутунро истифода мебарем. Барои рамзкушоӣ матн сутун ба сутун навишта мешавад. Илова бар ин, дар ҳар як сатр 4 символ ва дар ҳар як сутун 8 символ навиштан лозим аст.

[1]1) http://www.eapoe.org/works/essays/fwsw0741.htm
2) http://knowingpoe.thinkport.org/classconn/Secret_Writing_Overview.pdf

1) Бо назардошти ҷои холӣ (пробел) матни додашуда ба қисматҳое, ки аз 4 символ иборатанд, ҷудо карда мешавад. «И_ _ н сқб_ паор адша риам тмдз а_!н им. »
2) Ибтидо сутуни якумро барқарор мекунем, барои ин чор ҳарфи гурӯҳи аввалро дар сутуни якум менависем:

И	*	*	*	*	*	*	*	*
_	*	*	*	*	*	*	*	*
_	*	*	*	*	*	*	*	*
Е	*	*	*	*	*	*	*	*

3) Дар сутуни дуюм низ 4 символи гурӯҳи баъдиро менависем:

И	н	*	*	*	*	*	*
_	с	*	*	*	*	*	*
_	қ	*	*	*	*	*	*
Е	б	*	*	*	*	*	*

4) Ҳамин тариқ ҳамаи гурӯҳҳоро дар ҷадвал навишта мешаванд:

И	н	_	р	а	м	з	И
_	с	п	а	р	т	а	и
_	қ	а	д	и	м	_	м
е	б	о	ш	а	Д	!	.

5) Баъди навиштан матнро сатр ба сатр мехонем, ки “Ин рамзи Спартаи қадим аст!” ҳосил мешавад.

Барномаи рамзгузории тавассути Скитал дар забони C#

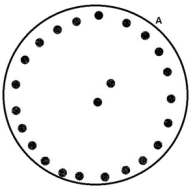
```
using System;
namespace SCITAL
{
   class Program
```

```
  {
    static void Main(string[] args)       {
      string skiText = Console.ReadLine();
      int stolbci = 0, count = 0;
      string[] mass = skiText.Split(" ".ToCharArray(),
StringSplitOptions.RemoveEmptyEntries);  //Сатрро
ба калимаҳо ҷудо карда, ҷойҳои холиро нест
мекунем.
      skiText = null;
      foreach (string r in mass)
        skiText += r;    //Сатри бе ҷойи холиро ба
даст меорем
      char[] rezArray = new char[skiText.Length];
//Барои таҳия намудани рамзи Скитал массиви
типи char-ро месозем
      for (int i = 1; i < skiText.Length; i++) {
        if (skiText.Length / i == 4){
          stolbci = i;     //миқдори сатрҳо дар рамз
ба таври пешфарз баробар аст ба 4
          break;
        }
      }
      for (int i = 0; i < stolbci; i++){
        int plus = i;
        {
          for (int j = 0; j < 4; j++) {
            rezArray[count] += skiText[plus];  //Аз
рӯӣ ҳарфҳо сатр месозем
```

```
                    plus += stolbci;
                    count++;
                }
            }
        }
        for (int i = 0; i < rezArray.Length; i++)
          Console.Write(rezArray[i]);    //Хоричқунии
натича
        Console.WriteLine();
        Console.ReadKey();
    }
}
}
```

6. Диски Энея

Диски Энея – асбоби криптографӣ барои ҳифзи итилоот мебошад, дар асри IV –и п.м. аз тарафи Энея Тактик[1] (юнонӣ. Αινείας ο Τακτικός; а. IV п.м.) сипаҳсолор ва сиёстмадори Юнони Қадим сохта шудааст. Асбоби мазкур дискест, ки диаметри он ба 15 см ва ғафсиаш ба 1-2 см баробар буда, ба миқдори алифбо сурохӣ дорад. Ҳар як сурохи ба як ҳарф мувофиқ гузошта мешавад. Дар маркази диск ғалтаке мавҷуд аст, ки дар он ришта печонида шудааст.



[1] http://www.xlegio.ru/sources/aeneas-tacticus/1st-military-theorist-of-antiquity.html

Рамзгузорӣ

Механизми рамзгузорӣ хеле сода мебошад. Барои рамзгузории пайғом пайдарпай риштаро ба сурохие, ки ҳарфро ифода мекунад мегузаронем. Дар натиҷа диск ва ришта пайғоми рамзгузошташударо ифода мекунанд.

Рамзкушоӣ

Барои рамзкушоӣ риштаро пайдарпай аз ҳар як сурохи бароварда, ҳарфи мувофиқи онро менависем. Пас аз навиштани ҳамаи ҳарфҳо матнро аз рост ба чап мехонем.

Дар ин навъ асбоби ҳимояи итилоот норасоии хеле зиёд мавҷуд мебошад. Матни рамзгузошташуда, барои ҳама дастрас буда, ҳар касе, ки дискро ба даст меорад, метавонад пайғомро хонад, агар моҳияти ин методро сарфаҳм равад.

7. Квадрати Полибия

Рамз ё квадрати Полибия (англ. Polybius square) аз тарафи корманди давлатӣ, сипаҳсолор ва таърихнигори Юнони Қадим Полибий [1] (асри II п.м.) сохта шудааст. Барои рамзгузории итилооти муҳим ҷадвали дорои n сатр ва m сутун сохта мешавад, ки сатрҳо ва сутунҳои он сар карда аз 1 рақамгузорӣ карда мешаванд. Дар ин ҷо параметрҳои n ва m тавре интихоб карда

[1] Юнонӣ. Πολύβιος, лот. Polybius; тақрибан соли 200 п.м. дар Мегалопол, Аркадия тавал-луд шуда, дар соли. 120 вафот кардааст.

мешаванд, ки ҳосили зарбашон тақрибан ба миқдори ҳарфҳои алифбо баробар шавад. Пас аз сохтани ҷадвал дар ҳар як катакча яктогӣ ҳарфҳои алифбо навишта мешаванд. Дар натиҷа ҳар як ҳарф ба ҷуфти рақамҳо, ки нишондиҳандаи сатр ва сутун мебошанд, мувофиқ меояд. Ҳангоми дар ҷадвал пурра нағунҷидани ҳамаи ҳарфҳои алифбо дар баъзе катакчаҳо дутогӣ ҳарф низ навиштан мумкин аст. Аммо агар ягон катакча холӣ монад, он бо ҷои холӣ ва ё ягон символи дигар пур карда мешавад. Ба сифати намуна якчанд алифборо дида мебароем.

Алифбои лотинӣ

Тавре ки медонем алифбои ҳозираи лотинӣ дорои 26 ҳарф мебошад. Бинобар ин, ҷадвали дорои 5 сатр ва 5 сутун варианти наздиктарин мебошад. (чунки 5*5=25 адади наздиктарин ба 26 аст). Азбаски ҳарфҳои I ва J бо ҳам монанд мебошанд, аз ин рӯ онҳоро дар як катакча менависем. Дар натиҷа ҷадвал ба сурати зерин ҳосил мешавад:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Алифбои криллӣ

Ғояи (Идеяи) сохтани ҷадвалро барои алифбои криллӣ дида мебароем. Аз баски миқдори ҳарфҳои алифбои криллӣ ба 33 баробар аст, бинобар ин, ҷадвали дорои 6 сатр ва 6 сутун месозем, чунки 36 наздиктарин адад ба 33 аст:

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Илова бар ин, метавон бо усули дигар барои алифбои криллӣ ҷадвал сохт. Дар ин усул ҳар як ҷуфти ҳарфҳои Е ва Э, И ва Й, Р ва С, Ф ва Х, Ш ва Щ – ро мувофиқан дар як катакча навишта ҳарфҳои Ы, Ь ва Ё –ро сарфи назар мекунем. Дар натиҷа ҷадвали зерин ҳосил мегардад:

	1	2	3	4	5
1	А	Б	В	Г	Д
2	Е/Э	Ж	З	И/Й	К
3	Л	М	Н	О	П
4	Р/С	Т	У	Ф/Х	Ц
5	Ч	Ш/ Щ	Ы	Ю	Я

Ба ҳамин монанд метавон барои дилхоҳ алифбо квадрат сохт.

Пас аз сохтани квадрат қадами дуввум тавассути он ягон итилоотро рамзгузорӣ карда мешавад. Барои рамзгузорӣ намудан якчанд усул бо истифода аз квадрати Полибия мавҷуд аст. Ҳоло сето маъмултарини онҳоро дида мебароем.

Усули 1

Талаб карда мешавад, ки матни «DONISHVAR» рамзгузорӣ карда шавад:

Барои рамзгузорӣ намудани матни додашуда аз ҷадвали Полибия, ки қаблан барои алифбои лотинӣ сохта будем, истифода мебарем. Қоидаи рамзгузорӣ чунин аст: агар матни додашуда дар сатри охири ҷадвал ҷойгир бошад, он гоҳ ҳарфи сатри аввали ҷадвал, ки бо ҳарфи додашуда дар як сутун мехобад гирифта мешавад. Дар ҳолати акс, ҳарфе, ки дар катакчаи поёнии ҳарфи додашуда ҷойгир аст гирифта мешавад.

Ҷадвали координатаҳо									
Ҳарфҳои матни ошкор:	D	O	N	I	S	H	V	A	R
Ҳарфҳои мати рамзгузошташуда:	I	T	S	O	X	N	A	F	W

Ҳамин тариқ, пас аз рамзгузорӣ ҳосил мекунем “ITSOXNAFW”.

Барномаи рамзгузории усули якуми квадрати Полибия дар java

```
  public class Polibiy {
   public byte[] encrypt(String text, char[][] matr) {
       byte[] ans = new byte[text.length() * 2];
      for (int c = 0; c < text.length(); c++) {
         for (int i = 0; i < matr.length; i++) {
          for (int j = 0; j < matr[i].length; j++) {
           if (matr[i][j] == text.charAt(c)) {
              ans[c * 2] = (byte)i;
              ans[c * 2 + 1] = (byte)j;
                 }
               }
         }
}
    return ans;
         }
public String decrypt(byte[] text, char[][] matr){
   StringBuilder s = new StringBuilder();
     for (int i = 0; i < text.length / 2; i++)          {
         s.append(matr[text[i * 2]][text[i * 2 + 1]]);
         }
         return s.toString();
  }
}
```

Усули 2

1) Ибтидо ҷадвали дорои се сатр ва n сутун месозем. Дар ин ҷо n миқдори ҳарфҳои матни ошкорро ифода

мекунад. Пас аз сохтани ҷадвал дар сатри якум ҳарфҳои матни ошкор, дар сатри дуюм координатаҳои уфуқии мувофиқи ҳар як ҳарф ва дар сатри сеюм координатаҳои амудии мувофиқи ҳар як ҳарф навишта мешаванд. Дар натиҷа ҷадвали зерин ҳосил мешавад:

Ҷадвали координатаҳо									
Ҳарфҳои матни ошкор:	D	O	N	I	S	H	V	A	R
Координатаи уфуқӣ:	4	4	3	4	3	3	1	1	2
Координатаҳои амудӣ:	1	3	3	2	4	2	5	1	4

1. Пас аз ин, координатаҳоро аз рӯйи сатр ҷуфт-ҷуфт менависем, ки шакли зеринро мегиранд:

44 34 33 11 21 33 24 25 14 (1*)

2. Дар қадами оянда координатаҳоро аз рӯйи квадрат бо ҳарф табдил медиҳем:

Ҷадвали координатаҳо								
Координатаи уфуқӣ:	4	3	3	1	2	3	2	1
Координатаҳои амудӣ:	4	4	3	1	1	3	4	4
Ҳарфҳо:	T	S	N	A	B	N	R	Q

Ҳамин тариқ матни додашуда рамзгузорӣ карда мешавад, ки шакли “TSNABNRQ” –ро дорад.

Барномаи рамзгузории усули дуюми квадрати Полибия дар забони C++

```
void __fastcall TForm1::Button1Click(TObject *Sender)
 {
        int v[1000], v1[100];
        bool y = false;
        AnsiString S, S3;
        char w[5][5];
        int i, j, k, len, n, m;
        char c = 'A' - 1;
        StringGrid1->ColCount = 6;
        StringGrid1->RowCount = 6;
        StringGrid1->FixedCols = 0;
        StringGrid1->FixedRows = 0;
        StringGrid1->DefaultColWidth = 30;
        for (i = 0; i<5; i++){
           for (j = 0; j<5; j++){
              if (c == 'I')
                  c += 2;
              else
                 c++;
                 w[i][j] = c;
                  StringGrid1->Cells[j + 1][i + 1] =
(AnsiString)w[i][j];
  }
   StringGrid1->Cells[i + 1][0] = IntToStr(i);
  StringGrid1->Cells[0][i + 1] = IntToStr(i);
```

```
}
        S = Memo1->Text;
        S = S.Trim();
        S3 = S;
        len = S.Length();
        for (k = 1; k <= len; k++){
                y = true;
                for (int i = 0; i<5; i++)
                for (int j = 0; j<5; j++)
                if (S[k] == w[i][j]){
                        v[k] = j;
                        v1[k] = i;
                        y = false;
                        break;
                }
                if (y){
                        v[k] = 10;
                        v1[k] = 10;
                }
        }
        for (i = 1; i <= len; i++){
          S3[i] = w[v[i]][v1[i]];
ListBox1->Items->Add(IntToStr(v[i]) + "  " + IntToStr(v1[i]));
}
 Memo2->Text = S3;
}
```

Усули 3

Ин усул нисбат ба ду усули дар боло овардашуда душвортар мебошад. Алгоритми ин усул чунин аст:

1) Ибтидо шифротексти аввала (1*) – ро ҳосил карда, дар ягон ҷо бе ҷои холӣ менависем.

443433112133242514

2) Пайдарпайии рақамҳои ҳосилшударо ба таври даврӣ як мавқеъ ба тарафи чап мекӯчонем (дилхоҳ миқдори қадамҳои ғайричуфт):

434331121332425144

3) Пайдарпайии ҳосилшударо ба гурӯҳҳои дутогӣ тақсим мекунем:

43 43 31 12 13 32 42 51 44

4) Координатаҳои ҳосилшударо аз рӯйи ҷадвал ба ҳарф табдил медиҳем, ки дар натиҷа матни рамзгузошташуда ба сурати “OOCFLHIET” пайдо мешавад.

Ҷадвали координатаҳо									
Координатаи уфуқӣ:	4	4	3	1	1	3	4	5	4
Координатаҳои амудӣ:	3	3	1	2	3	2	2	1	4
Ҳарфҳо:	O	O	C	F	L	H	I	E	T

Барномаи рамзгузории усули сеюми квадрати Полибия дар забони C++

```
void __fastcall TForm1::Button3Click(TObject *Sender)
      {
```

```
        vector <int> vec;
        int v[1000], v1[100];
        bool y = false;
        AnsiString S, S3;
        char w[5][5];
        int i, j, k, len, n, m;
        char c = 'A' - 1;
        StringGrid1->ColCount = 6;
        StringGrid1->RowCount = 6;
        StringGrid1->FixedCols = 0;
        StringGrid1->FixedRows = 0;
        StringGrid1->DefaultColWidth = 30;
        for (i = 0; i<5; i++){
                for (j = 0; j<5; j++){
                        if (c == 'I')
                                c += 2;
                        else
                                c++;
                        w[i][j] = c;
StringGrid1->Cells[j + 1][i + 1] = (AnsiString)w[i][j];
                }
        StringGrid1->Cells[i + 1][0] = IntToStr(i + 1);
        StringGrid1->Cells[0][i + 1] = IntToStr(i + 1);
        }
        S = Memo1->Text;
        S = S.Trim();
        S3 = S;
        len = S.Length();
```

```
for (k = 1; k <= len; k++){
        y = true;
        for (int i = 0; i<5; i++)
        for (int j = 0; j<5; j++)
        if (S[k] == w[i][j]){
                v[k] = j;
                v1[k] = i;
                y = false;
                break;
        }
        if (y){
                v[k] = 10;
                v1[k] = 10;
        }
}
for (i = 1; i <= len; i++)
        vec.push_back(v[i] + 1);
for (i = 1; i <= len; i++)
        vec.push_back(v1[i] + 1);
int h = vec[0];
for (i = 0; i<vec.size() - 1; i++){
        vec[i] = vec[i + 1];
}
vec[vec.size() - 1] = h;
for (i = 0, k = 1; i<vec.size() - 1; i += 2) {
        v[k] = vec[i];
        v1[k] = vec[i + 1];
        k++;
```

```
        }
        for (i = 1; i <= len; i++){
          S3[i] = w[v1[i] - 1][v[i] - 1];
          ListBox1->Items->Add(IntToStr(v[i]) + "  " +
IntToStr(v1[i]));  }
        Memo2->Text = S3;
}
```

Қайд кардан ба маврид аст, ки барои квадрати Полибия инчунин метавон калид низ истифода кард. Дар ибтидо ҳарфҳои калид бетакроршавии ҳарфҳо дар ҷадвал навишта шуда, дар катакчаҳои боқимонда ҳарфҳои дигари алифбо, ки дар таркиби калид мавҷуд нестанд, навишта мешаванд.

Мисол. Бо истифода аз калиди «DAFTAR» матни «DONISHVAR» рамзгузорӣ карда шавад.

Ҳал. Барои рамзгузорӣ намудан аз алгоритми зерин истифода мебарем:

1) Ибтидо квадрат месозем. Барои сохтани квадрат аввал ҳарфҳои калид ва сипас ҳарфҳои боқимондаи алифборо дар квадрат пайдарпай менависем:

	1	2	3	4	5
1	D	A	F	T	R
2	B	C	E	G	H
3	I	K	L	M	N
4	O	P	Q	S	U
5	V	W	X	Y	Z

2) Аз рӯӣ квадрати сохтаамон координатаҳои ҳарфҳоро менависем:

Ҷадвали координатаҳо									
Ҳарфҳои матни ошкор:	D	O	N	I	S	H	V	A	R
Координатаҳои уфуқӣ:	1	1	5	1	4	5	1	2	5
Координатаҳои амудӣ:	1	4	3	3	4	2	5	1	1

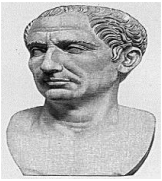
3) Координатаҳои ҳосилшударо аз рӯйи сатр навишта, дутогӣ ба гурӯҳҳо тақсим мекунем:

11 51 45 12 51 43 34 25 11

Координатаҳои ҳосилшударо аз рӯйи ҷадвал ба ҳарф табдил медиҳем, ки дар натиҷа матни рамзгузошташуда ба сурати “DRYBRMQWD” пайдо мешавад.

Ҷадвали координатаҳо									
Координатаҳои уфуқӣ:	1	5	4	1	5	4	3	2	1
Координатаҳои амудӣ:	1	1	5	2	1	3	4	5	1
Ҳарфҳо:	D	R	Y	B	R	M	Q	W	D

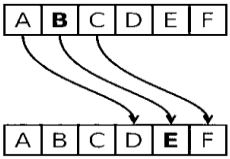
8. Рамзи Сезар



Рамзи Сезар (рамзи *лағжиш* ё коди Сезар) яке аз методҳои сода ва маъмули рамзгузорӣ мебошад, ки тақрибан асри I –и п.м. аз тарафи ходими давлатӣ, сиёсатмадор, сипаҳсолор, нависанда, консули (номи

шахсони олимартабаи ҳукумати дар Рими Қадим ва Франсия) Рими Қадим Гай Юлий Сезар [1] (талафузи дурусти ин калима ба Қайсар наздик мебошад; лот. Gaius Iulius Caesar [ˈgaːiʊs ˈjuːliʊs ˈkaɐ̯sar]; 12 ё 13 июли соли 100 п.м. — 15 марти соли 44 п.м.) сохта шудааст.

Рамзи мазкур – рамзи ҷойгузорӣ (подстановка [2]) буда, дар он ҳар як ҳарфи матни ошкор бо ҳарфе, ки дар алифбо якчанд мавқеъ дар тарафи рост ё чапи он ҷойгир аст, иваз карда мешавад. Масалан, дар рамзи се лағжиш ба тарафи чап ҳарфи A бо ҳарфи D, ҳарфи B бо ҳарфи E, ҳарфи C бо ҳарфи F ва ҳоказо иваз карда мешаванд.



Модели математикӣ

Агар сар карда аз 0 ҳарфҳои алифборо рақамгузорӣ кунем, он гоҳ барои рамзгузорӣ ва рамзкушоӣ мувофиқан аз формулаҳои зерин истифода бурда мешавад:

$$y = (x + k) mod\ n, \qquad (1)$$

$$x = (y - k + n) mod\ n. \qquad (2)$$

Дар ин ҷо x –рақами рамзи матни кушод(қимати ададии ҳарфи матни кушод), y – рақами рамзи (символи) матни рамзгузошташуда, n – миқдори ҳарфҳои алифбо ва k – калид мебошад. Қайд мекунем, ки параметри k

[1] https://en.wikipedia.org/wiki/Caesar_cipher
[2] https://en.wikipedia.org/wiki/Substitution_cipher

миқдори лағжиш ба чап ва ё ростро ифода мекунад. Тавре ки аз асари “зиндагии дувоздаҳ шоҳ”-и Гай Светоний Транквилл маълум аст, Сезар дар ибтидо калиди $k = 3$-ро истифода кардааст.

Мисол. Бо истифода аз калиди $k = 3$ матни “МАКТАВ” рамзгузорӣ карда шавад.

Ҳал. Барои рамзгузорӣ намудани матни додашуда, метавон аз усулҳои зиёде истифода кард, аммо аз ҳама усули содатарин он аст, ки ҷадвали дорои 26 (миқдори ҳарфҳои алифбои лотинӣ) сутун ва ду сатр сохта шавад.

Дар сатри якуми ин ҷадвал ҳарфҳои алифбои лотиниро бо тартиб аз рӯйи алифбо менависем. Дар сатри дуюм бошад, ҳарфҳои алифборои пас аз лағжонидани даврӣ се мавқеъба тарафи рост менависем:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Пас аз сохтани ҷадвал барои рамзгузорӣ намудани матни додашудаи “МАКТАВ” ҳар як ҳарфи онро ба ҳарфи дар сатри дуюм навишташуда мувофиқан иваз мекунем. Аз баски дар зери ҳарфи М ҳарфи J ҷойгир аст, бинобар ин, онро бо J ва ҳарфи А –ро бо X ва ҳоказо иваз мекунем. Дар натиҷа, пайғоми рамзгузошташуда шакли “JXHQXY” - ро мегирад.

Барои рамзкушоӣ бошад, баръакси амал карда мешавад, яъне аз сатри дуюм ба якум.

Барномаи рамзи Сезар дар забони C++ барои алифбои калони лотинӣ

```
#include <iostream>
```

```
#include <string>
using namespace std;
int main(int argc, char** argv) {
  string S;
   int k=3, i,n,T;
  cout<<"S=";cin>>S;
  cout<<"k=";cin>>k;
  n=S.length();
  for (int i = 0; i <n; i++){
          T = (int)S[i] + k;
          if (T>256)
            T = T - 256;
          S[i] = (char)T;
 }
cout<<S;
 return 0;
}
```

9. Тараққиёти рамзгузорӣ дар мамолики Шарқи наздик

Тавре ки қайд кардем марҳилаи дуюми рамзгузорӣ дар мамолики Шарқи наздик ба вуҷуд омада, рушту густариш ёфтаст. Бинобар ин дар ин ҷо хизмати якчанд олимони машриқро меорем.

Абу Абдураҳмон ал –Халил ибни Аҳмад ал-Фараҳидӣ

Ал-Фараҳидӣ [1] соли 718 дар сарзамини ҳозира Омон ба дунё омадааст. Соли 751 дар Басра (Ироқ) вафот кардааст. Дар алифбои арабӣ ҳамза ва ҳаракатро дохил намуда, хурдтарин воҳиди овоз ҳарфро муқаррар намуд. Ӯ асаре бо номи "Китоб-ал-муаммо" навишт, ки дар он доир ба методҳои криптографӣ ҳарф меравад. Ал–Фараҳидӣ нахустин шуда бо имконияти истифодаи ҷумлаҳои стандартии матни ошкор барои рамзгузории матнӣ таваҷҷуҳ кард.

Дар асоси методи рамзкушоии сохтаи худ китоби "Китоб ал-Муаммо" – ро навишт. Боре аз Ал-Фараҳидӣ талаб карда шуд, ки мактуби императори Юнонро, ки бо забони юнонӣ навишта шуда буд рамзкушоӣ кунад. Ӯ методи рамзкушоии худро чунин маънидод кард:

Ман ба худ гуфтам, ки мактуб бояд бо ибораи "Ба номи Худо" ё бо ин монанд оғоз шавад. Сипас, дар асоси ин калима матнро рамзкушоӣ кардам, ки ҳаммааш дуруст баромад.

---

[1] https://en.wikipedia.org/wiki/Al-Khalil_ibn_Ahmad_al-Farahidi

1) *Reuschel W.* Al-Halil Ibn Ahmad, der Lebrer Slbawaihs, als Grammatiker. Berlin, 1959.
2) *Ryding K. C.* Early Medieval Arabic: Studies on Al-Khalil ibn Ahmad. Georgetown, 1998.

Ин метод солҳои 1940-1945 дар Ҷанги дуюми ҷаҳони барои шикастани комуникатсияи олмониҳо истифода шудааст.

Абӯ Юсуф Яъқуб ал-Киндӣ

Ал-Киндӣ тақрибан соли 801 дар шаҳри Куфа ё Басра таваллуд шудааст. Ал-Киндӣ муаллифи асарҳои зиёде оиди мантиқ, этика, математика, криптография, астрономия, тиб, метеорология, оптика ва мусиқӣ мебошад. Дар ғарби Европа бо номи Alkindus машҳур аст. Соли 873 дар Бағдод вафот кардааст.

Қайд кардан ба маврид аст, ки асари "Китоб ал-Муаммо"-и Фараҳидӣ то замони мо омада нарасидааст, танҳо олимони дигар дар бораи он ёд кардаанд. Дар асоси асари мазкур Абу Юсуф Яъқуб ибни Исҳоқ ибни Собеъ ал Киндӣ асари бо номи "Рисола оиди хондани мактубҳои рамзгузошташуда(О дешифровке криптографических сообщений)[1]" асари боарзише навишт.

[1] https://en.wikipedia.org/wiki/History_of_cryptography

Саҳифаи нахустини дастнависи асари ал-Киндӣ

Дар методҳои пешниҳод кардаи Халил ибни Аҳмад навгониҳои зиёде мавҷуд буданд, аз ҷумла истифодаи ҷойивазкунӣ ва комбинатсияи калимаҳои гуногун. Ҳамаи навгониҳо ва инқилобҳои системаҳои криптографии пешниҳодкардаи Ал-Киндиро дар ду ҷумлаи зерин меорем.

“...яке аз усулҳои хондани матни рамзгузошташуда (агар мо донем, ки дар кадом забон навишта шудааст) ин гирифтани матни ошкоре бо андозаи ҳамон мактуб ё

такрибан ба он баробар (дар ҳамон забон) ва ҳисоб намудани миқдори такроршавии ҳар як ҳарф мебошад. Ҳарфи аз ҳама зиёд такроршударо “якум”, ҳарфи дуюм зиёдтар такроршударо “дуюм”, ҳарфе ки басомади он дар ҷои сеюм меистад “сеюм” ва ҳоказо номгузорӣ мекунем. Ин амалро то ҳисоб намудани миқдори такроршавии ҳамаи ҳарфҳои матни ошкори интихобкардаамон давом медиҳем.

Пас аз ин, дар матни рамзгузошташудае, (матни ки мо мехоҳем онро хонем) ба ҳамин монанд символҳои онро мураттаб мекунем.

Ҳарфи (символи) аз ҳама зиёд такроршударо дар матни рамзгузошташуда ёфта онро бо ҳарфи аввали матни ошкоро иваз мекунем ва ҳарфи дуюмине, ки бисёртар такрор шудааст, бо ҳарфи дуюми матни ошкор ва ба ҳамин минвол то охир ҳамаи символҳои матни рамзгузошташударо (матне ки мо мехоҳем рамзкушоӣ кунем) иваз мекунем.” Дар натиҷа мактуб рамзкушоӣ карда мешавад.

Дар ҷойи дигар Алкиндӣ чунин мефармояд:

“Агар Шумо хоҳед, ки мактуби рамзгузошташудае, ки ба дастатон расидааст хонед, бояд дар аввал миқдори ҳарфҳои мактуб ва сипас миқдори такроршавии ҳар як ҳарфро муайян кунед. Агар созандаи рамз бодиққат буда

ҳудуди байни калимаҳоро махфӣ карда бошад, пас нахуст масъала ёфтани аломати ҷудокунандаи байни калимаҳо мебошад. Ин амал чунин иҷро карда мешавад:

Шумо ҳарфҳоро интихоб карда, бо он кор мекунед, бо назардошти пешфарзе ки ҳарфи оянда символи ҷудокунандаи калимаҳо мебошад. Ҳамин тариқ, Шумо ҳамаи номаро бо назардошти комбинатсияи мувофиҳи ҳарфҳо, ки тавассути онҳо калима сохтан мумкин аст, меомӯзед. Агар ин амал бо муваффақият ба анҷом расид, ба ҳамин кор ба анҷом мерасад, дар ҳолати акс Шумо бо навбат ҳарфи навбатиро интихоб карда, то пайдо кардани аломати ҷудокунандаи калимаҳо, амали қаблиро анҷом медиҳед.

Сипас ба Шумо лозим аст, ки ҳарфе, ки дар мактуб бисёр такрор шудааст пайдо карда, онро ба намунаи басомади ҳарфҳое, ки дар матн вомехурад муқоиса кунед. Вақте муайян мекунед, ки як ҳарф нисбат ба дигар ҳарф бисёртар дар мактуб во мехурад, фарз ин “алиф” аст. Баъд аз ин фарз мекунем, ки ҳарфи дигаре, ки бисёр такрор мешавад “лом” мебошад. Дурустии фарзи Шуморо бояд дохили он, ки дар бисёр матнҳо ҳарфи “лом” баъд аз “алиф” меояд исбот мекунад.

Калимаи нахустине, ки дар мактуб тахмин мекунед, бояд аз ду ҳарф иборат бошад. Ин амал ба роҳи баҳодиҳии

эҳтимолияти калонтарин камбинатсияи ҳарфҳо иҷро карда мешавад. Шумо эквиваленти онҳоро ҳар маротиба ҳангоми дар мактуб рӯй ба рӯй шуданатон менависед. Айнан ин амалҳоро бо калимаҳои дорои се ҳарф иҷро мекунед. Шумо эквиваленти онҳоро ҳар маротиба менависед. Ин амал барои калимаҳои чор ё панҷ ҳарф дошта низ тадбиқ мекунед. Ҳангоми пайдо шудани ягон шубҳа, ҳар маротиба бояд ду ё се ва ё зиёд фарз карда, ҳар яки онҳоро қайд кунед, то он замоне, ки дар асоси дигар калима онҳо тасдиқ карда мешаванд".

Методи Ал-Киндиро метавон ба таври содда дар алифбои русӣ тадбиқ кард. Барои ин бояд, матни дилхоҳ ё ягон матнро гирифта, миқдори такроршавии ҳарфҳоро муайян кард. Дар забони русӣ ҳарфи аз ҳама бештар истифода мешуда аввал – "о" баъд "е" сипас "а" ва ғайра мебошад. Сипас, матни пушидаро хонда, дар он басомади ҳар як ҳарфро бояд муайян кард. Агар дар матни рамзгузошташуда миқдори такроршавии "ю" аз ҳама бештар бошад, бояд он бо ҳарфи "о" иваз карда шавад. Агар ҳарфи дуюм зиёдтар истифодашуда "э" бошад, он бояд бо "е" ва ҳамин тавр то охир бояд корро анҷом дод. Методи Ал-Киндӣ ба ҷойи тафтиши калидҳои бешумор матни рамзгузошташуда бо истифодаи таҳлили криптографии ҳарфҳо рамзкушоӣ карда мешавад.

Ҷадвали 1. *Ҷадвали басомади ҳарфҳо дар алифбои кириллӣ*							
Ҳарф	Басомад %	Ҳарф	Басомад %	Ҳарф	Басомад %	Ҳарф	Басомад %
О	11,08	Р	4,45	Ы	1,96	Х	0,89
Е, Ё	8,41	В	4,33	Ь	1,92	Ш	0,81
А	7,92	К	3,36	З	1,75	Ю	0,61
И	6,83	М	3,26	Г	1,74	Э	0,38
Н	6,72	Д	3,05	Б	1,71	Щ	0,37
Т	6,18	П	2,81	Ч	1,47	Ц	0,36
С	5,33	У	2,80	Й	1,12	Ф	0,19
Л	5,00	Я	2,13	Ж	1,05	Ъ	0,02

Муайянкунии миқдори такроршавии ҳарф масъалаи шикастани рамзҳои якалифбогироо ҳал мекунад. Онро вобаста аз бузургӣ ва характери матн истифода мекунад. Басомади ҳарфҳои баъзе забон наметавонанд ба басомади ҳарфҳои мактуб мувофиқ бошанд. Масалан, дар мактубҳои кутоҳе, ки дар он таъсири атмосфераро дар ҳаракати зебра дар Африко баҳс мекунад. «Из-за озоновых дыр от Занзибары до Замбии и Заира зебры бегают зигзагами». Агар бо истифодаи алгоритми якалифбогӣ рамзгузорӣ карда шавад, тавассути басомади ҳарфҳо рамзкушоии он ғайриимкон аст. Чунки дар ин ҷо ҳарфи “з” нисбат ба нутқи гуфтугӯӣ зиёдтар истифода шудааст. Дар матнҳои техникӣ бошад ҳарфи “ф” нисбати дигар ҳарфҳо баъзан зиёдтар истифода мешавад, чунки калимаҳои функсия, дифференсиал,

диффузия, коэффитсиент ва ғайра бисёртар истифода мешаванд.

Агар пайғоми рамзгузошташуда бо роҳи муайянкунии миқдори такроршавии ҳарфҳо рамзкушои карда нашавад, (агар пайғом хеле кутоҳ бошад) Ал-Киндӣ пешниҳод мекунад, ки хислати якҷоя истифодабарии ҳарфҳо ва ё хислати якҷоя истифодабарии ҳарфҳои мушаххас истифода карда шавад. Масалан, биаграммаҳои (гурӯҳи аз ду ҳарф) дар забони русӣ бисёристифодашаванда: ет, но, ен, то, на, ра, ли, во мебошанд. Статистикаи якҷоя истифодабарии ҳарфҳои садонок ва ҳамсадо хеле муҳим мебошад. Масалан, пеш аз ҳарфҳои ь, ы, ъ, и баъди ҳарфи э метавонад, садонок истифода шавад. Пас аз садонок омадани ҳамсадо эҳтимолияти 87%-ро дорад. Илова бар ин, калимае, ки дар ибтидои мактуб навишта мешавад, нақши калон дорад. Масалан, дар мактубҳои бо забони арабӣ навишташуда, дар ибтидо калимаи “Бисмиллаҳир Раҳманир Раҳим” (Ба номӣ Аллоҳи Бахшояндаи Меҳрубон) навишта мешавад.

Ал-Киндӣ ҷадвали такроршавии ҳарфҳои алифбои арабиро, ки дар асоси матнҳои 7 саҳифа чунин пешниҳод кардааст:

Ҳарф	Басомад	Ҳарф	Басомад	Ҳарф	Басомад	Ҳарф	Басомад
ا	600	ر	155	س	91	ش	—
ل	437	ع	131	ق	63	ض	—

م	320	ف	122	ح	57	خ	—
ه	273	ت	120	ج	46	ث	17
و	262	ب	112	ذ	35	ط	15
ي	252	ك	112	ص	32	غ	15
ن	221	د	92	خ	20	ظ	8

Ал-Киндӣ ҳамчун олими нахустини “басомади криптографӣ” ба ҳисоб меравад. То нимаи асри IX дар дунё фақат методҳои криптографии моноалфавитӣ (дар он ҳар як ҳарфи матни ошкор ба ягон ҳарфи матни рамзгузошташуда, якқиммата иваз карда мешавад), маъмул буданд. Математик ва файласуфи араб Ал-Киндӣ дар корҳои худ методи рамзкушои мактубҳои бо чунин усул рамзгузошташударо бо таври комил оварда, инчунин ба инкишофи рамзгузорӣ рамзи бисёралифбогӣ таъсири зиёд расонидааст. Дар кишварҳои Аврупо рамзи полиалфавитӣ тақрибан дар асри XV ба вуҷуд омадааст.

Дастнависи Ал-Киндӣ то замони мо омада нарасидааст. Аммо то замони мо нусхаи он расидааст, аз китобхонаи Сулаймонии шаҳри Истанбули Туркия ёфт шудааст. Ин нусха дорои хатогиҳои синтаксисӣ ва мавзӯии зиёд мебошад.

Шаҳобуддин Абӯ Аббос Аҳмад ибни Али ибни Аҳмад ал – Қалқашандӣ

Шаҳобуддин Абӯ Аббос Аҳмад ибни Алӣ ибни Аҳмад ал – Қалқашандӣ соли 1355 дар Каир таваллуд шуда, соли 1412 дар Иерусалим вафот кардааст.

Соли 1412 Ал – Қалкашандӣ энсиклопедияи 14 ҷилдаеро навишт[1], ки ҷилди 14-уми он “Шауба ал-Аша” ё “Рисола оиди хондани мактубҳои рамзгузошташуда” ном дошт, ки дар он маълумот оиди 7 методи рамзгузорӣ оварда шудааст.

1) Иваз намудани як ҳарф ба ҳарфи дигар;
2) Навиштани ҳарфҳо бо тартиби дигар;
3) Ба таври баръакс навиштани якчанд ҳарфи калима;
4) Иваз намудани ҳарф бо рақам, бо назардошти иваз намудани ҳарфи арабӣ ба адад;
5) Иваз намудани ҳар як ҳарфи матни ошкор бо ду ҳарфи арабӣ, ки метавон онҳоро ба сифати ададҳое, ки суммаи онҳо ба бузургии ҳарфӣ (рақамӣ) матни кушод баробар мешавад;
6) Ивази ҳар як ҳарф бо номи ягон одам;
7) Истифодаи номи шаҳрҳо, ҳолати сайёраҳо, номи меваҳо, дарахтҳо ва ғайраҳо.

[1] http://www.vostlit.info/Texts/rus17/Al_Kalkasandi/pred2.phtml?id=12555

Нахустин маротиба дар таърихи рамзгузорӣ дар ин инсклопедия руйхати системаҳои ҷойгардонӣ (перестановка) ва ивазкуни (замена) оварда шудааст. Аз ҳама асос нахустин маротиба дар бораи таҳлили криптографӣ тадқиқи шифротекст дар инсклопедияи мазкур сухан рафтааст. Олимони араб ба муайянкунии басомад такроршавии калимаҳо машғул шудаанд. Ҳангоми сохтани вожанома муаллиф пайдоиши басомади ҳарфҳоро ба назар гирифт, инчунин муайян кард, ки кадом ҳарф баъди кадом ҳарф меояд ва кадом ҳарфҳо дар ҳамсоягӣ ҳеҷ вақт вонамехуранд.

10.Диски Алберт

Леон Батист Алберт (1404-1472), математик, архитектор, ва гуманист соли 1466-67 асаре бо номи

“Принсипи кодҳои таркибёфта (De componendis Cypris)” навишт, ки яке аз китобҳои криптографии куҳнатарин дар мамлакатҳои Ғарб ба ҳисоб меравад. Дар ин рисола ибтидо рамзҳои якалифбогии ҷойгузориро таҳлил карда, сипас нахустин ҷадвали басомади ҳарфҳоро сохтааст.

Алберт нахустин касест, ки рамзи бисёралифбогии ҷойгардониро бо номи диски (рамзи) Алберт пешниҳод

кардааст. Дар асари "José Luis Tábara, Breve Historia de La Criptografía Clásica" истифода онро бо шакли зайл тавзеҳ медиҳад:

"Бигузор ду диски мисин, ки яке аз дигараш 1/10 ҳисса калон буда, беҳаракат аст дода шуда бошад. Ҳалқаи дискҳоро ба 24 қисм, ки сектор ном дорад ҷудо карда, дар ҳар як сектори диски калони яктоги ҳамаи ҳарфҳои алифбои лотиниро бо ранги сурх менависем, яъне ибтидо ҳарфи A баъд B ва ҳоказо ба ғайр аз ҳарфи H, K ва якчанд ҳарфи дигар, ки зарурати навиштан надоранд, боқимонда ҳамаи ҳарфҳоро менависем".

Қайд. *Дар алифбои лотинӣ ҳарфҳои «C» ва «K» як овозро ифода карда, аз партофтани ҳарфи "H" маънои калима дигар намешавад***.**

Дар забони лотинӣ ҳарфҳои j, u, w ва y мавҷуд нестанд, аз ин рӯ бо назардошти қайд ҳангоми навиштани ҳарфҳои дар диски калон 4 сектор холӣ мемонад, ки онҳоро бо ададҳои 1, 2, 3, 4 пур мекунем. Айнан ба ҳамин монанд диски хурдро пур мекунем.

"... ҳарфҳои хурдро на аз рӯйи алифбо ҳамчун диски калон, балки бо шакли тасодуфӣ дар диски хурд менависем. Масалан, метавон фарз кард, ки ҳарфи якум a, дуюм c, сеюм e ва ҳоказо мебошанд. Ҳамин тариқ 24 сектор диски хурд бо илова намудани символҳои &, k, h ва

у пур карда мешаванд. Пас аз иҷрои ин амал, диски хурдро дар дохили диски калон тавре мегузорем, ки аз маркази онҳо тири умумие, ки дар атрофи он бояд диски хурд чарх занад гузарад“.

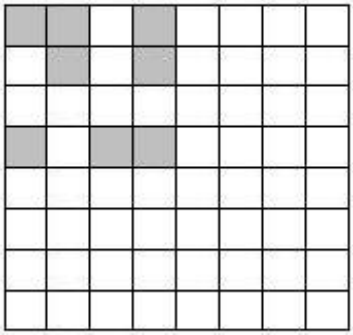
Дар диски хурд ягон ҳарфро интихоб мекунем, масалан k. Пас аз ин диски хурдро тавре ҳаракат медиҳем, ки ҳарфи интихобшуда дар зери ягон ҳарф қарор гирад, масалан B. Ин ҳарфро ба ҷои ҳарфи k дар мактубе, ки бояд рамзгузорӣ кунем менависем.

Ин тарз ҷойгиршавии дискҳоро истифода карда, ҳамаи ҳарфҳои пайғомро мувофиқан ба ҳарфҳои дар диски беруна (калон) навишташуда иваз мекунем. Пас аз навиштани се ё чор мактуб метавон ҳолати ҷойгиршавии дискҳоро тавре иваз кард, ки ҳарфи k ба ҳарфи D (ё ягон ҳарфи дигар) мувофиқ ояд. Акнун мактубҳои навбатиро аз рӯйи ин ҳолати ҷойгиршавии дискҳо менависем (рамзгузорӣ мекунем).

11.Панҷараи Кардано

Соли 1550 математики итолиёвӣ Ҷ. Кардано (1501-1576) барои рамзгузорӣ ва рамзкушои кардани мактубҳои бисёр муҳим воситаи рамзгузорие сохт, ки бо номи

панҷараи Кардано [1] маъмул аст. Панҷараи мазкур шакли росткунҷавӣ ё квадратӣ дошта, аз картони одӣ, пергамент ва ё метали пластикии тунук сохта мешавад, ки дорои якчанд сурохи мебошад. Дар ҳар як сурохии он имконияти навиштани як символ ва ё як калима мавҷуд аст. Одатан миқдори чунин панҷара вобаста ба миқдори тарафҳо сохта мешаванд. Якчанд усули рамзгузорӣ тавассути панҷараи Кардано мавҷуд аст. Дар ин ҷо усули содатарини онро меорем. Бо назардошти тарафҳо бигузор чунин панҷара сохта шуда бошад:



дар ин ҷо катакчаҳои ранги хокистарӣ дошта, сурохиҳои панҷарарро ифода мекунанд.

Пас аз оне, ки панҷара сохта шуд, барои рамзгузорӣ онро дар болои варақе, ки дар он бояд матни рамзгузошташуда навишта шавад, гузошта мешавад. Дар

[1] https://en.wikipedia.org/wiki/Cardan_grille

варақи мазкур низ монанди панҷара раҳҳои амудӣ ва уфуқӣ тавре, кашида мешаванд, ки андозаи ҳар як катакча ба андозаи катакчаҳои панҷара (катакчаҳое, ки дар онҳо танҳо як символ навиштан мумкин аст) мувофиқ оянд.

Мисол. Бо истифода аз панҷараи сохтаамон матни "Шифрование с помощью решетки Кардано"-ро рамзгузорӣ мекунем.

Барои иҷрои ин амал панҷарарро дар болои варақ гузошта як қисми матнро менависем:

ш	и		ф				
	р		о				
в		а	н				

Пас аз навиштани як қисми матн панҷарорарро 90^0 ё 180^0 тоб дода, дар катакчаҳои холӣ қисми дигари матнро менависем:

ш	и		ф	и			е
	р		о			с	п
				о			
в		а	н	м		о	щ

Агар амали 90^0 тобдиҳии панҷарараро ду маротибаи дигар такрор кунем, шакли зерин ҳосил мешавад:

ш	и		ф	и			е
	р		о			с	п
				о			
в		а	н	м		о	щ
и	к		а	ь	ю		р
			р				
д	а			е		ш	
н			о	е		т	к

Қадами навбати панҷарараро аз рӯйи варақ гирифта, дар катакчаҳои холӣ ҳарф (символ) –ҳои дилхоҳе то пуршавии ҷадвал менависем. Дар натиҷа матни додашуда ба сурати зерин рамзгузорӣ карда мешавад:

ш	и	к	ф	и	т	с	е
м	р	в	о	п	а	с	п
в	и	р	а	о	ц	ф	ю
в	я	а	н	м	п	о	щ
и	к	ц	а	ь	ю	э	р
и	с	х	р	г	л	е	х
д	а	ю	ж	е	ы	ш	з
н	ч	й	о	е	й	т	к

Қайд. *Ҳангоми тоб додани панҷараи Кардано бояд диққат дод, ки ду ҳарф болои ҳам наоянд.*

Саволҳо барои мустаҳкамкунӣ

1) Кадом мафҳуми асосии криптографияро медонед?
2) Таърихи криптография чанд марҳиларо дарбар мегирад?
3) Рамзи Атбаш чӣ гуна рамз аст?
4) Сохти асбоби скитал чӣ гуна буд?
5) Диски Энея бо чи мақсад сохта шуд?
6) Тарзи рамзкушоии диски Энея чӣ гуна аст?
7) Моҳияти асоси квадрати Полиби аз чӣ иборат аст?
8) Рамзи Сезар чӣ гуна рамз аст ва аз рамзҳои пешина чӣ фарқ мекунад?
9) Тараққиёти рамзгузорӣ дар мамолики машриқ чӣ гуна буд?
10) Ки аввалин шуда, ҷадвали басомади ҳарфҳоро сохт?
11) Бо кадом усул дар машриқ рамзшиканӣ мекарданд?

12) Дар кишварҳои Шарқ кадом китобҳои оиди криптография навишта шудааст?
13) Диски Алберт чӣ гуна диск буд ва чӣ тавр итилоот тавасути он рамзгузорӣ мешуданд?
14) Моҳияти асосии панҷараи Кардано аз чӣ иборат аст?
15) Тавассути панҷараи Кардани чӣ тавр рамзгузорӣ сурат мегирифт?

Боби 7. Рамзҳои бисёралифбогӣ ва математикӣ

1. Рамзи Гронсфилд

Рамзи мазкур модификатсияи рамзи Сезар буда, дар он калид на аз як адад, балки аз пайдарпайии рақамҳо иборат мебошад. Барои рамзгузории итилоот ибтидо ҳамаи ҳарфҳои алифбо сар карда аз 1 рақамгузоӣ карда мешаванд, сипас ҷадвали дорои 3 сатр ва n сутун сохта шуда, дар сатри якуми ҷадвал ҳарфҳои матни ошкор ва дар сатри дуюм рақамҳои калид навишта мешаванд. Агар дарозии калид аз дарозии матни ошкор кутоҳ бошад, калидро якчанд маротиба пайдарпай то баробар шудан ба матни ошкорро менависем. Барои ҳосил намудани элементҳои сатри сеюм, қимати ададии ҳар як ҳарфи сатри якумро ба қимати мувофиқи калид ҷамъ карда, сипас барои натиҷаи ҳосилшуда ҳарфи ба он мувофиқро менависем.

Умуман якчанд усули рамзгузорӣ тавассути методи мазкур мавҷуд аст, ҳоло бо мисоле яке аз ин усулҳоро дида мебароем.

Мисол. Бо истифода аз калиди 1234 матни DONISH рамзгузорӣ карда шавад. Алгоритми рамзгузорӣ чунин аст:

Ҷадвали дорои се сатр ва 6 сутун тасвир мекунем.

Матни ошкор						
Калид						
Матни рамзгузошташуда						

Дар сатри якуми ҷадвал ҳарфҳои матни ошкор ва дар сатри дуюм рақамҳои калид навишта мешаванд. Азбаски дарозии калид аз дарозии матн хурд аст, бинобар ин рақамҳои калидро то баробар шудан ба матни ошкор такроран менависем.

Матни ошкор	D	O	N	I	S	H
Калид	1	2	3	4	1	2
Матни рамзгузошташуда						

Барои ҳосил намудани сатри сеюм қимати ададии (рақами тартибӣ) ҳарфҳои сатри якумро бо қимати калид ҷамъ карда, ҳарфи ба адади ҳосилшударо мувофиқро менависем. Бо суханҳои дигар дар сатри сеюм ҳарферо менависем, ки сар карда аз ҳарфи матни ошкор k мавқеъ дар тарафи рости алифбо ҷойгир аст. Дар ин ҷо k рақами ба ҳарфи додашуда мувофиқи ҳарфи матни ошкор аст. Азбаски дар алифбо ҳарфе, ки пас аз як мавқеи ҳарфи D ҷойгир аст, ҳарфи E мебошад, бинобар ин, дар катакчаи якуми сатри сеюм ҳарфи E - ро менависем. Дар катакчаи дуюм бошад, ҳарферо менависем, ки дар алифбо чор ду дар тарафи рости ҳарфи Q ҷойгир аст. Ин ҳарф S аст. Ҳамин тариқ ҳамаи катакчаҳои сатри сеюмро пур мекунем.

Матни ошкор	D	O	N	I	S	H
Калид	1	2	3	4	1	2
Матни рамзгузошташуда	E	Q	Q	M	T	J

Бо ҳамин минвол матни лозимӣ рамзгузорӣ карда мешавад.

Модели математикии рамзгузоӣ ва рамзкушои тавассути методи Гронсфилд мувофиқан чунин шакл доранд:

$$C_i = (P_i + K_i)\ mod\ n \qquad (1),$$

$$P_i = (C_i - K_i + n) mod\ n \qquad (2).$$

Илова бар ин, барои рамзгузоӣ метавон аз ҷадвали Гронсфилд истифода кард, ки шакли зеринро дорад:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Қайд. *Тарзи истифодаи ин ҷадвал хело сода мебошад. Масалан, барои ба калиди 1 рамзгузорӣ кардан ҳарфи S ҳарферо мегирем, ки дар бурриши сатри 1 ва сутуни S ҷойгир аст. Ин ҳарфи T аст.*

Барномаи рамзгузории методи Гронсфилд дар забони C#:

```
string key = "2015", text = "gronsfeld";
string abc = "abcdefghijklmnopqrstuvwxyz", newKey =
key, result = "";
bool encode = true;
int op = encode ? +1 : -1, offset, indexOf = 0;
while (newKey.Length < text.Length)
{
   newKey += key;
}
if (newKey.Length > text.Length)
{
   newKey = newKey.Substring(0, newKey.Length -
(newKey.Length - text.Length));
}
for (int i = 0; i < text.Length; i++)
{
   indexOf = abc.IndexOf(text[i]);
   if (indexOf != -1)
   {
   offset = abc.IndexOf(text[i]) +
(Convert.ToInt32(newKey[i]) - 48) * op;
      if (offset > abc.Length)
         offset = offset - abc.Length;
      else if (offset < 0)
         offset = abc.Length + offset;
```

```
        result += abc[offset];
    } else
        result += text[i];
}
```

2. Рамзи Тритемия

Тавре медонем, дар рамзҳои ивазкунӣ (замена) – и сода барои калиди қайдкардашудаи k дилхоҳ ҳарфи матни кушода ба яке аз ҳарфҳои алифбое, ки тавассути он навишта шудааст ё алифбои дигар иваз карда мешавад. Аз ин рӯ рамзи ивазкунии содаро метавон ба таври осон бо ҳисобкунии басомади ҳарфҳои матни рамзгузошташуда шикаст. Қайд кардан ба маврид аст, ки дар алифбоҳои гуногун як ҳарф метавонад бо басомадҳои гуногун истифода шавад.

Дар асри XVI олими немис Иоганн Тритемия [1] (аксари таърихнигорон онро падари дуюми криптография меноманд) дар китоби панҷуми силсилаи “Poligraphia” чопи соли 1518 методи рамзгузории наверо пешниҳод намудааст, ки дар он ҳар як ҳарфи оянда тавассути рамзи хусусии лағжиш рамзгузорӣ карда мешаванд. Барои ин Тритемия ҷадвалеро фикр карда баромад, дар сатри

[1] https://en.wikipedia.org/wiki/Johannes_Trithemius

якуми он ҳарфҳои алифбо бе тағйир навишта шуда, дар сатри дуюм сар карда аз ҳарфи дуюми алифбо то охир ва баъд ҳарфи якум (лағжиши даври як мавқеъ ба тарафи рост) навишта мешуд. Ҳамин тариқ, дар ҳар сатри минбаъда алифбо як мавқеъ ба тарафи рост ба таври даврӣ (кучонида шуда) навишта мешаванд. Масалан, барои алифбои лотинӣ ин ҷадвал шакли зеринро дорад:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X
Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y
W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z

Алгоритми рамзгузорӣ тавассути ин ҷадвал чунин аст: Агар ҳарфи матни ошкор дар сатри якум дорои координатаи (1, j) бошад, (дар ин ҷо j-рақами тартибии сутунро ифода мекунад) он гоҳ дар сатри і-юм он бо ҳарфе ки дорои координатаи (і, j) аст иваз карда мешавад (і-рақами тартибии ҳарф дар матн). Бо суханҳои дигар ҳарфе, ки дар сатри якум дорои рақами тартибии j мебошад, бо ҳарфи j-юми сатри і иваз карда мешавад. Пас

аз оне, ки сатри охирон истифода карда шуд, боз ба сатри якум бармегардем. Бо ин усул як ҳарфи матни кушод метавонад бо ҳарфҳои гуногун иваз карда шавад.

Мисол. Матни МАКТАВ-ро бо истифода аз ҷадвали Тритемия рамзгузорӣ мекунем.

Ҳал. Ҳарфи якуми матн М бе тағйир гузошта шуда, ҳарфи дуюм А бо ҳарфи В, ҳарфи сеюм К бо ҳарфи М, ҳарфи чорум Т бо ҳарфи У, ҳарфи панҷум А бо ҳарфи Е, ҳарфи шашум Б бо ҳарфи G иваз карда мешавад. Дар натиҷа матни рамзгузошташуда шакли "MBMYEG"– ро мегирад.

Тавре ки дида мешавад, калид дар ин метод вуҷуд надорад. Баъзан варианти душвори методи мазкурро ҳангоми бо тартиби тасодуфӣ ҷойгиркунии тартиби ҳарфҳо ва интихоби усули душвори тартиби сатрҳо истифода кардан мумкин аст.

3. Рамзи Виженер

Рамз ё квадрати Виженер аз тарафи олими фаронсавӣ Блейз де Виженер) (Blaise de Vigenere[1]) соли

1585 сохта шудааст, ки монанди ҷадвали Тритемия ба таври даври кучонидани ҳарфҳои алифбо ҳосил карда мешавад, яъне дар сатри якуми ҷадвал ҳарфҳои алифбо

[1] https://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re

бетағйир навишта мешаванд. Сатри і-юми ҷадвал аз сатри і-1 –ум бо тариқи даври лағжонидан ба як мавқеъ ҳосил карда мешавад. Дар сатри якум ҳарфҳои алифбо метавонанд аз рӯйи тартиб ва ё ба таври тасодуфӣ ҷойгир карда шаванд. Фарқияти асосии ҷадвали Виженер аз ҷадвали Тритемия дар он аст, ки дар ҷадвали Виженер як сатр ва як сутуни иловагӣ мавҷуд аст, ки мувофиқан барои ифодакунии алифбои матни кушод ва алифбои калид истифода бурда мешаванд. Илова бар ин дар рамзи Виженер метавон аз калид низ истифода кард. Калид аз пайдарпайии ҳарфҳои алифбое, ки тавассути он ҷадвал сохта шудааст, иборат мебошад. Агар дарозии калид аз дарозии матни ошкор хурд бошад, он гоҳ калид ба таври даврӣ то ба дарозии матни ошкор баробар шудан навишта мешавад.

Ҷадвали Виженер барои алифбои лотинӣ шакли зеринро дорад:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Тавре ки дида мешавад дар ин ҷадвал 26 рамзи гуногуни Сезар мавҷуд аст. Қоидаи рамзгузории методи мазкур чунин аст: Агар ҳарфи матни кушод дорои координатаҳои (1, j) (дар ин ҷо j-рақами тартибии сутунро ифода мекунад) ва ҳарфи калид дорои координатаҳои (i,1) бошад, он гоҳ ба сифати ҳарфи матни рамзгузошташуда, ҳарфе интихоб карда мешавад, ки дорои координатаҳои (i, j) аст. Дар ин ҷо фарз карда мешавад, ки ҳар як символи матни кушод ба як символи калид мувофиқат гузошта мешавад.

Мисол. Матни MAKTAB-ро бо истифода аз ҷадвали Виженер ва калиди DARS рамзгузорӣ мекунем:

Ҳал. Азбаски дарозии калид аз дарозии матни ошкор хурд мебошад, бинобар ин, аввал калидро якчанд

маротиба навишта, дарозиашро ба матни ошкор баробар мекунем:

Матни ошкор: MAKTAB

Калид: DARSDA

Пас аз оне ки дарозии калид бо дарозии матни ошкор баробар шуд, матни ошкорро рамзгузорӣ мекунем.

Азбаски ҳарфи якуми матни кушод M дорои координатаҳои (1,13) ва ҳарфи якуми калид D дорои координатаҳои (4,1) мебошад, бинобар ин ҳарфи M-ро бо ҳарфи дорои координатаҳои (4, 13), яъне P иваз мекунем. Ҳарфи дуюми матни ошкор A бошад, дорои координатаҳои (1,1) буда, ҳарфи дуюми калид A низ дорои координатаҳои (1,1) мебошад, аз ин рӯ онро бетағйир мегузорем. Ба ҳамин монанд ҳамаи ҳарфҳои матни ошкор рамзгузорӣ карда мешаванд. Дар натиҷа матни рамзгузошташуда ба сурати “PABLDB” ҳосил мешавад.

Модели математикӣ

Агар ҳамаи ҳарфҳои ягон алифборо сар карда аз 0 рақамгузорӣ кунем, он гоҳ формулаҳои рамзгузорӣ ва рамзкушоӣ мувофиқан ба сурати зерин ҳосил карда мешаванд:

$$C_i = (P_i + K_i)\ mod\ n, \qquad (1)$$

$$P_i = (C_i - K_i + n) mod\ n. \qquad (2)$$

Қайд кардан ба маврид аст, ки рамзи Виженер якчанд маротиба сохта шудааст. Нахустин маротиба ин методро

Ҷован Баттист Беллазо (итал. Giovan Battista Bellaso) дар китоби “La cifra del. Sig. Giovan Battista Bellaso” соли 1553 навиштааст. Аммо дар асри XIX номи дипломати фаронсавӣ Блез Виженер гирифт.

Барномаи рамзгузории методи Виженер ар забони C++

```
string  crypt(string S, string K){
  int i, T, m, n;
  m = S.size();
  n = K.size();
  for (i = 0; i < m; i++){
          T = ((int)S[i] + (int)K[i % n]) % 26;
          S[i] = (char)(T + 65);
 }
 return S;
}
```

4. Рамзи Плейфер

Рамзи Плейфер ё квадрати Плейфер[1] соли 1854 аз тарафи физикдони англис Чарлз Уитсон сохта шудааст. Азбаски дӯсти Уитсон Лорд Леон Плейфер ин рамзро дар корҳои давлатии Англия бисёр истифода бурдааст, бинобар ин, бо номи Рамзи Плейфер маъмул мебошад.

Чарл Уитсон

[1] https://en.wikipedia.org/wiki/Playfair_cipher

Рамзи мазкур матритсаи дорои 5 сатр ва 5 сутунро (барои алифбои лотинӣ) истифода мебарад, ки дорои калид ва ҳарфҳои алифбо мебошад. Барои сохтани ҷадвал ва истифодаи рамз бояд калид ва чор қоидаи асосиро дар ёд гирифт. Ибтидо дар ҷадвал ҳарфҳои калид бе такроршавӣ ва ҳарфҳои боқимондаи алифбо, ки дар калид вуҷуд надоранд, навишта мешаванд. Ҳарфҳои калидро метавон дар сатри нахустин ва ё ба таври ихтиёрӣ аз кунҷи чапи болоӣ ба марказ навишт. Одатан дар ҳангоми сохтани ҷадвали барои алифбои лотинӣ ҳарфи Q сарфи назар карда мешавад ва ё ҳарфҳои I ва J дар як катакча навишта мешаванд.


Лорд Леон Плейфер

Барои рамзгузорӣ ибтидо матн ба биаграммаҳо (гурӯҳои иборат аз ду символ) ҷудо карда мешавад. Масалан, матни «Hello World» пас аз ҷудокунӣ шакли «HE LL OW OR LD» -ро соҳиб мешавад. Пас аз оне ки матн ба биаграммаҳо ҷудо карда шуд, аз қоидаҳои зерин истифода бурда мешавад:

1) Агар ду символи биаграмма бо ҳамдигар монанд бошанд, (ё дар охир як символ боқи монад), он гоҳ пас аз символи якум ҳарфи X (баъзан Q) илова карда, мешавад. Пас аз ин ҷуфти нави символҳоро рамзгузорӣ

карда амали рамзгузориамонро давом медиҳем. Масалан, калимаи Balloon ба сурати Ba-lx-lo-on ҷудо карда мешавад.

2) Агар символҳои биаграмаи матни кушод дар як сатр хобанд, он гоҳ ин символҳо мувофиқан ба символҳои тарафи росташон иваз карда мешаванд. Агар ягонто аз ин символҳо дар охири сатр ҷойгир бошад, он гоҳ ба символи аввалаи сатр иваз карда мешавад.
3) Агар символҳои биаграммаи матни кушод дар як сутун хобанд, он гоҳ ин символҳо мувофиқан ба символҳои дар поёнашон ҷойгирбуда иваз карда мешаванд. Агар ягонто аз ин символҳо дар охири сутун ҷойгир бошад, он гоҳ ба символи аввалаи сутун иваз карда мешавад.
4) Агар символҳои биаграмма дар сатр ва сутунҳои гуногун ҷойгир бошанд, он гоҳ ба символҳои ҳамон сатр, ки дар кунҷҳои дигари ин ҷадвал ҷойгиранд, иваз карда мешаванд.

Барои рамзкушоӣ бошад, аз инверсияи ин қоидаҳо истифода бурда шуда, ҳарфи зиёдатии X (Q) аз матн нест карда мешавад. Ҳоло бо мисоле ҳамаи ин қоидаҳоро нишон медиҳем. Масалан, барои рамзгузорӣ кардани биаграммаи OR чор қоидаи (ҳолати) асосиро дида мебароем.

1)	2)	3)	4)
* * * * * * O Y R Z * * * * * * * * * * * * * * * OR бо YZ иваз карда мешавад	* * O * * * * B * * * * * * * * * R * * * * Y * * OR бо BY иваз карда мешавад	Z * * O * * * * * * * * * * * R * * X * * * * * * OR бо ZX иваз карда мешавад	* * * * * * * * * * Y O Z * R * * * * * * * * * * OR бо ZY иваз карда мешавад

Акнун мисоли содаеро дида мебароем.

Мисол. Бигузор калимаи калид DAFTAR ошад, он гоҳ ҷадвали зеринро ҳосил мекунем:

D	A	F	T	R
B	C	E	G	H
I	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

Матни «HALLI MASALA»-ро рамзгузорӣ мекунем. Барои рамзгузорӣ намудан ибтидо матнро бо биаграммаҳо тақсим мекуне: HA LL IM AS AL A

Аз баски дар биаграммаи дуюм ду ҳарфи L пайдарпай омадааст, бинобар ин, дар байни онҳо ҳарфи X- ро гузошта, давоми матро аз нав ба биаграммаҳо тақсим мекунем.

HA LX LI MA SA LA

Акнун қоидаҳои дар боло овардашуда ва ҷадвали сохтамонро истифода бурда ҳар як биаграммаро пайдарпай рамзгузорӣ мекунем:

Матни ошкор: HA LX LI MA SA LA
Матни рамзгузошташуда: RC QF MK TK TP FK

Ҳамин тариқ матни « HALLI MASALA» ба сурати «RCQFMKTKTPFK» рамзгузорӣ карда шуд.

5. Рамзи Вернам

Рамзи Вернам[1] соли 1917 аз тарафи кормандони ширкати полиграфии AT&T (Амрико) Гилберт Вернам ва Мейджор Ҷозеф Моборн сохта шудааст. Ибтидо онҳо ақидаи ба таври автоматӣ рамзгузорӣ намудани пайғомҳои телеграфиро бо истифода аз кодҳои телетайпии Бодо, яъне «комбинатсияи импулсӣ» панҷқимата пешниҳод карда буданд. Масалан, комбинатсияи («– – – + +») ҳарфи А-ро ифода намуда, комбинатсияи («+ + – + +») бошад, символи гузариш аз ҳарф ба рақамро ифода менамояд.

[1] https://en.wikipedia.org/wiki/One-time_pad

Дар лентаи коғазӣ ҳангоми кор бо телетайп аломати «+» мавҷудияти сурохӣ ва аломати «–» мавҷуд набудани онро ифода мекунад.

Вернам ба таври электромеханикӣ аз рӯйи координатҳо ҷамъ намудани импулсҳои матни кушодро бо истифода аз импулсҳои гамма, ки қаблан дар лента насб карда шуда буданд, пешниҳод кард. Амали ҷамъ аз рӯйи модули 2 иҷро карда мешавад, ки чунин амалкард дорад:

$\oplus$	0	1
0	0	1
1	1	0

Қайд. *Дар ин ҷо гамма гуфта символҳои калид дар назар дошта мешаванд. Агар дарозии калид аз дарозии матн хурд бошад, он гоҳ такроран чанд маротиба то ба андозаи матн баробар шудан символҳои онро менависем.*

Барои моҳияти ин методро дарк кардан ибтидо амали хог-ро дар забони Паскал дида мебароем.

Амали ё (хог)-амали кор бо битҳо буда, ба қимати ҳақ доро аст, агар танҳо қимати яке аз амалвандҳои додашуда ҳақ бошад, яъне:

x	y	$x\ xor\ y$
1	1	0
0	1	1
1	0	1
0	0	0

Мисол. Бигузор x=25 ва y=45 бошад. Онҳоро ба намуди системаи дӯӣ мегардонем:

x	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1
y	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
x xor y	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0

Аз ин ҷо x xor y=25 xor 45=52 мешавад.

Умуман, формулаҳои математикии рамзгузорӣ ва рамзкушоии рамзи Вернам шакли зеринро доранд:

$$C_i = P_i \oplus K_i, \qquad (1)$$

$$P_i = C_i \oplus K_i. \qquad (2)$$

Дар ин ҷо амали $\oplus$ амали XOR- ро ифода мекунад.

Соли 1945 К. Шеннон устувории математикии рамзи Вернамро исбот намуд.

Қайд кардан ба маврид аст, ки рамзи гаммиронидашударо солҳои 20-ум олмониҳо дар корҳои дипломатии худ, англисҳо ва амрикоиҳо дар ҷанги дуюми ҷаҳони истифода карданд.

6. Рамзи Хилл

Рамзи Хилл [1] рамзи полиграмии ҷойгардонӣ [2] буда, метавонад, дар як вақт як блоки матнро бо истифода аз алгебраи хаттӣ ва арифметикаи бақияҳо рамзгузорӣ

[1] https://en.wikipedia.org/wiki/Hill_cipher

[2] Рамзи полиграмии ҷойгардонӣ рамзест, ки як бора на як символ балки як гурӯҳи символҳоро рамзгузорӣ (рамзкушой) мекунад.

кунад. Рамзи мазкур соли 1929 аз тарафи математики амрикой Лестер Хилл сохта шудааст. Ибтидо Хилл ин рамзро моҳи июн-июли ҳамон сол дар мақолаи «Cryptography in an Algebraic Alphabet» дар журнали «The American Mathematical Monthly» чоп намуд. Моҳи августи ҳамон сол Хилл дар штати Колорадо (Боулдере) пеши ҷамъияти математикони Амрико ин рамзро муаррифӣ намуд (баромад кард). Баъдтар моҳи марти соли 1931 Хилл бо номи «Concerning Certain Linear Transformation Apparatus of Cryptography» дар журнали «The American Mathematical Monthly» мақолаеро чоп намуд.

Рамзи Хилл нахустин рамзест, ки дар амалия барои якбора рамзгузории зиёда аз се символ истифода шуд (ҳарчанд ки бо душворӣ). Рамзи мазкурро бо иллати заъиф будани устуворӣ ва мавҷуд набудани алгоритми ҳосил намудани матритсаи рост ва баръакс дар амалия бисёр истифода нашуд.

Ҳангоми истифодаи методи Хилл ибтидо ҳарфҳои алифбо сар карда аз 0 рақамгузорӣ карда мешаванд. Блоки иборат аз n ҳарф ҳамчун вектори n – ченака ба назар гирифта шуда, бо матритсаи квадратии тартиби n аз рӯйи модули M (M-миқдори ҳарфҳои алифбо, масалан барои алифбои лотинӣ M=26 мебошад) зарб карда мешавад. Дар

ин ҷо элементҳои матритсаи квадратӣ аз символҳои (рақами символҳои) калид тартиб дода мешаванд. Матритсаи квадратӣ тавре интихоб карда мешавад, ки дар $\mathbb{Z}_M$ барои он матритсаи баръакс вуҷуд дошта бошад. Дар сурати акс, матни рамзгузошташударо рамзкушои кардан ғайриимкон мегардад.

Ҳангоми n = 3 будан, барои алифбои лотинӣ метавон системаро ба сурати зерин навишт:

$$\begin{cases} c_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 \ (mod\ 26) \\ c_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 \ (mod\ 26) \\ c_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 \ (mod\ 26) \end{cases}$$

Агар ин системаро ба сурати матритсавӣ нависем шакли зеринро мегирад:

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} (mod\ 26)$$

ё

$$C = KP\ (mod\ 26)$$

дар ин ҷо P ва C — векторҳои сутунии дорои се элемента буда, мувофиқан матни ошкор ва рамзгузошташударо ифода мекунанд. K — матритсаи 3x3 буда калидро ифода мекунад. Барои ин мисол ҳамаи амалҳо аз рӯйи модули 26 иҷро карда мешаванд.

Барои рамзкушоӣ намудан матни рамзгузошта ибтидо матритсаи баръакс ба K, яъне K^{-1} ҳисоб карда

мешавад. Тавре медонем барои матритсаи додашуда матритсаи баръакс ҳамон вақт мавҷуд аст, агар муайянкунандаи матритса аз 0 фарқ карда, бо асоси модул тақсимкунандаи умумӣ надошта бошанд, яъне бо модул байнан сода бошад. Дар ҳолати мавҷуд набудани матритсаи баъакс истифодаи матриса дар методи Хилл ғайриимкон аст. Аз ин рӯ, матритсаи дигар бояд тартиб дода шавад, яъне калиди нав бояд интихоб карда шавад.

Дар ҳолати умумӣ алгоритмҳои рамзгузорӣ ва рамзкушоӣ методи Хилл мувофиқан шакли зеринро доранд:

$$C = E(K, P) = KP \ (mod\ 26),$$
$$P = D(K, C) = K^{-1}C \ (mod\ 26) = K^{-1}KP \ (mod\ 26) = P$$

Пеш аз рамзгузорӣ намудан, ибтидо дар ҷадвале, ҳарфҳои ягон алифбо, масалан, лотиниро мувофиқан бо кодҳояшон (рақамҳои тартибӣ) менависем.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Мисол. Матни “MAKTAB” – ро бо истифода аз калиди “OMUZGORON” рамзгузорӣ мекунем. Аз ҳарфҳои (коди ҳарфҳои) калид матритсаи квадратии K – ро ҳосил мекунем:

$$K = \begin{bmatrix} O & M & U \\ Z & G & O \\ R & O & N \end{bmatrix} = \begin{bmatrix} 79 & 77 & 85 \\ 90 & 71 & 79 \\ 82 & 79 & 78 \end{bmatrix}$$

Муайянкунандаи маритсаи K–ро меёмем.

$$|K| = \begin{vmatrix} 79 & 77 & 85 \\ 90 & 71 & 79 \\ 82 & 79 & 78 \end{vmatrix} = 12209.$$

Барои матритсаи K матритсаи баръакс вуҷуд дорад, чунки муайянкунандаи асосии он аз 0 фарқ карда, бо модул (26) байнан сода аст. Акнун матни додашударо бо блокҳои иборат аз 3 символ ҷудо карда, пайдарпай ҳар як блокро рамзгузорӣ мекунем. Аз баски коди ҳарфи 'M' = 12, 'A' =0 ва 'K' = 10 мебошад, бинобар ин, се ҳарфи аввалаи матн ба намуди векторӣ шакли зеринро мегиранд:

$$P_1 = \begin{bmatrix} M \\ A \\ K \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \\ 10 \end{bmatrix}.$$

Акнун ин векторро бо калид аз рӯи модули 26 зарб карда ҳосил мекунем:

$$C_1 = KP_1 (mod\ 26) = \begin{bmatrix} 79 & 77 & 85 \\ 90 & 71 & 79 \\ 82 & 79 & 78 \end{bmatrix} \begin{bmatrix} 12 \\ 0 \\ 10 \end{bmatrix} (mod\ 26)$$

$$= \begin{bmatrix} 1798 \\ 1870 \\ 1764 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 4 \\ 24 \\ 22 \end{bmatrix}.$$

Вектори рамзгузошташуда шакли “EYW” –ро соҳиб мешавад. Акнун матни “TAB” –ро ба сурати вектори менависем:

$$P_2 = \begin{bmatrix} T \\ A \\ B \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \\ 1 \end{bmatrix}.$$

Барои рамзгузорӣ намудан, ин векторро низ бо матрисаи К зарб мекунем:

$$C_2 = KP_2(mod\ 26) = \begin{bmatrix} 79 & 77 & 85 \\ 90 & 71 & 79 \\ 82 & 79 & 78 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \\ 1 \end{bmatrix} (mod\ 26)$$

$$= \begin{bmatrix} 1586 \\ 1789 \\ 1636 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 0 \\ 21 \\ 24 \end{bmatrix}.$$

Ин вектор матни рамзгузошташудаи “AVY”-ро мувофиқ меояд. Пас аз рамзгузорӣ намудани ҳамаи блокҳо онҳоро пасиҳам менависем, ки дар натиҷа матни рамзгузошташудаи “EYWAVY” - ҳосил мешавад.

Рамзкушоӣ

Барои рамзкушӣ намудан, ибтидо матритсаи баръакси К – ро ҳисоб мекунем:

$$K^{-1}\ (mod\ 26) = \begin{bmatrix} 19 & 23 & 24 \\ 2 & 12 & 9 \\ 20 & 17 & 9 \end{bmatrix}.$$

Матни рамзгузошташудаи “EYWAVY”-ро низ ба блокҳо тақсим карда, рамзкушоӣ мекунем. Ба сифати намуна блоки “EYW”-ро рамзкушоӣ мекунем.

$$P_1 = K^{-1}C_1(mod\ 26) = \begin{bmatrix} 19 & 23 & 24 \\ 2 & 12 & 9 \\ 20 & 17 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 24 \\ 22 \end{bmatrix} (mod\ 26) =$$

$$\begin{bmatrix} 1156 \\ 494 \\ 686 \end{bmatrix} (mod\ 26) = \begin{bmatrix} 12 \\ 0 \\ 10 \end{bmatrix}.$$

Ин вектор ба матни “MAK” мувофиқ меояд. Ба ҳамин монанд, қисми дуюми матни рамзгузошташуда, рамзкушоӣ карда мешавад.

Барномаи методи рамзгузории Хилл дар C++:

```
#include <string.h>
#include <iostream>
using namespace std;
//функсия барои ҳисобкунии дарозии массив
unsigned int Lenght(const char s[])
{
	int L = 0;
	while (s[L++]);
	return (L - 1);
}
//Функсия барои ҳисобкунӣ аз рӯйи модули 26
unsigned short mod26(int c)
{
	if (c>0)
	{
		unsigned int c2 = c / 26;
		return c - (26 * c2);
	}
	if (c<0)
	{
		unsigned int c2 = abs(c) / 26 + 1;
		return c + (26 * c2);
	}
```

```
        return 0;
}
double determ(int** Arr, int size)
{
        int i, j;
        double det = 0;
        int** matr;
        if (size == 1)
        {
                det = Arr[0][0];
        }
        else if (size == 2)
        {
  det = Arr[0][0] * Arr[1][1] - Arr[0][1] * Arr[1][0];
        }
        else{
                matr = new int*[size - 1];
                for (i = 0; i<size; ++i){
                        for (j = 0; j<size - 1; ++j)
                        {
                                if (j<i)
                                        matr[j] = Arr[j];
                                else
                                matr[j] = Arr[j + 1];
                        }
det += pow((double)-1, (i + j))*determ(matr, size -
1)*Arr[i][size - 1];
                }
```

```
                delete[] matr;
        }
        return det;
}
int _tmain(int argc, _TCHAR* argv[]){
        int size = 3, S = 0, w=0;
        string abc =
"ABCDEFGHIJKLMNOPQRSTUVWXYZ";
        string text = "ARABOVM";
        unsigned short *cript;;
        cript = new unsigned short[text.size()];
        unsigned short *word;;
        word = new unsigned short[text.size()];
        int**key;
        key = new int*[size];
        //Сохтани калид
        for (int i = 0; i < size; ++i)
                key[i] = new int[size];
        while (S == 0){
                for (int i = 0; i < size; ++i){
                        for (int j = 0; j < size; ++j){

                                key[i][j] = rand() % 5 + 1;
                        }
                }
                S = determ(key, size);
        }
        //Хоричкунии калид ба намуди матритса
```

```
        for (int i = 0; i<size; ++i){
                for (int j = 0; j<size; ++j)
                        cout << key[i][j] << ' ';
                cout << endl;
        }
        // Агар дарозии матн каратии 3 набошад, бо илова намудани символи хати поён онро бо 3 каратӣ мекунем
        if (text.size() % 3 != 0){
                while (text.size() % 3 != 0)
                        text += '_';
                cout << text.c_str() << endl;;
        }
        cout << "матни ошкор:"<<text.c_str() << endl;
//то ҳол массиви text ба охир нарасидааст
while (w <= text.size()){
        for (int i = 0; i<25; i++){
//ба массиви word қимати ададдии коди ҳарфро мебахшем
                        if (text[w] == abc[i])
                                word[w] = i;
                }
                w++;
        }
        cout << "Ба даст оварии shifr ба намуди қисматҳо ба 3 тақсимшуда" << endl << " " << endl;
        //Зарби матритсаи key ба вектори slova аз рӯйи mod 26
```

```
        for (int k = 0; k<text.size(); k += 3){
                for (int i = 0; i<3; i++){
        cript[i + k] = mod26(key[i][0] * word[0 + k] +
key[i][1] * word[1 + k] + key[i][2] * word[2 + k]);
                        cout << cript[i + k] << " ";
                }
                cout << endl;
        }
        cout << " Хориҷкунии шифр ба намуди массиви
сатрӣ:" << endl;
        for (int i = 0; i<text.size(); i++)
        cout << cript[i] << "=" << abc[cript[i]] << endl;
        cin.get();
        return 0;
}
```

7. Рамзи Афинавӣ

Рамзи Афинавӣ [1] – ин ҳолати умумии рамзи моноалфавитии ивазкунӣ мебошад. Дар рамзи мазкур ҳар як ҳарфи алифбо бо як ададӣ бутуни фосилаи [0, m-1] мувофиқ гузошта мешавад. Дар ин ҷо m миқдори ҳарфҳои алифборо ифода мекунад. Сипас, тавассути арифметикаи бақияҳо барои ҳар як ададе, ки ба як символи матни кушода мувофиқ меояд, ададӣ нав ҳисоб карда мешавад.

[1] https://en.wikipedia.org/wiki/Affine_cipher

Ададӣ ҳисоб--кардашуда шифротексти куҳнаро иваз мекунад. Функсияи рамзгузорӣ барои ҳар як символ шакли зеринро дорад:

$$E(x) = (ax + b) mod\ m$$

дар ин ҷо m −миқдори ҳарфҳои алифбо буда, a ва b калид ба ҳисоб мераванд. Ададӣ a тавре интихоб карда мешавад, ки бо ададӣ m байнан сода бошанд.

Функсияи рамзкушоӣ бошад шакли зеринро дорад:

$$D(x) = a^{-1}(x - b) mod\ m$$

дар ин ҷо a^{-1} ададӣ ба a аз рӯйи модули m баръакс мебошад, яъне он ададест, ки шарти зеринро қаноат кунонад:

$$1 \equiv aa^{-1}\ mod\ m.$$

Тавре медонем, ададӣ баръакс ба ададӣ a танҳо ҳолате вуҷуд дошта метавонад, ки агар a ва m байнан сода бошанд. Агар ин хосият ба назар гирифта нашавад, амали рамзкушоӣ ғайриимкон мегардад. Ҳоло нишон медиҳем, ки функсияи рамзкушоӣ ба функсияи рамзгузорӣ баръакс мебошад. Дар ҳақиқат

$$\begin{aligned} D\big(E(x)\big) &= a^{-1}(E(x) - b) mod\ m \\ &= a^{-1}\Big(\big((ax + b) mod\ m\big) - b\Big) mod\ m \\ &= a^{-1}(ax + b - b) mod\ m = a^{-1}\ ax\ mod\ m \\ &= x\ mod\ m. \end{aligned}$$

Миқдори имконпазири калидро барои рамзи афинавӣ метавон тавассути функсияи Эйлер $\varphi(m)$ муайян кард.

Рамзгузорӣ

Бигузор ҳамаи ҳарфҳои алифбои лотинӣ бо қимати рақамиашон (рақами тартибиашон) дар ҷадвали зерин гирд оварда шуда бошанд:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Мисол. Талаб карда мешавад, ки матни "DUSHANBE" –ро бо истифодаи ҷадвали дар боло овардашуда ва қиматҳои $a = 3, b = 4$ ва $m = 26$ миқдори ҳарфҳои алифбои лотинӣ) рамзгузорӣ карда шавад. Тавре ки қайд кардем, дар ин ҷо танҳо барои ададӣ a маҳдудият (шарт) гузошта мешавад, чунки дар сурати бо ададӣ m байнан сода набудани он рамзкушоӣ ғайриимкон мегардад. Қимати a метавонад яке аз ададҳои {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 , 25} бошад. Қимати b ба таври ихтиёрӣ интихоб карда мешавад. Ҳамин тариқ, барои мисоли мо функсияи рамзгузорӣ шакли зеринро мегирад:

$$E(x) = (3x + 4) mod\ 26$$

Қадами нахустин дар рамзгузорӣ навиштани ададҳои мувофиқи ҳарфҳои матни ошкор мебошад, барои матни додашудаи мо чунин ҷадвал ҳосил карда мешавад:

Матни ошкор	D	U	S	H	A	N	B	E
x	3	20	18	7	0	13	1	4

Акнун барои ҳар як қимати x қимати $(3x + 4)$ –ро ҳисоб карда натиҷаро ба 26 тақсим мекунем ва бақияи тақсимро дар ҷадвали зерин менависем:

Матни ошкор	D	U	S	H	A	N	B	E
x	3	20	18	7	0	13	1	4
$3x+4$	13	64	58	25	4	43	7	16
$(3x+4)\ (mod\ 26)$	13	12	6	25	4	17	7	16

Пас аз иҷрои ин амал, ба ҷои рақамҳои ҳосилшуда ҳарфҳои мувофиқро менависем, дар натиҷа матни рамз-гузошташуда ба сурати "NMGZERHQ" пайдо мешавад. Дар ҷадвали зерин ҳамаи қадамҳои рамзи аффинавӣ оварда шудаанд.

Матни ошкор	D	U	S	H	A	N	B	E
x	3	20	18	7	0	13	1	4
$3x+4$	13	64	58	25	4	43	7	16
$(3x+4) mod\ 26$	13	12	6	25	4	17	7	16
Матни рамзгузошташуда	N	M	G	Z	E	R	H	Q

Рамзкушоӣ

Дар ин ҷо матне, ки қаблан рамзгузорӣ карда будем, яъне "EJJEKIEJNESR" -ро рамзкушоӣ мекунем. Дар ин ҳолат аз функсияи рамзкушоӣ $D(y)=a^{-1}(y-b) mod\ m$ истифода бурда мешавад. Дар ин ҷо $b=4, m=26$ ва $a^{-1}=9$ мебошад. Ибтидо қиматҳои ададии матни "NMGZERHQ"-ро дар ҷадвали зерин менависем:

Матни рамзгузошташуда	N	M	G	Z	E	R	H	Q
У	13	12	6	25	4	17	7	16

Акнун барои ҳар як қимати у қимати $9(y-4)$-ро ҳисоб карда, ба 26 тақсим мекунем ва бақияро дар ҷадвали зерин менависем.

Матни рамзгузошташуда	N	M	G	Z	E	R	H	Q
у	13	12	6	25	4	17	7	16
$9(у-4)$	81	72	18	189	0	117	27	108
$9(у-4)\ mod\ 26$	3	20	18	7	0	13	1	4

Дар қадами охирон матни рамзгузошташударо рамзкушоӣ мекунем, яъне ба ҷои қиматҳои сатри охирони ҷадвал ҳарфҳои мувофиқашонро менависем, ки "DUSHANBE" ҳосил мешавад.

Матни рамзгузошташуда	N	M	G	Z	E	R	H	Q
у	13	12	6	25	4	17	7	16
$9(у-4)$	81	72	18	189	0	117	27	108
$9(у-4)\ mod\ 26$	3	20	18	7	0	13	1	4
Матни ошкор	D	U	S	H	A	N	B	E

Барои тез намудани суръати рамзгузорӣ ва рамзкушоӣ ибтидо ҳамаи ҳарфҳои алифборо рамзгузорӣ карда ҷадвали мувофиқро ҳосил мекунем.

Алифбо	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$(3x+4)$	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1
Ҳарфҳо	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B

Қайд. *Ҳангоми* $a = 1$ *будан аз рамзи аффиавӣ рамзи Сезар ҳосил мешавад.*

Барномаи рамзгузорӣ ва рамзкушоии методи Афиавӣ дар забони Java:

```
public static void main(String[] args) {
  String input = "ATTACKATDAWN";
  int x = 3;
  int y = 4;
  String enc = encrypt(input,x,y);
  String dec = decrypt(enc,x,y);
  System.out.println("Input:     " + input);
  System.out.println("Decrypted: " + enc);
  System.out.println("Decrypted: " + dec);
}
public static String encrypt(String input,int FK,int SK) {
  String str = "";
  for (int in = 0; in < input.length(); in++) {
   char get = input.charAt(in);
    if (Character.isLetter(get)) {
     // ax + b % 26
    get = (char) ((FK * (int)(get + 'A') + SK) % 26 + 'A');
  }
   str +=get;
}
return str;
}
public static String decrypt(String input,int FK,int SK) {
  String str = "";
  int x = 0;
```

```
  int inverse = 0;
   while(true) {
    inverse = FK * x % 26;
     if(inverse == 1)
      break;
     x++;
  }
for (int in = 0; in < input.length(); in++) {
  char get = input.charAt(in);
  if (Character.isLetter(get)) {
    get = (char)(x * ((get + 'A') - SK) % 26 + 'A');
   }
 str +=get;
}
return str;
 }
```

8. Рамзи тригонометрӣ

Тавре медонем, муодилаи мавҷ

$$y = \cos(x + N \cdot dx) \qquad (1)$$

дорои лаппиши (амплитудаи) доимӣ буда, дар тамоми тири ададӣ ($x \in (-\infty, +\infty)$) бефосила мебошад. Ҳолати аз ҳама ҷолиб ин аст, ки агар $dx \neq \frac{2\pi}{N}$ бошад (дар ин ҷо дилхоҳ ададӣ бутун), он гоҳ даври амплитудаи функсияи мазкур беохир мешавад.

Соли 2005 В.П. Сазов[1] дар конфронси умумиросиягии «РусКрипто» методи нави криптографиеро пешниҳод кард, ки дар он муодилаи (1) истифода шудааст. Соли 2011 бошад Городилов А. Ю. ва Митраков А. А.[2] мақолае чоп карданд, ки дар он гуфта шудааст, ки методи тригонометрӣ як воситаи содаи рамзгузорӣ буда, бар муқобили ягон алгоритм ва стандарт сохта нашудааст.

Шарҳи алгоритм

Дар тири x ҳамаи символҳои ягон алифбо ё ҳамаи символҳои клавиатураро (256 символ), ки сар карда аз 0 то 255 рақамгузорӣ шудаанд, ба тартиб (метавонанд ба таври тасодуфӣ) навишта мешаванд. Формулаҳои рамзгузорӣ ва рамзкушоӣ мувофиқан шакли зеринро доранд:

$$\mathrm{y} = x + N\cos(z + \mathrm{n}\cdot \mathrm{d}x) \pmod{\mathrm{N}} \qquad (2)$$

$$x = y - N\cos(z + \mathrm{n}\cdot \mathrm{d}x) \pmod{\mathrm{N}} \qquad (3)$$

дар ин ҷо x −қимати рақамии (рақами тартибии) ҳарфе, ки бояд рамзгузорӣ карда шавад, N-миқдори ҳарфҳои алифбо, z ва dx калид (ададҳои ҳақиқӣ), n рақами тартибии ҳарфе, ки бояд рамзгузорӣ карда шавад (мавқеи ҳарф дар матни ошкор) ва у символи рамзгузошташуда мебошад.

[1] Сизов В.П. Криптографические алгоритмы на основе тригонометрических функций . URL: http://www.ruscrypto.ru/sources/conference/rc2005

[2] Городилов А. Ю., Митраков А. А. Криптоанализ тригонометрического шифра с помощью генетичес-кого алгоритма // Вестник Пермского уни вер си тета, 2011. Вып. 4(8).

Пас аз рамзгузорӣ матне ҳосил мешавад, ки андозааш ба андозаи матни ошкор баробар буда, ба ҳамон алифбо ифода карда мешавад. Қайд кардан ба маврид аст, ки ҳангоми рамзгузорӣ ва рамзкушоӣ ададҳои ҳосилшуда то бутун яклухт карда мешаванд. Дар ин навъ рамзгузорӣ ба сифати қимати ададии ҳарфҳо метавон аз ададҳои ҳақиқӣ низ истифода кард. Бо мисоли кучаке истифодаи алгоритми мазкурро дида мебароем.

Мисол. Матни “АБГ” –ро ки дар алифбои 33 ҳарфаи алифбои криллӣ навишта шудааст, бо истифода аз рамзи тригонометри рамзгузорӣ мекунем. Қимати калидҳои махфӣ $z = \frac{1}{2}$ ва $dx = 7$ – ро мегирем. Ҳар як ҳарфи алифбо на бо як адад, балки бо нимintервали ададҳои ҳақиқӣ мувофиқ гузошта мешавад:

А => [0..1), Б => [1..2), В => [2..3), ….

Ба сифати x маркази интервалҳоро гирифта, ба формулаи (1) мегузорем ва ҳосил мекунем.

$$y_1 = 0.5 + 33\cos\left(\frac{1}{2} + 1 \cdot 7\right) \approx 11{,}93 \Rightarrow \text{К};$$

$$y_2 = 1.5 + 33\cos\left(\frac{1}{2} + 2 \cdot 7\right) \approx -10{,}21 = 22{,}79 \pmod{33} \Rightarrow \text{Х};$$

$$y_3 = 3.5 + 33\cos\left(\frac{1}{2} + 3 \cdot 7\right) \approx -25{,}59 = 7{,}40 \pmod{33} \Rightarrow \text{Ж}.$$

Дар натиҷа матни рамзгузошташуда ба сурати “КХЖ” ҳосил мешавад.

Барои рамзкушоӣ бошад, аз формулаи (2) истифода бурда мешавад.

$$x_1 = 11.5 - 33\cos\left(\frac{1}{2} + 1 \cdot 7\right) \approx 0{,}06 \Rightarrow \text{А};$$

$$x_2 = 22.5 - 33\cos\left(\frac{1}{2} + 2 \cdot 7\right) \approx 34{,}21 = 1.21 \pmod{33} = \Rightarrow \text{Б};$$

$$x_3 = 7.5 - 33\cos\left(\frac{1}{2} + 3 \cdot 7\right) \approx 36{,}59 = 3{,}59 \pmod{33} \Rightarrow \text{Г}.$$

Қайд кардан лозим аст, ки устувории криптографиро дар ин ҷо ададҳои махфӣ кафолат медиҳанд.

Барои рамзгузорӣ ва рамзкушоӣ кардан мувофиқан метавон аз зербарномаҳои зерин истифода кард.

Барномаи рамзгузорӣ.

```
#include <iostream>
#include <string.h>
#include <cmath>
using namespace std;
int main(int argc, char** argv) {
    string S=" man ba maktab";
    double z=0.5,dx=7, x;
     int i, n,  k, y;
     k=S.length();
     for (i=0; i<k; i++){
          x=(int)S[i];
           y=(int)x+n*cos(z+i*dx);
           y=y%256;
           S[i]=(char) y;
      }
   cout<<S<<endl;
```

```
return 0;
}
```

Барномаи рамзкушой

```
#include <iostream>
#include <string.h>
#include <cmath>
using namespace std;
int main(int argc, char** argv) {
  string S;
  double z=0.5,dx=7, x;
  int i, n,  k, y;
  cin>>S;
 cout<<"n="; cin>>n; //n=254;
  k=S.length();
  for (i=0; i<k; i++){
          x=(int)S[i];
           y=(int)x-n*cos(z+i*dx);
           y=y%256;
           S[i]=(char) y;
  }
  cout<<S<<endl;
return 0;
}
```

Саволҳо барои мустаҳкамкунӣ

1. Рамзи Гронсфилд кай сохта шудааст?
2. Моҳияти рамзи Гронсфилд аз чӣ иборат аст ва аз рамзи Сезар чӣ фарқ мекунад?
3. Рамзи Тритемия чӣ гуна рамз аст?
4. Рамзи Виженер аз рамзи Тритемия чӣ фарқ дорад?
5. Рамзи Плейфер кай сохта шудааст ва моҳияти он аз чӣ иборат аст?
6. Барои чи рамзи Хилл истифодаи васеъ пайдо накард?
7. Моҳияти рамзи Хилл аз чӣ иборат аст ва дар он чӣ тавр калид интихоб карда мешавад?
8. Рамзи тригонометри дар асоси чи ташкил ёфтааст?
9. Бо кадом мақсад рамзи тригонометри сохта шудааст?

ФАСЛИ 3. МЕТОДҲОИ МУОСИРИ РАМЗГУЗОРӢ

Боби 8. Методҳои рамзгузории бо калидҳои кушода

То ҳол мо методҳои криптографиеро мавриди баҳс қарор додем, ки барои рамзгузорӣ ва рамзкушоӣ танҳо аз як калид истифода карда мешуд. Ҳоло бошад усули нави рамзгузориро дида меброем, ки дар барои рамзгузорӣ ва рамзкушоӣ калидҳои алоҳида истифода бурда мешавад.

1. Алгоритми Диффи - Ҳеллман

Асосгузори методҳои криптографии бо калидҳои кушода олимони америкоӣ Уитфилд Диффи[1] (Whitfield Diffie) ва Мартин Ҳеллман (Martin Hellman) буда, инчунин новобаста аз онҳо Ралф Меркл (Ralph Merkle) низ ба ҳисоб меравад. Нахустин маротиба Диффи-Ҳеллман пешниҳод карданд, ки дар криптография на аз

як калид, балки аз ду калид: калиди рамзгузорӣ ва калиди рамзкушоӣ истифода бурда шавад. Диффи ва Ҳеллман соли 1976 ин ақидаро дар конференсияи миллии компютерии Амрико пешниҳод карда, пас аз чанд моҳ

[1] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

таҳти унвони «New Directions in Cryptography[1]» мақолаеро чоп карданд.

Пас аз як соли ин ҳодиса алгоритми рамзгузории ассиметрии RSA пайдо шуд. Ин алгоритмро баъдан мавриди баҳс қарор медиҳем.

Соли 2012 Мартин Ҳеллман хизматҳои Меркл-ро ба назар гирифта, пешниҳод кард, ки ин алгоритм „алгоритми Диффи-Ҳеллман-Меркл“ номгузорӣ карда шавад. Бо назардошти пешниҳод Мартин Хелман дар патенти U.S. Patent 4 200 770 номи се муаллиф Ҳеллман, Диффи ва Меркл зикр карда шудааст.

Декабри соли 1997 маълумоте пайдо шуд, ки гӯё соли 1974 Малколм Вилямс алгоритми математикии дар асоси қонуни комутативии дараҷа, ҳангоми пай дар пай ба дараҷабардориро исбот карда будааст

$$(b^x)^y = (b^y)^x = b^{xy}.$$

Методи мазкурро метавон аналоги алгоритми Диффи-Ҳеллман номид.

Шарҳи алгоритм

Фарз мекунем, ки ду муштарӣ бо номҳои Алӣ ва Валӣ мехоҳанд бо ҳамдигар мубодилаи итилоот кунанд. Фарз мекунем, ки ибтидо барои онҳо ду ададиҳои р ва g маълум мебошанд. Баъдтар тарзи интихоби ин параметрҳоро мавриди баҳс қарор медиҳем.

[1] http://www.cse.msstate.edu/~ramkumar/diffie-hellman.pdf

Барои сохтани калиди махфӣ ҳарду муштарӣ яктоӣ адади ихтиёрии тасодуфиро интихоб мекунанд: масалан, Алӣ — адади a, Вали - ададӣ b. Пас аз ин, Алӣ қимати ифодаи зеринро ҳисоб карда, натиҷаро ба Валӣ равон мекунад.

$$A = g^a \ mod \ p \qquad (1)$$

Валӣ дар навбати худ қимати ифодаи

$$B = g^b \ mod \ p \qquad (2)$$

–ро ҳисоб намуда, натиҷаро ба Алӣ равон мекунад.

Қадами навбати Алӣ дар асоси адади a ва B қимати ифодаи зеринро ҳисоб мекунад:

$$B^a mod \ p = g^{ab} \ mod \ p \qquad (3)$$

Дар ҳамин ҳол Валӣ дар асоси адади b ва A қимати ифодаи

$$A^b mod \ p = g^{ab} \ mod \ p \qquad (4)$$

–ро ҳисоб мекунад:

Бе душвори метавон дид, ки Алӣ ва Валӣ як адад (калид)-ро ба даст меоранд :

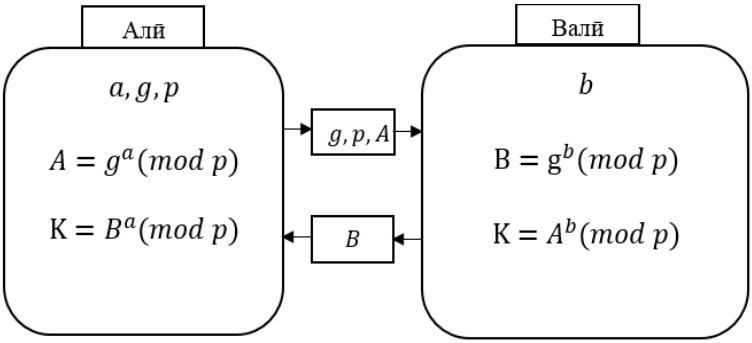
$$K = g^{ab} \ mod \ p \qquad (5)$$

Дар ҳақиқат:

$$B^a \ mod \ p \ = \ (g^b \ mod \ p)^a \ mod \ p \ = \ g^{ab} \ mod \ p$$
$$= \ (g^a \ mod \ p)^b \ mod \ p = \ A^b \ mod \ p.$$

Адади ҳосилшуда, яъне K –ро онҳо метавонанд ҳамчун калиди махфӣ истифода кунанд. Дар ин ҷо ададҳои p, a ва b ба қадри кифоя калон буда, суиқасдкунанда наметавонад ҳангоми ба даст овардани А ва B қимати ифодаҳои (3) ва (4) – ро ҳисоб кунад.

Шакли схематикии ин алгоритм чунин аст:



Тавре, ки қайд кардем барои ҳисоб намудани $A = g^a \bmod p$ метавон аз методи modInverse() истифода кард. **Мисол**.

```
import java.math.BigInteger;
import java.util.Scanner;
public class modPow{
public static void main(String[] args)
{
    BigInteger g,a,p,S;
    Scanner sc=new Scanner(System.in);
    g=sc.nextBigInteger();
    a=sc.nextBigInteger();
    p=sc.nextBigInteger();
    S=g.modPow(a, p);
    System.out.println(S);
 }
}
```

Дар амалия ба сифати a ва b ададҳои тартибӣ 10^{100} ва барои p тартиби 10^{300} истифода бурда мешавад. Адади g шарт нест, ки калон бошад, одатан аз доираи даҳии якум гирифта мешавад.

Қайд. *Барои мубодилаи итилоот намудан, ибтидо адади содаи калони p ва адади g* ($1 < g < p - 1$ *интихоб карда мешавад. Дар ин ҷо адади* g *тавре интихоб карда мешавад, ки барои он ҳамаи ададҳои* $\{1, 2, 3, \dots, p - 1\}$ *– ро ҳамчун дараҷаи гуногуни* $g \bmod p$ *тасвир кардан мумкин бошад. Барои таъмини бехатарии криптографӣ, адади p тавре интихоб карда мешавад, ки шарти зеринро қаноат кунонад.*

$$p = 2q + 1$$

дар ин ҷо q *низ ягон адади сода мебошад. Аз ин ҷо ба сифати* g *метавон чунин ададеро интихоб кард, ки барои он нобаробариҳои зерин иҷро гарданд:*

$$1 < g < p - 1 \text{ ва } g^q \bmod p \neq 1 \qquad (*)$$

Мисол. *Бигузор* $\mathrm{p} = 23$ бошад, он гоҳ $\mathrm{p} = 2 * 11 + 1$ *мешавад, аз ин ҷо* $q = 11$ *мешавад. Акнун параметри* g *– ро интихоб мекунем. Ибтидо* $g = 3 -$ ро *месанҷем: азбаски* $3^{11} \bmod 23 = 1$ *буда, шарти (*) иҷро намегардад, бинобар ин қимати дигаре барои* g *интихоб мекунем. Бигузор* $g = 5$ *бошад, он гоҳ* $5^{11} \bmod 23 = 22 \neq 1$ *мешавад. Тавре ки аён аст, барои* $g = 5$ *ҳарду нобаробарии (*) иҷро мешаванд. Ҳамин тариқ, мо параметрҳои* $p = 23$ ва $g = 5 -$ *ро интихоб кардем.*

Одатан ададҳои p ва g *–ро яке аз тарафҳо интихоб карда, ба дигараш равон мекунад (дар шабака паҳн мекунад).*

Тасдиқот. *Бигузор Карим криптоаналитик аст. Ҳарчанд ки ӯ пайғомҳои Алӣ ва Валиро ба даст оварда бошад ҳам, наметавонад маълумоти асл (калидҳои махфиро)-ро иваз кунад.*

Дурустии ин тасдиқотро бо мисол дида мебароем. Дар ҳақиқат, бигузор Муштариён Алӣ ва Валӣ параметрҳои зеринро интихоб ва ҳисоб карда бошанд.

s = 2 калиди махфӣ.

g = решаи ибтидоӣ аз рӯйи модули p ($g = 5$)

p = адади содаи кушода (p = 23)

a = калиди махфии Алӣ ($a = 6$)

A = калиди кушодаи Алӣ ($A = g^a \bmod p = 8$)

b = калиди махфии Валӣ (b = 15)

B = калиди кушодаи Валӣ ($B = g^b \bmod p = 19$)

Алӣ	
Қимат	Намедонад
p = 23	**b = ?**
g = 5	
a = 6	
A = 5^6 mod 23 = 8	
B = 5^b mod 23 = 19	
s = 19^6 mod 23 = **2**	

Валӣ	
Медонад	Намедонад
p = 23	**a = ?**
g = 5	
b = 15	
B = 5^{15} mod 23 = 19	
A = 5^a mod 23 = 8	
s = 8^{15} mod 23 = **2**	
s = 19^a mod 23 = **2**	

Карим	
медонад	намедонад
p = 23	**a = ?**
g = 5	**b = ?**
	s = ?
A = 5^a mod 23 = 8	
B = 5^6 mod 23 = 19	
s = 19^a mod 23	
s = 8^b	

s = 8^b mod 23 = **2**	
s = 19^6 mod 23 = 8^6 mod 23	
s = 2	

s = 8^{15} mod 23 = 19^a mod 23	
s = 2	

mod 23	
s = 19^a mod 23 = 8^bmod 23	

2. Алгоритми Диффи-Ҳеллман барои се ва ё зиёда муштарӣ

Алгоритми Диффи-Ҳеллман на танҳо барои ду муштарӣ (иштирокчӣ) пешбинӣ шудааст, балки онро метавон барои якчанд муштари низ истифода кард. Ҳолатеро мебинем, ки Алӣ, Валӣ ва Карим якҷоя калиди умумӣ ҳосил мекунанд. Дар ин ҳолат пайдарпай амалҳо ба сурати зерин ичро карда мешаванд:

1) Тарафҳо оиди параметрҳои алгоритм p ва g ба мувофиқа мерасанд;
2) Ҳар як муштарӣ мувофиқан калидҳои махфии худ $-a, b$ ва c –ро интихоб мекунад:
3) Алӣ қимати ифодаи $A = g^a \ mod \ p$ –ро ҳисоб карда ба Валӣ равон мекунад;
4) Валӣ бошад, қимати ифодаҳои $B_1 = (g^a)^b mod \, p$ ва $B = g^b mod \, p$ –ро ҳисоб карда, ба Карим мефиристонад;

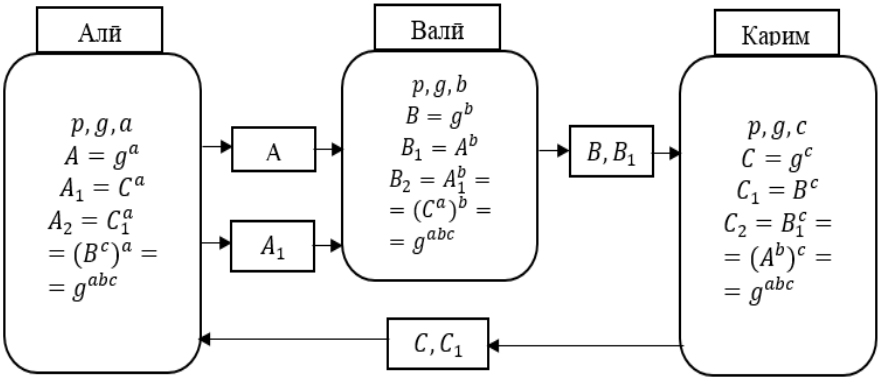
5) Дар навбати худ Карим қимати ифодаи $C_1 = (g^b)^c \, mod \, p = g^{bc} \, mod \, p$ ва $C = g^c \, mod \, p$ –ро ҳисоб карда ба Алӣ мефиристонад, қимати $C_2 = (g^{ab})^c \, mod \, p = g^{bca} = g^{abc} \, mod \, p$ –ро ҳисоб карда ҳамчун калиди махфӣ нигоҳ медорад.

6) Алӣ қимати ифодаи $A_2 = (g^{bc})^a \, mod \, p = g^{bca} mod \, p = g^{abc} \, mod \, p$ –ро ҳисоб карда ҳамчун калиди махфӣ нигоҳ дошта, қимати $A_1 = (g^c)^a \bmod p = g^{ca} \, mod \, p$ –ро ҳисоб карда ба Валӣ мефиристонад;

7) Валӣ барои ҳосил кардани калиди махфии умумӣ қимати ифодаи $B_2 = (g^{ca})^b mod \, p = g^{cab} = g^{abc} \, mod \, p$ –ро ҳисоб карда ҳамчун калиди махфӣ нигоҳ медорад;

Дар ин ҳолат ҳар як муштарӣ метавонад қиматҳои $A = g^a, A = g^b, A = g^c, A = g^{ab}, A = g^{ac}, A = g^{bc}$ мушоҳида кунад, аммо дидани дилхоҳ комбинатсияи $A = g^{abc}$ ғайриимкон аст.

Шакли схематикии ин алгоритм чунин аст:



3. Рамзи Шамир

Рамзи Шамир соли 1979 аз тарафи криптоаналитикӣ изроилӣ

Ади Шамир [1] (Adi Shamir) барои мубодилаи пайѓомҳои махфӣ бо истифода аз алгоритми Диффи-Ҳеллман сохта шудааст.

Рамзи мазкурро дида мебароем. Бигузор ду муштарӣ Алӣ ва Валӣ мехоҳанд тавассути канали алоқа бо ҳам мубодилаи итилоот кунанд, масалан, Алӣ мехоҳад, ки пайѓоми m – ро ба Валӣ тавре равон кунад, ки касе аз моҳияти он огоҳ нагардад. Барои иҷрои ин амал Алӣ адади содаи бузурги p-ро интихоб карда, ба

[1] **Ади Шамир** (яҳудӣ. עדי שמיר, 6 июли соли 1952 дар шаҳри Тел-Абиби Изроил ба дунё омадааст) — криптоаналитикӣ машҳури изроилӣ, олими соҳаи назарияи системаи ҳисобкуниниҳо, профессори информатики ва математикаи амалӣ дар институти Вейстман дорандаи лаурети Тюринг.

Валӣ равон мекунад. Илова бар ин , Алӣ ду адади ихтиёрии A_1 ва A_2 – ро тавре интихоб мекунад, ки барои онҳо баробарии зерин ичро гардад.

$$A_1 A_2 \ mod \ (p-1) = 1 \qquad (1)$$

Ин ададҳоро Алӣ махфӣ нигоҳ медорад. Валӣ дар навбати худ ду адади B_1 ва B_2 –ро тавре интихоб мекунад, ки барои онҳо баробарии зерин ичро гардад:

$$B_1 B_2 \ mod \ (p-1) = 1 \qquad (2)$$

Ин ададҳоро Валӣ махфӣ нигоҳ медорад. Пас аз ин, Алӣ бо истифодаи протоколи се зинагӣ пайғоми m – ро ба Валӣ равон мекунад. Агар $m < p$ (m ҳамчун адад дар назар гирифта мешавад) бошад, он гоҳ дарҳол равон карда мешавад. Дар ҳолати акс, агар $m \geq p$ бошад, пайғоми m ба сурати $m_1, m_2, \dots, m_t$ (дар ин ҷо $m_i < p$) тасвир карда шуда, пайдарпай равон карда мешавад. Дар ин ҳолат барои рамзгузории ҳар як m_i хуб мешавад, ки ҷуфтҳои (A_1, A_2) ва (B_1, B_2) интихоб карда шаванд, дар ҳолати акс эътиборнокии (надёжность) система кам мешавад. Дар ҳоли ҳозир чунин рамзро барои равон кардани ададҳое (калидҳои махфӣ) ки аз р хурданд истифода мебаранд. Аз ин рӯ ҳолати $m < p$ –ро мавриди баҳс қарор медиҳем.

Умуман, алгоритми Шамир аз чор қадам иборат аст.

Қадами 1. Алӣ адади $C_1 = m^{A_1} \ mod \ p$ (m – пайғоми ошкор) – ро ҳисоб карда, ба Валӣ равон мекунад.

Қадами 2. Валӣ адади C_1 – ро ба даст оварда, адади $E_1 = {C_1}^{B_1} \ mod \ p$ ро ҳисоб карда, натиҷаро ба Алӣ равон мекунад.

Қадами 3. Алӣ адади $C_2 = {E_1}^{A_2} \ mod \ p$ –ро ҳисоб карда, ба Валӣ равон мекунад.

Қадами 4. Валӣ адади $E_2 = {C_2}^{B_2} \ mod \ p$ –ро ҳисоб карда, соҳиби матни ошкор мешавад.

Бедуншворӣ дидан мукин аст, ки

1) Адади $E_2 = m$ аст, яъне дар натиҷаи амаликунии протокол аз Алӣ ба ҷониби Валӣ ҳақиқатан матни ошкор равон карда мешавад.
2) Рамзшикан (злоумышленник) наметавонад, муайян кунад, ки чӣ гуна итилоот равон карда шудааст.

Исбот. Тавре медонем, дилхоҳ адади бутуни $e \geq 0$–ро метавон ба шакли $e = k(p-1) + r \ \ (0 \leq r < 1)$ тасвир кард, ки дар ин ҷо $r = e \ mod \ (p-1)$ аст. Бинобар ин, аз рӯйи теоремаи Ферма ҳосил мекунем.

$$x^e mod \ p = x^{k(p-1)+r} \ mod \ p = (1^k x^r) mod \ p$$
$$= x^{emod \ (p-1)} \ mod \ p$$

Дурустии қисми аввали тасдиқот аз баробарии зерин бармеояд.

$$E_2 = {\mathrm{C}_2}^{B_2} mod \ p = ({E_1}^{A_2})^{B_2} mod \ p = ({\mathrm{C}_1}^{B_1})^{A_2 B_2} mod \ p =$$

$$= (m^{A_1})^{A_2 B_1 B_2} mod \ p = m^{A_1 A_2 B_1 B_2} mod \ p$$

$$= m^{(A_1 A_2 B_1 B_2) mod \ (p-1)} mod \ p = m$$

Исботи қисми дуюми теорема аз фарзе, ки барои муайянкунии m рамзшикан истифода мебарад, истифода

мекунем. Ибтидо он қимати B_1-ро ҳисоб карда, пас B_2 ва дар охир қимати $E_2 = m$–ро ҳисоб мекунад. Аммо барои ичрои ин амал ба рамзшикан лозим аст, ки масъалаи логарифмирониии дискретиро ҳал кунад, лекин дар амалия барои адади кифоя калони р ин амал ғайриимкон аст.

Методи ёфтани ҷуфтҳои (A_1, A_2) ва (B_1, B_2) - ро, ки муодилаҳои (1) (2) –ро қаноат мекунонанд, тавзеҳ медиҳем. Барои ин кифоя аст, ки амалҳои яке аз муштариён, масалан Алиро нишон диҳем, амалҳои Валӣ низ ба ҳамин монанд ичро карда мешаванд. Алӣ адади $A_1 -$ ро ба сурати тасодуфӣ тавре интихоб мекунад, ки бо $p - 1$ байнан сода бошад. Пас аз ин, қимати A_2 бо истифода аз алгоритми васеъкардашудаи Евклид ҳисоб карда мешавад.

Мисол. Бигузор Алӣ мехоҳад пайғоми $m = 10$ – ро ба Валӣ равон кунад.

Ҳал. Барои ичрои ин амал ибтидо адади содаи $p = 23$ ва $A_1 = 7$ ва $(\text{КТУ}(7, 22) = 1) -$ ро интихоб карда, сипас қимати $A_2 = 19$ - ро ҳисоб мекунад. Ба ҳамин монанд Валӣ параметри $B_1 = 5$ (бо адади 22 байни ҳам сода) – ро интихоб карда, қимати $B_2 = 9$–ро ҳисоб мекунад.

Акнун онҳо аз қадамҳои алгоритми Шамир истифода мекунанд.

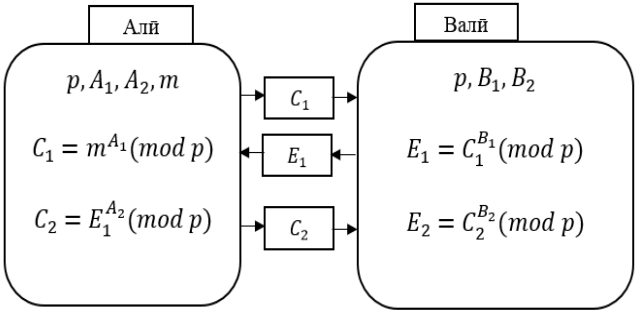
Қадами 1. $C_1 = 10^7 \ mod \ 23 = 14;$

Қадами 2. $\text{E}_1 = 14^5 \ mod \ 23 = 15;$

Қадами 3. $C_2 = 15^{19}\ mod\ 23 = 19$;

Қадами 4. $E_2 = 19^9\ mod\ 23 = 10$;

Ҳамин тариқ, Валӣ пайғоми фиристодашударо ба даст меорад. Намуди схематикии ин алгоритм чунин аст:



4. Алгоритми Ал-Ҷамол

Рамз (алгоритми) Ал-Ҷамол соли 1984-85 аз тарафи криптографӣ мисрӣ Тоҳир Ал-Ҷамол [1] барои мубодилаи

[1] Тоҳир Ал-Ҷамол 18-уми августи соли 1955 дар шаҳри Қоҳираи Миср ба дунё омадааст. Соли 1976 пас аз хатми мактаби миёна ба донишгоҳи Қоҳира дар факултети Электромеханика дохил шуд. Усули тадриси устодон ва чанд омилҳои дигар сабаб шуданд, ки Тоҳир донишгоҳро тарк карда, соли 1979 ба донишгоҳи Стенфорди Амрико дохил шуд. Бо роҳбарии Мартин Говард соли 1981 Тоҳир қадами нахустини худро ба олами криптографӣ ниҳод. Соли 1984 унвони PhD ро дар донишгоҳи Стенфорд соҳиб шуд. Тоҳир дар ширкатҳои монанди Hewlett-Packard, Netscape, Kroll ва ғайра кору фаъолият кардааст. Соли 2008 Тоҳир ба сифати директори техникии ширкати Tumbleweed Communications таъин шуд.

Илова бар ин, Тоҳир яке аз мушовирони директори Vindicia, ва ширкатҳои Onset Ventures, Glenbrook partners, PGP corporation, Arcot Systems, Finjan, Facetime, Simplified ва Zetta мебошад.

мактубҳои рамзгузошташуда, тавассути канали алоқаи кушод, сохта шудааст. Фарқияти асосии методи мазкур аз методи Шамир дар он аст, ки дар ин метод танҳо як маротиба пайғом равон карда мешавад. Ҳоло шарҳи мухтасари методи Ал-Ҷамолро меорем.

Бигузор якчанд муштарӣ бо номҳои Алӣ, Валӣ, Карим, ..., мехоҳанд бо ҳамдигар тавассути канали алоқаи кушод (умумӣ) мубодилаи итилоот кунанд. Барои иҷрои ин амал аз алгоритми Ал-Ҷамол истифода карда мешавад.

Ибтидо барои ҳамаи гурӯҳи муштариён чунин ададиҳои содаи калони p ва адади g интихоб карда мешавад. Ададҳои мазкурро метавонад яке аз онҳо интихоб карда ба дигарон равон кунад ва ё ҳамаи муштариён дар якҷоягӣ ин ададҳоро интихоб кунанд. Пас аз ин, ҳар як муштарӣ ададиҳои махфии C_i $(1 < C_i < p - 1 -$ ро интихоб карда, мувофиқи он қимати $D_i -$ ро ҳисоб мекунад.

$$D_i = g^{C_i} \, mod \, p \qquad (1)$$

Дар натиҷа ҷадвали зерин ҳосил мешавад.

Муштарӣ	Калиди махфӣ	Калиди кушода
Алӣ	C_1	D_1
Валӣ	C_2	D_2
Карим	C_3	D_3

Акнун ба сифати намуна, нишон медиҳем, ки Алӣ чӣ тавр пайғоми m-ро ба Валӣ равон мекунад. Тавре ки қаблан дар методи Шамир гуфта будем, ҳар як символи мактуб ба сурати ададиҳои $m < p$ тасвир карда мешавад.

Қадами 1. Валӣ қимати ифодаи

$$D_2 = g^{C_2} \ mod \ p \qquad (1)$$

−ро ҳисоб карда, дар шабака интишор мекунад (ба Алӣ равон мекунад).

Қадами 1. Алӣ ададӣ тасодуфии C_1 $(1 \leq C_1 \leq p - 2$ −ро интихоб карда, қимати ифодаҳои

$$D_1 = g^{C_1} \ mod \ p \qquad (2)$$

$$C = m \cdot {D_2}^{C_1} \ mod \ p \qquad (3)$$

ҳисоб мекунад ва натиҷа, ҷуфти (D_1,C)-ро ба Валӣ равон мекунад.

Қадами 2. Валӣ ҷуфти ададҳои (D_1,C)-ро ба даст оварда, қимати ифодаи зеринро ҳисоб мекунад.

$$E = C \cdot {D_1}^{p-1-C_2} \ mod \ p \qquad (4)$$

Бе душворӣ дидан мумктин аст, ки:

1) Валӣ пайғоми $E = m$ −ро ба даст меорад.

2) Рамзшикан наметавонад ҳатто бо донистани ададҳои p, g, D_2, D_1 ва C қимати m −ро ба даст орад.

Дар ҳақиқат, бо ифодаи (3) қимати C-ро ба ифодаи (4) мегузорем.

$$E = m \cdot {D_2}^{C_1} \cdot r^{p-1-C_2} \ mod \ p.$$

Акнун ба сифати D_1 ифодаи (2) ва ба сифати D_2 ифодаи (1)-ро истифода, бурда ҳосил мекунем.

$$E = m \cdot (g^{C_2})^{C_1} \cdot (g^{C_1})^{p-1-C_2} mod \ p$$
$$= m \cdot g^{C_2 C_1 + C_1(p-1) - C_1 C_2} \ mod \ p =$$
$$= m \cdot g^{C_1(p-1)} \ mod \ p.$$

Аз ин ҷо мувофиқи теоремаи Ферма ҳосил мекунем:

$$g^{C_1(p-1)} \bmod p = 1^{C_1} \bmod p = 1.$$

Ҳамин тариқ, дурустии пайғоми равонкардашуда исбот шуд.

Барои исботи қисми дуюм, дида мешавад, ки душман бо истифода аз (2) наметавонад C_1 –ро ҳисоб кунад, чунки ин масъалаи логарифмирониии дискретӣ мебошад. Аз ин рӯ он наметавонад дар ифодаи (3) m–ро ёбад, чунки он бо ададӣ номаълум зарб карда шудааст. Илова бар ин, душман наметавонад пайғоми Валиро низ ба даст орад, зеро барои он ададӣ махфии C_2 низ номаълум мебошад. (ҳисобкунии C_2 аз рӯйи формулаи (1) низ масъалаи логарифмирониии дискретӣ мебошад).

Мисол. Алӣ мехоҳад, ки пайғоми m=15 –ро ба Валӣ равон кунад. Параметрҳоро монанди мисоли дар рамзи Шамир дида баромадаамон интихоб мекунем, яъне p=23 ва g=5. Бигузор Валӣ ададӣ тасодуфии (калиди мах-фӣ) $C_2 = 13$ –ро интихоб карда бошад, бо истифода аз (1) $D_2 = 5^{13} \bmod 23 = 21$ –ро ҳисоб карда, ба Алӣ равон мекунад. Алӣ дар навбати худ ададӣ тасодуфии C_1=7 -ро интихоб мекунад. Пас аз ин қимати ифодаҳои (2) ва (3)

$$D_1 = 5^7 \bmod 23 = 17, \quad C = 15 \cdot 21^7 \bmod 23 = 15 \cdot 10 \bmod 23 = 12 -$$

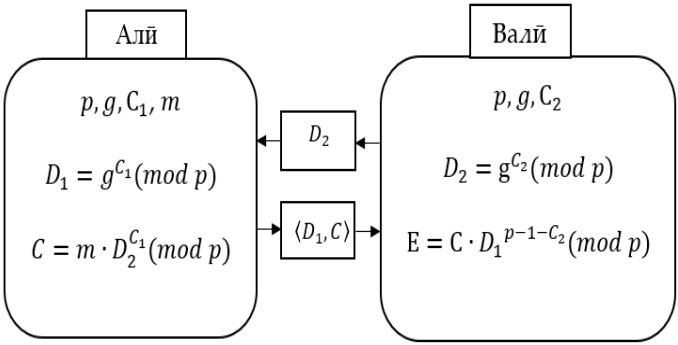
ро ҳисоб карда, натиҷаҳои ҳосилшуда D_1 ва C–ро ба Валӣ равон мекунад. Валӣ бошад бо истифода аз (4) қимати ифодаи

$$E = 12 \cdot 17^{23-1-13} \bmod 23 = 12 \cdot 17^{9} \bmod 23 = 12 \cdot 7 \bmod 23 = 15 -$$

ро ҳисоб карда, пайғоми лозимиро ба даст меорад.

Ба ҳамин монанд, ҳамаи муштариён метавонанд бо ҳам мубодилаи итилоот кунанд. тавре ки аён аст, ҳар як муштарие, ки калиди кушодаи Валиро медонад метавонад бо он, пайғомеро, ки тавассути калиди кушодаи D_2 рамзгузорӣ шудааст, равон кунад. Лекин ба ғайр аз Валӣ каси дигар наметавонад, танҳо бо истифодаи калиди ба худаш махфии C_2 мактуби равонкардашударо рамзкушоӣ кунад. Қайд кардан ба маврид аст, ки дар ин усули рамзгузорӣ ҳаҷми шифр аз ҳаҷми матн ду маротиба зиёдтар мешавад.

Ба намуди схематикӣ ин алгоритм шакли зеринро дорад:



5. Алгоритми RSA (варианти таълимӣ)

Рамзи RSA аз ҷониби се олими амрикоӣ Ривест[1] (Ron Rivesst), Шамир(Adi Shamir), Л.Аддеман[1] (Leonard

[1] Роналд Линн Ривест(***англ.*** Ronald Linn Rivest) соли 1947 дар шаҳри Скенектади штати Ню-Йорк ба дунё омадааст. Соли 1965 мактаби

Adleman) сохта шудааст, ки то ҳоло васеъ истифода бурда мешавад.


Ронала Линн Ривест

Тавре ки медонем, рамзи Шамир масъалаи равон кардани иттилооти муҳимро тавассути хати алоқаи кушода пурра ҳал карда буд. Аммо иттилоот дар ин вақт (тавассути ин рамз) аз як муштарӣ ба муштари дигар се маротиба равон карда мешуд, ин бошад норасоии алгоритми мазкурро ифода мекунад. Рамзи Ал-Ҷамол ин масъаларо бо як маротиба равонкунӣ ҳал намуд, лекин дар


Леонард Макс Адлеман

давлатӣ «Niskayuna high school» -ро хатм кард. Соли 1969 дар донишгоҳи Иелск соҳиби унвони бакалавр шуда, соли 1974 бошад, дар донишгоҳи Стенфордс соҳиби унвони докторӣ Ph.D дар соҳаи илмҳои компютерӣ гардид. Ибтидо дар донишгоҳи Стенфорд дар соҳаи зеҳни сунъӣ кор карда, сипас ҳамчун математик ва информатикаи назариявӣ кор кард. Айни ҳол дар институти технологиии Массачусетия кор мекунад. Ҳамчун таҳиякунандаи алгоритмҳои криптографии RSA, RC2, RC4, RC5, RC6, MD2, MD4, MD5, MD6 маъруф мебошад.

1 Леонард Макс Адлеман (англ. Leonard Adleman — Эйдлмен) 31-уми декабри соли 1945 дар Калифорнияи ИМА ба дунё омадааст. Соли 1989 Адлеман дар факултети илмҳои компютерии донишгоҳи Калифорнияи Ҷанубӣ ҳамчун коргари асосӣ ба кор оғоз кард. Соли 1983 соҳиби унвони профессори гардида, соли 1985 бошад, соҳиби рутбаи профессори илмҳои компютерии Генри Салватор (the Henry Salvatori professor of Computer Science) шуд. Илова бар ин ӯ биологияи молекулярӣ буда, ҳаммуалифӣ алгоритми RSA ва ҳисобкуниҳои ДНК мебошад.

ин рамз ҳаҷми иттилооти равонкардашуда, аз ҳаҷми иттилооти ошкор ду маротиба зиёд мешавад. Системаи RSA бошад, чунин норасоиҳоро бартараф намуд.

Алгоритми мазкур аз се қадам иборат мебошад. Ҳоло ҳар яки ин қадамҳоро мухтасар мавриди баҳс қарор медиҳем

Қадами 1. Ибтидо калидҳои махфӣ ва ошкор интихоб карда мешаванд.

1) Ду ададӣ содаи $p = 3$ ва $q = 7$ интихоб карда мешаванд.
2) Ададҳои додашударо зарб карда модул, яъне n-ро меёбем: $n = p \cdot q = 3 \cdot 7 = 21$.
3) Қимати функсияи Эйлер ҳисоб карда мешавад: $\varphi = (p - 1) \cdot (q - 1) = 2 \cdot 6 = 12$.
4) Чунин ададӣ e , ки шартҳои зеринро қаноат мекунонад, интихоб карда мешавад.

4.1. Он бояд сода бошад.

4.2. Аз қимати φ бояд хурд бошад. Барои мисоли мо метавон ададҳои 3, 5, 7, 11-ро истифода кард.

4.3. Бо φ бояд байнан сода бошад. Барои мисоли мо метавон ададҳои 5, 7, 11-ро истифода кард..

4.4. Барои мисоли мо варианти мувофиқ $e = 5$ мебошад.

Дар ин ҷо Алӣ ҷуфти ададҳои $\{e, n\}$ — ро ҳамчун калиди кушода интихоб карда, ба Валӣ равон мекунад. Пас аз ин, Алӣ калиди махфиашро интихоб мекунад. Барои иҷрои ин амал, бояд ададе интихоб карда шавад, ки аз рӯйи модули φ ба ададиe баръакс бошад, яъне d интихоб карда мешавад. Дар ин ҷо метавонад бо назардошти

маълумотҳои дар боло овардашуда $d = 17$- ро истифода кард. Ҳамин тариқ, ҷуфти ададҳои $\{d, n\}$ –ро Алӣ ҳамчун калиди махфии интихоб карда, махфӣ нигоҳ медорад.

Қадами 2. Рамзгузорӣ.

Пас аз интихоби параметрҳои лозимӣ Алӣ метавонад ба рамзгузорӣ оғоз кунад. Масалан, барои рамзгузорӣ намудани матни m=19 бо истифода аз калидҳои {e, n} = {5, 21} чунин амал карда мешавад.

Алӣ бо истифода аз формулаи $C = m^d \ mod \ n$ матни додашуда рамзгузорӣ карда, натиҷаи ҳосилшуда, яъне C=10-ро ба Валӣ равон мекунад.

Қайд. *Набояд қимати ададии пайғом m аз ададиn калон бошад, вагарна ягон натиҷаи дуруст ба даст намеояд.*

Қадами 3. Валӣ пас аз оне, ки пайғоми Алиро ба даст меорад, бо истифода аз калидҳои $\{d, n\} = \{17, 21\}$ метавонад матнро рамзкушоӣ кунад. Барои иҷрои ин амал, аз формулаи $M = e^d \ mod \ n = 10^{17} \ mod \ 21 = 19$ истифода карда, пайғоми асларо ба даст меорад.

Мисол. Бо истифода аз алгоритми RSA пайғоми m=CAB рамзгузорӣ карда шавад.

Ҳал. Ибтидо ададҳои содаи $p = 3$ ва $q = 11$ - ро интихоб карда, қимати модул $n = 3 \cdot 11 = 33$ ва функсияи Эйлер $\varphi = (p - 1) * (q - 1) = 20$ ҳисоб карда мешавад. Пас аз ин, Алӣ метавонад ба сифати d ададиn 3 ва бо сифати e ададиn 7-ро интихоб кунад.

Матни додашуда ҳамчун ададиn бутуни фосилаи аз 1 то 26 тасвир карда мешавад, масалан, ҳарфи A =1, B=2, C=3 ва ғайра.

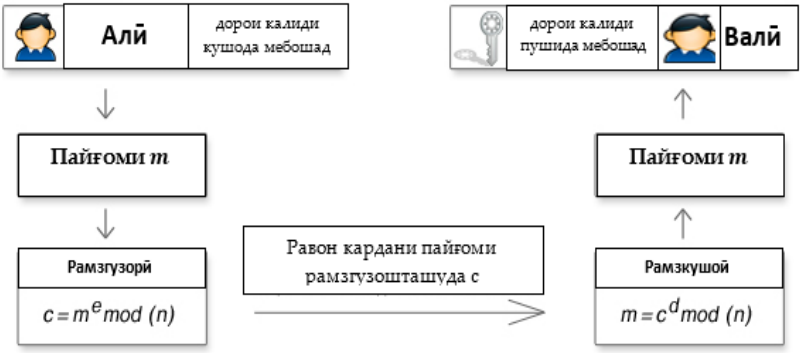
Али бо истифода аз калиди кушодааш {7,33} матни додашударо рамзгузорӣ мекунад.

$$C_1 = 3^7 \, mod \, 33 = 2187 \, mod \, 33 = 9;$$
$$C_2 = 1^7 \, mod \, 33 = 1 \, mod \, 33 = 1;$$
$$C_3 = 2^7 \, mod \, 33 = 128 \, mod \, 33 = 29;$$

Барои рамзкушоӣ кардан Валӣ аз калидҳои пушидаи {3,33} матни рамзгузошташударо рамзкушоӣ мекунад.

$$M_1 = 9^3 \, mod \, 33 = 729 \, mod \, 33 = 3;$$
$$M_2 = 1^3 \, mod \, 33 = 1 \, mod \, 33 = 1;$$
$$M_3 = 29^3 \, mod \, 33 = 24389 \, mod \, 33 = 2;$$

Ҳамин тариқ, матн рамзкушоӣ карда мешавад. Шакли схематикии ин алгоритм чунин аст.



6. Рамзи RSA бо функсияи яктарафа бо гузариши махфӣ (тайный ход)

Дар мавзӯи қаблӣ варианти таълимии рамзи RSA мавриди баҳс қарор гирифта буд. Ҳоло бошад, ба таври пурра рамзи мазкурро дида мебароем.

Қайд мекунем, ки системаи RSA метавонад, аз як элементи криптографии муосир, функсияи яктарафа бо гузариши махфӣ (trapdoor function) истифода барад.

Ин система аз ду далели назарияи ададҳо ташкил ёфтааст.

1) Масъалаи тафтиши сода будани адад, нисбати (қиёсан) осон мебошад.

2) Масъалаи чудокунии ададии намуди $n = pq$ (p ва q – ададҳои сода) ба зарбкунандаҳо хеле душвор мебошад, агар мо танҳо n-ро донем, p ва q – ададҳои калон (ин масъала фактаризатсия номида мешавад).

Бигузор дар системаи мо муштариён бо номҳои Алӣ, Валӣ, Карим,…. мавҷуд бошанд. Ҳар як муштарӣ ду ададии тассодуфии содаи бузургии P ва Q – ро интихоб карда, сипас қимати ададии

$$N = PQ \qquad (1)$$

-ро ҳисоб мекунад. Дар ин ҷо N- иттилооти кушода буда, барои ҳамаи муштариён дастрас мебошад.

Баъд аз ин муштарӣ қимати ададии $\phi = (P-1)(Q-1)$ – ро ҳисоб карда, ададии ихтиёрии $d < a$ – ро ки ба ϕ байнан сода мебошад, интихоб мекунад. Баъд ин тавассути алгоритми васеъкардашудаи Евклид, чунин ададии c – ро ҳисоб мекунад (меёбад), ки барои он баробарии зерин иҷро гардад

$$c \cdot d mod\ \phi = 1 \qquad (2)$$

Ҳамаи иттилоотҳои муштариён, чӣ калиди махфӣ ва чӣ калиди пушида дар ҷадвали зерин гирд оварда шудаанд.

Муштариён	Калиди махфи	Калиди кушода
A	C_A	$d_A,\ N_A$
B	C_B	$d_B,\ N_B$
C	C_C	$d_C,\ N_C$

Бигузор Алӣ мехоҳад, пайғоми $m-$ро ба Валӣ равон кунад. Дар ин ҷо пайғоми m ҳамчун ададе, ки шарти $m < N_B -$ро қаноат мекунонад, тасвир карда мешавад. (Дар оянда индекси B – ишорагарӣ он аст, ки параметрҳо ба Валӣ таалуқ доранд)

Қадами 1. Алӣ мактубро бо истифодаи параметрҳои кушодаи Валӣ ва формулаи

$$e = m^{d_B}\ mod\ N_B, \qquad (3)$$

рамзгузорӣ карда, тавассути хати алоқаи кушод, қимати e –ро ба Валӣ равон мекунад.

Қадами 2. Валӣ пайғоми рамзгузоштаро ба даст оварда, қимати

$$m^1 = e^{c_B}\ mod\ N_B \qquad (4)$$

-ро ҳисоб мекунад.

Тасдиқоти 1. Барои протоколи RSA $m' = m$ аст, яъне Валӣ пайғоми аслро аз Алӣ ба даст меорад.

Исбот. Аз тарзи сохтани протокол истифода мебарем

$$m' = e^{C_B} \, mod N_B = m^{d_B c_B} \, mod \, N_B$$

Баробарии (2) маънои онро дорад, ки барои ягон k баробарии зерин иҷро мегардад

$$C_B d_B = k \, \varphi_B + 1.$$

Бо назардошти функсияи Эйлер ҳосил мекунем.

$$\varphi_B = (P_B - 1)(Q_B - 1) = \varphi(N_B),$$

яъне дар ин ҷо $\varphi(\cdot)$ −функсияи Эйлер мебошад. Аз ин ҷо ва хосияти функсияи Эйлер ҳосил мекунем.

$$m' = m^{k\varphi(N_B)+1} \, mod \, N_B = m.$$

Тасдиқоти 2. (Хосияти протоколи RSA)

1) Протокол иттилоотро дуруст (корректно) рамзгузорӣ ва рамзкушоӣ мекунад.

2) Душман (злоумышленник) ҳангоми калон будани P ва Q ҳарчанд, ки ҳамаи иттилоот ва параметрҳои кушодаро низ ба даст оварад наметавонад пайғоми аслро ба даст орад.

Исбот. Исботи қисми аввали тасдиқот аз тасдиқи 1 бармеояд. Барои исботи қисми дуюми тасдиқот пайхас мекунем, ки душман танҳо параметрҳои N ва d − ро медонад. Барои ёфтани C он бояд қимати $\varphi = (P - 1)(Q - 1)$-ро донад, лекин барои ин талаб карда мешавад, ки параметрҳои P ва Q − ро низ донад. Умуман он метавонад

N-ро ба зарбкунандаҳо ҷудо карда P ва Q −ро ба даст орад, лекин ин масъала хеле душвор мебошад.

Функсияи яктарафаи $y = x^d \, mod \, N$ дар системаи RSA истифодашаванда функсияе мебошад, ки имконияти ба таври сода ҳисобкунии функсияи $x = \sqrt[d]{y} \, mod \, N$ −ро дар сурати маълум будани ҷудокуни N ба зарбшавандаҳо фароҳам меорад. (Дар ҳақиқат метавон ба содагӣ аввал қимати $\varphi = (P-1)(Q-1)$ ва боъд қимати $C = d^{-1} mod \, \varphi$ −ро ҳисоб кард). Агар P ва Q номаълум бошанд, он гоҳ ҳисобкунии қимати функсияи баръакс дар амалия ғайриимкон (душвор) мебошад. Чунин функсияҳои яктарафа дар дигар бахшҳои криптография низ татбиқ карда мешаванд.

Қайд мекунем, ки барои схемаҳои RSA, ба ҳар як муштарӣ зарур аст, ки ҷуфти ададҳои содаи P ва Q −и худро интихоб кунанд, яъне ҳамаи модулҳои $N_A, N_{B,\dots} N_C$ бояд гуногун бошанд. (дар акси ҳол як муштарӣ метавонад иттилооти барои муштарии дигар пешбинишударо хонад). Аммо ин аз параметри дуюми d талаб карда намешавад. Параметри d метавонад барои ҳамаи муштариён якхела бошад. Баъзан пешниҳод карда мешавад, ки $d = 3$ (бо мувофиқати P ва Q) интихоб карда шавад. он гоҳ рамзгузорӣ хеле зуд, танҳо бо иҷрои ду амали зарб иҷро карда мешавад.

Мисол. Фарз мекунем, ки Алӣ мехоҳад пайғоми $m = 15 -$ ро ба Валӣ равон кунад. Бигузор Валӣ параметрҳои зеринро интихоб карда бошад:

$$P_B = 3, \qquad Q_B = 11, \qquad N_B = 33, \qquad d_B = 3.$$

(3 бо $\varphi(33) = 20$ байниҳам сода мебошанд). Бо истифода аз алгоритми васеъкардашудаи Евклид, қимати C_B –ро меёбад.

$$C_B = 7$$

(санҷиш $3 \cdot 7 \; mod \; 20 = 1$). Пайғоми m –ро бо истифода бо формулаи (3) рамзгузорӣ мекунад:

$$e = 15^2 \cdot 15 \; mod \; 33 = 27 \cdot 15 \; mod \; 33 = 9$$

Ададӣ 9-ро Алӣ ба Валӣ тавассути канали алоқаи кушод равон мекунад. Танҳо Валӣ $C_B = 7$ –ро медонад, бинобар ин, бо истифодаи формулаи (4) пайғоми ба дастовардаашро рамзкушоӣ мекунад

$$m' = 9^2 \; mod \; 33 = 9^{2^2} \cdot 9^2 \; mod \; 33 = 15^2 \cdot 15 \cdot 9 \; mod \; 33 = 15$$

Ҳамин тариқ, Валӣ пайғоми Алиро рамзкушоӣ кард.

Як норасоии рамзи RSA –ро ҳангоми калон будани P ва Q дида мебароем. Бигузор Алӣ мехоҳад бо истифода аз параметрҳои кушодаи Валӣ (ададҳои N_B ва d_B) пайғомеро ба ӯ равона кунад. Дар ин ҳолат душман наметавонад, пайғоми барои Валӣ пешбинӣ шударо хонад, аммо метавонад, аз номи Алӣ ба Валӣ пайғом равон кунад. Барои ҳалли ин масъала аз протоколҳои

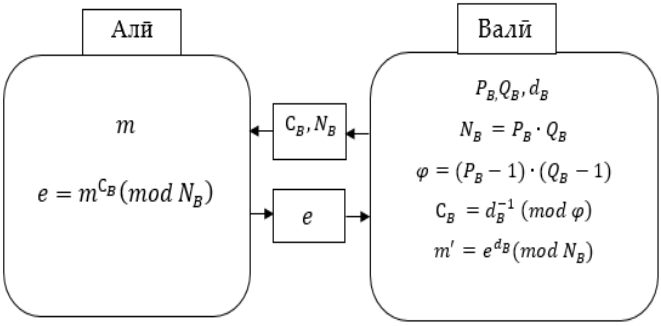
душвортаре истифода бурда мешавад, масалан ҳолати зерин.

Алӣ мехоҳад пайғоми m −ро ба Валӣ равон кунад. Ибтидо Алӣ адади $e = m^{C_A} \ mod \ N_A$ − ро ҳисоб мекунад. Душман бошад, ин амалро иҷро карда наметавонад, чунки C_A махфӣ мебошад. Пас аз ин, Алӣ қимати $f = e^{d_B} \ mod \ N_B$ −ро ҳисоб карда қиматашро ба Валӣ равон мекунад. Валӣ f −ро ба даст оварда, пайдарпай ададҳои $u = f^{C_B} \ mod \ N_B$ ва $\omega = u^{d_A} \ mod \ N_A$ ро ҳисоб мекунад.

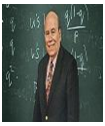
Дар натиҷа, Валӣ пайғом $\omega = m$ −ро ба даст меорад. Монанди схемаи муқаррарии RSA дар ин ҷо низ душман наметавонад, пайғомро хонад, аммо фарқияти асосӣ дар он аст, ки дар ин ҷо душман наметавонад аз номи Алӣ пайғом равон кунад. (Чунки адади махфии C_A − ро намедонад).

Дар ин ҷо мо ба ҳолати нав дучор омадем. Валӣ медонад, ки пайғом аз Алӣ омадааст, яъне Алӣ онро тавассути калиди махфии C_A рамзгузорӣ карда “имзо” гузоштааст. Ин мисоли “имзои электронӣ” ба ҳисоб меравад. Дар криптографияи муосир аз ин имзоҳо ба таври васеъ истифода бурда мешуд. Дар оянда “имзоҳои электронӣ”-ро пурратар дида мебароем.

Ба намуди схематикӣ ин алгоритм шакли зеринро дорад:



7. Алгоритми Рабин



Алгоритми Рабин[1] дар асоси масъалаи душвори факторизатсияи ададҳои калон асос ёфтааст, ки соли 1979 аз тарафи криптогарфи изроили Михаэл Ошер Рабин (нем. Michael Oser Rabin, ибр. מִיכָאֵל אשֶׁר רַבִּין,) сохта шудааст. Дақиқан, ин алгоритм бо масъалаи мураккаби ҳисобкунии решаи квадратӣ аз рӯйи модули ададии $N = p \cdot q$ алоқаманд мебошад. Бинобар ин, аз рӯйи баъзе муносибатҳо методи мазкур нисбат ба методи RSA устувортар мебошад. Қаблан дар боби 5 тарзи ҳисобкунии решаи квадратӣ аз

[1] Михаэл Рабин соли 1931 дар шаҳри Бреслау (пештар Вротслав), ба дунё омадааст. Соли 1953 дар донишгоҳи яҳудии Иерусалим магистратураро хатм кард. Соли 1956 дар донишгоҳи Принстонск рисолаашро ҳимоя карда доктори фалсафа шуд. Сар карда аз сентябри соли 2008 ӯ дар соҳаи бехатарии компютер корҳои татқиқотӣ бурда, дар донишгоҳҳои Иерусалим ва Гарвардия дарс мегӯяд. Дорои унвони фахрии дошишгоҳҳои Бордо (1996), Хайф (1996), донишгоҳи озоди (кушоди) Изроил (1999), донишгоҳи Бен-Гуриона (2000), донишгоҳи Вротслав (2007).

рӯйи модули додашударо мавриди баҳс қарор дода будем. Ҳоло бошад, алгоритми Рабинро мухтасар мавриди баҳс қарор медиҳем. Моҳияти алгоритми мазкур чунин аст:

Ду ададӣ содаи гуногун тавре интихоб карда мешаванд, ки баробарии зеринро қаноат кунонанд:

$$p = q = 3(mod\ 4).$$

Чунин интихоби махсус, аз рӯйи модулҳои p ва q ҷараёни аз реша барориро хеле тез мегардонад. Калиди махфӣ дар рамзи мазкур ҷуфти ададҳои (p, q) ба ҳисоб мераванд. Калиди ошкор бошад, ҳосили зарби калидҳои махфӣ $N = p \cdot q$ ва интихоби ададии тасодуфии $B \in \{0, 1, 2, \dots, N-1\}$ мебошад, яъне ҷуфти ададҳои (N, B) калиди кушода ба ҳисоб мераванд.

Барои рамзгузории матни $m < N$ аз формулаи зерин истифода бурда мешавад:

$$C = m \cdot (m + B)(mod\ N) \qquad (1)$$

Қайд кардан ба маврид аст, ки амали рамзгузорӣ аз амалҳои ҷамъ ва зарб аз рӯйи модули N ташкил ёфтааст. Бинобар ин, суръати разгузорӣ дар муқоиса бо методи RSA тезтар мебошад.

Барои рамзкушоӣ бошад, аз формулаи

$$m = \sqrt{\frac{B^2}{4} + C} - \frac{B}{2}\ (mod\ N) \qquad (2)$$

истифода бурда мешавад.

Азбаски N ҳосили зарби ду ададӣ содаи p ва q мебошад, бинобар ин, чор ҳолати (имконияти) решаи

квадратӣ аз рӯйи модули N мавҷуд аст. Аз ин рӯ, ҳангоми рамзкушоӣ чор варианти матни ошкор ба даст меояд.

Бе душвори метавон дид, ки ҳангоми рамзкушоӣ матни ошкор ба даст меояд. Дар ҳақиқат, қимати C-ро аз формулаҳои (1) ба (2) гузошта ҳосил мекунем:

$$\sqrt{\frac{B^2}{4}+C}-\frac{B}{2}=\sqrt{\frac{B^2+4m(m+B)}{4}}-\frac{B}{2}$$
$$=\sqrt{\frac{4m^2+4mB+B^2}{4}}-\frac{B}{2}=\sqrt{\frac{(2m+B)^2}{4}}-\frac{B}{2}$$
$$=\frac{2m+B}{2}-\frac{B}{2}=m.$$

Дар ин ҷо интихоби решаи дуруст, аз байни ҳамаи ҳолатҳои имконпазир фарз карда шудааст.

Мисол. Бигузор калидҳои кушода ва пушида шакли зеринро дошта бошанд:

$$p=127,\quad q=131,\quad N=16\,637,\quad B=12\,345.$$

Барои рамзгузории пайғоми $m=4410$ аз формулаи (1) истифода бурда ҳосил мекунем.

$$C=m(m+B)(mod\ N)=4633.$$

Барои рамзкушоӣ бошад, ибтидо қимати

$$T=\frac{B^2}{4}+C(mod\ N)=1500$$

$-$ро ба даст оварда, аз рӯйи модули p ва q решаи $T-$ро ҳисоб мекунем:

$$\sqrt{T}(mod\ p)=\pm 22,\qquad \sqrt{T}(mod\ q)=\pm 37.$$

Пас аз ин, бо истифода аз ТЧБ аз ҷуфти

$$\pm 22\ (mod\ p)\ \text{ ва }\pm 37\ (mod\ q)$$

решаи квадратии адади T −ро (аз рӯй модули N) меёбем:

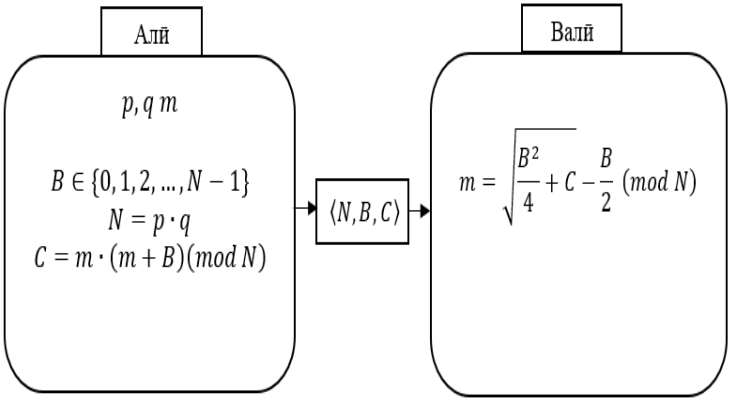
$$s = \sqrt{T}(mod\ N) = \pm 3705 \quad ё \quad \pm 14\ 373$$

Дар ин ҷо чор варианти рамзкушой

$$4410,\ 5851,\quad 15\ 078\ ё\ 16\ 519$$

аз формулаи $s - \frac{B}{2} = s - \frac{12345}{2}$ ба даст меояд.

Намуди схематикии ин алгоримт чунин аст:



Саволҳо барои мустаҳкамкунӣ

1. Чи чиз боиси пайдоиши методҳои криптографии бо калидҳои кушода шуд?
2. Алгоритми Диффи-Ҳеллман чӣ гуна алгоритм аст ва кай сохта шудааст?
3. Ду муштари Алӣ ва Валӣ бо истифода аз алгоритми Диффи-Ҳеллман чӣ тавр метавонанд калиди умумӣ созанд?

4. Оё метавон алгоритми Диффи-Ҳеллман-ро барои се ва ё зиёда муштари истифода кард?
5. Рамзи Шамир кай сохта шуд ва чӣ тавр тавассути он итилоот рамзгузорӣ карда мешавад?
6. Рамзи Ал-Ҷамо аз рамзи Шамир чӣ фарқ дорад?
7. Моҳияти рамзи RSA аз чӣ иборат аст?
8. Оё рамзи RSA аз рамзи Ал-Ҷамол ва Шамир ягон бартари дорад?
9. Рамзи Рабин кай сохта шуд ва моҳияти он аз чӣ иборат аст?
10. Ҳангоми рамзкушой чи тавр варианти дуруст интихоб карда мешавад?

Боби 9. Имзоҳои электронӣ-рақамӣ

Маълумот оиди имзои электронӣ

Пас аз пайдоиши методҳои рамзгузорӣ бо калидҳои кушода, инқилоби бузурге дар шабака ва технологияҳои муосир ба вуҷуд омад. Дар ин ҳангом имконияти ҳалли масъалаҳое, ки солҳо ҳалнашаванда буданд, пайдо гашта, дар амалия татбиқи хеле зиёд пайдо карданд. Яке аз воситаҳои муҳиме, ки дар ин давра ба вуҷуд омад, ин имзои электронӣ ё рақамӣ мебошад. Дар бисёр кишварҳои ҷаҳон аз ҷумла Россия оиди имзои электронӣ (рақамӣ) стандарт қабул карда шуда, ин мафҳум дар қонунгузории шаҳрвандӣ низ истифода бурда мешавад.

Пеш аз мавриди баҳс қарор додани методҳои криптографӣ дар имзоҳои электронӣ се хосияти асосии имзои электронӣ (ҳатто имзои дастӣ) – ро дида мебароем.

1) Ҳуҷҷатҳоро танҳо соҳибони “қонунӣ” метавонанд имзо гузоранд (яъне ҳеҷ кас наметавонад аз номи (ҷойи) дигар кас имзо гузорад.
2) Соҳиби имзо метавонад аз он даст кашад.
3) Дар ҳолати пайдошавии баҳс барои муайянкунии соҳияти имзо шахси сеюм, масалан, судя метавонад низ иштирок кунад.

Имзоҳои электронӣ бояд ҳамаи ин хосиятҳоро доро бошанд. Баръакси имзоҳои дастӣ соҳибони имзоҳои рақамӣ метавонанд аз ҳамдигар дар масофаи ҳазорҳо

километр дур ҷойгир бошанд ва бо ҳамдигар тавассути шабака мубодилаи иттилоот кунанд.

Ба ғайр аз имзоҳои муқарарӣ, дар дунёи воқеӣ имзоҳои дигаре, ки имзоҳои нотариалӣ ном доранд низ мавҷуданд. Дар имзоҳои мазкур шахси муайяне (нотариус) тавассути муҳр ва имзоҳои худ ҳуҷҷатҳоро тасдиқ мекунад. Пас аз ин, дилхоҳ шахси дигар метавонад ба соҳибияти онҳо гувоҳӣ диҳад. Имзои электронии нотариалӣ, айнан монанди имзоҳои дигар амалӣ карда мешавад (гузошта мешавад).

Барои ба моҳияти имзоҳои электронӣ сарфаҳм рафтан, ибтидо ҳэш-функсияҳо ва сипас якчанд алгоритми сохтани имзои элктронӣ-рақамиро мавриди баҳс қарор медиҳем.

Ҳэш-функсияҳо

Ҳэш-функсия (hash function) дар ҳимояи иттилоот роли муҳим бозида, барои ҳимояи ҳуҷҷатҳои электронӣ аз модификатсия ва тағйирдиҳӣ сохта шудааст. Бо маънои том функсияи ҳэширонӣ ё ҳэш-функсия гуфта, чунин функсияи Н-ро меноманд, ки хосиятҳои зеринро қаноат мекунонад:

1) Барои блоки дилхоҳ дарозӣ доштаи итилоот татбиқшаванда будан.
2) Ба сифати натиҷа ҳосил кардани дарозии қайд кардашуда (масалан, дар функсияи ҳэширонии класикии MD5 -128 бит, дар стандартӣ амрикоии SHA-160 бит).

3) Нисбатан тез будани ҳисобкунии қимати $H = h(M)$ (дар вақти полиномалӣ аз дарозии пайғоми М).
4) Аз рӯӣ Н-и додашуда ёфтани чунин М, ки $h(M) = M$ шавад ғайриимкон будан.
5) Номумкин будан аз рӯйи ҳисобкунӣ барои дилхоҳ y ёфтани чунин x, ки $y = h(x)$ шавад.
6) Ғайриимкон будани ёфтани ҷуфти дилхоҳи (x, y), ки $H(y) = H(x)$ шавад.

Ҳэш-функсияе, ки фақат 5 хосияти авваларо қаноат мекунонад, ҳэш-функсияи сода ё суст номида мешавад.

Ҳэш-функсияи устувор ҳэшфункснояст, ки ҳамаи хосиятҳои 1-6-ро қаноат мекунонад.

Барои ҳисобкунии ҳэш-функсия усулҳои зиёде мавҷуданд. Ҳоло як усули содатаринро дида мебароем. Бигузор пайғоми M дода шуда бошад, барои ҳисобкунии ҳэш-функсияи он, яъне $H(M)$ аз формулаи зерин истифода бурда мешавад.

$$H_i = (H_{i-1} + M_i)^2 \ mod \ n \qquad (1)$$

дар ин ҷо M_i – қимати ададии ҳарфҳои (символҳои) матни додашуда, n ягон ададӣ сода мебошад. H_i дорои хосиятҳои зерин мебошад.

$$\mathrm{H}_0 = 0;$$
$$\mathrm{H}_1 = (\mathrm{H}_0 + M_1)^2;$$
$$\mathrm{H}_2 = (\mathrm{H}_1 + M_2)^2;$$
$$\mathrm{H}_3 = (\mathrm{H}_2 + M_3)^2;$$
$$\dots \dots \dots \dots \dots$$
$$\mathrm{H}_k = (\mathrm{H}_{k-1} + M_k)^2;$$

Мисоли 1. Ҳэш-функсияи матни КАРИМ бо истифода аз калиди $n = 91$ ҳисоб карда шавад.

Символҳои матни додашудаи M_i	Қимати ададии символҳои M_i	$H_0 = 0$
К	12	$H_1 = (H_0 + M_1)^2 \ mod$ n=(0+12)² mod 91=53
А	1	$H_2 = (H_1 + M_2)^2 \ mod$ n=(53+1)² mod 91=4
Р	18	$H_3 = (H_2 + M_3)^2 \ mod$ n=(4+18)² mod 91=29
И	9	$H_4 = (H_3 + M_4)^2 \ mod$ n=(29+9)² mod 91=79
М	14	$H_5 = (H_4 + M_5)^2 \ mod$ n=(79+14)² mod 91=4

Аз ин ҷо қимати ҳэш-функсия ба $H(M) = H_5 = 4$ баробар мешавад.

Мисоли 2. Ҳэш-функсияи матни МАША-ро бо истифода аз калиди (5, 91) ҳисоб карда шавад.

Символҳои матни додашудаи M_i	Қимати ададии символҳои M_i	$H_0 = 0$
М	14	$H_1 = (H_0 + M_1)^2 \ mod$ n=(0+14)² mod 91=14
А	1	$H_2 = (H_1 + M_2)^2 \ mod$ n=(14+1)² mod 91=43
Ш	26	$H_3 = (H_2 + M_3)^2 \ mod$ n=(43+26)² mod 91=29
А	1	$H_4 = (H_3 + M_4)^2 \ mod$ n=(29+1)² mod 91=81

Аз ин ҷо қимати ҳэш-функсия ба $H(M) = \mathrm{H}_4 = 81$ баробар мешавад.

1. Алгоритми MD5

MD5 (англ. Message Digest) алгоритми ҳэширонии 128 бити буда, соли 1991 аз тарафи Р.Ривест корманди донишкадаи Массачусетский (ИМА) сохта шудааст. Алгоритми мазкур барои сохтани нақш ё дейджести пайғоми дарозии дилхоҳ дошта истифода шуда, версияи беҳтаркардашудаи (аз нуқтаи назари бехатарӣ) алгоритм ба ҳисоб меравад. Қаблан алгоритмҳои MD1, MD2 ва ғайра мавҷуд буданд. Ин алгоритмро барои тафтиши соҳибияти пайғомҳои нашршуда тавассути муқоисаи дейджести пайғом (бо нашри ҳэшҳо) истифода бурда мешавад.

Алгоритм тавре сохта шудааст, ки дар протсессорҳои 32 разрияда тез кор мекунад. Дар алгоритм ҷадвалҳои ҷойгузории бисёр истифода бурда намешавад.

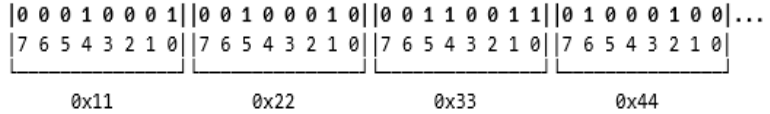
Ҳангоми тавзеҳи алгоритм зери мафҳуми калима пайдарпайии 32-бита фаҳмида мешавад.

Пайдарпайии битҳо метавонанд ҳамчун пайдарпайии байтҳо, ки ҳар кадомашон ба 8 бит баробар мебошанд, инъикос карда шаванд. Дар дохили байт битҳо бо чунин шакл гузошта мешаванд: ибтидо (аз тарафи чап) байтҳое маънои бештар дошта (битҳои калон, ки дорои дараҷаи дӯӣ калон мебошанд: $2^7, 2^6, \ldots$) дар охир (тарафи рост) битҳои маънои камтар дошта (битҳои хурд, ки бо $2^2, 2^1, 2^0$ мувофиқанд). Чунин тартиби гузаштани бит (ё

байт) big-endian (тартиб аз калон ба хурд) номида мешавад.

Пайдарпайии байтҳоро метавонад, ҳамчун пайдарпайии калимаҳои 32-бита интерпритатсия кард, дар ин ҷо ҳар як пайдарпайии гурӯҳи аз чор байт як калимаро ифода мекунад. Дар дохили калима байтҳо чунин гузошта мешаванд: ибтидо байтҳои маънои камтар дошта, сипас маънои зиёдтар. Чунин тартиби гузориши бит (ё байт) ittle-endian (тартиб аз хурд ба калон) номида мешавад.

Масалан, агар пайдарпайии битҳо (қайд карда шуда) чунин дода шуда бошанд.



Онгоҳ онро метавон ҳамчун 4 байтҳои гузошташуда ($0 \times 11, 0 \times 22, 0 \times 33, 0 \times 44$ -ададҳои шонздаҳӣ) ё ҳамчун калимаи 0×44332211инъикос (тасвир) кард.

Бигузор $'+'$ – амали ҷамъро аз рӯйи модули 2^{32} ифода кунад, яъне $a + b \equiv (a + b)(mod\ 2^{32})$. Бигузор ифодаи $'X \ll s'$–лағжиши даврии адади X –ро ба андозаи s ба тарафи чап ифода кунад.

Шарҳи алгоритм

Бигузор пайғоми M, ки дарозиаш ба b баробар аст дода шуда бошад ва ҳисобкунии ҳэш-функсияи он талаб карда шавад. Дар ин ҷо адади b –ягон адади мусбат мебошад (каратии 8 будани он шарт нест). Пас метавон

пайғоми M-ро ба намуди пайдарпайии битҳои $m_0, m_1, \dots, m_{b-2}, m_{b-1}$ инъикос кард.

Барои ҳисобкунии ҳэш-функсияи қадамҳои зеринро иҷро мекунем:

Қадами 1. Ҳамроҳкунии битҳои иловагӣ. Дар охири пайғом бити '1' илова карда, пас аз он то замоне, ки дарозии пайғоми ҳосилшуда L шарти $L \equiv 448 (\mathrm{mod}\ 512)$–ро қаноат кунонидан бити сифрӣ ('0') ҳамроҳ карда мешавад. Ҳамин тариқ, метавон аз 1 то 512 бит ҳамроҳ кард.

Пас аз ин, лозим аст, ки пайғомро аз пайдарапайии битҳо, ки ба шакли байтҳо гурӯҳбанди шудааст, ба пайдарпайии калимаҳо, бо назардошти қоидаи little-endian табдил дод.

Қадами 2. Иловакунии дарозии пайғоми ибтидоӣ. Дар охири натиҷаи аз қадами 1 ҳосилшуда 64 бити хурд, ки аз шакли дӯии адади (пайғоми ибтидоӣ) ҳосил шудааст, илова карда мешавад. Дар ин ҳангом аввал 4 байти хурд, ва сипас байтҳои калон навишта мешаванд. Дар натиҷа пайғоме ҳосил мешавад, ки дарозиаш ба 512 бит баробар аст, яъне пайғоме ҳосилшударо метавон ба блокҳое, ки шакли калимаи 32 битаи шонздаҳиро доранд: $M_0, M_1, \dots, M_{N-1}$ (дар ин ҷо N каратии 16 аст) тақсим кард.

Қадами 3. Қимати ибтидоӣ бахшидан ба буфер. Буфер аз 4 калимаҳои 32-битаи (A, B, C, D) иборат буда, барои ҳисобкунии ҳэш-функсия истифода мешавад. Дар ибтидоӣ кори алгоритм ба буфер қиматиҳои ибтидоии зерин бахшида мешаванд.

A: 01 23 45 67, яъне A = 0x67452301
B: 89 AB CD EF, яъне B = 0xEFCDAB89
C: FE DC BA 98, яъне C = 0x98BADCFE
D: 76 54 32 10, яъне D = 0x10325476

Илова бар ин, чор функсияе, ки дар оянда истифода мешаванд, муайян карда мешаванд. Дар ин ҷо $'\wedge'$, $'\vee'$, $'\neg'$, ва $'\oplus'$ амалҳои битӣ мебошанд.

$$F(x,y,z) = (x \wedge y) \vee (\neg x \wedge z)$$
$$G(x,y,z) = (x \wedge z) \vee (\neg z \wedge y)$$
$$H(x,y,z) = x \oplus y \oplus z$$
$$I(x,y,z) = y \oplus (\neg z \vee x)$$

Дар охир ҷадвали доимиҳои $T[1 \ldots 64]$ муайян карда мешавад, дар ин ҷо элементи i–юм тавассути формулаи зерин муайян карда мешавад.

$$T[i] = int(4\,294\,967\,296 \cdot |\sin(i)|),$$

дар ин ҷо i бо радиан буда, $4\,294\,967\,296 = 2^{32}$. мебошад.

Қадами 4. Даври (сикли) асосӣ. Ҳар як қадами сикли дохилӣ (аз рӯӣ параметри i) аз коркарди як блоки 512 битаи блоки пайғом иборат мебошад.

```
 for i = 0 to N/16-1 do
// Нусхабардории блоки i-юми пайғом ба массиви X
     For j = 0 to 15 do
       X[j] = M[i*16 + j].
 end
  // Сабти қимати ҷории буфер
AA = A
BB = B
CC = C
DD = D
```

```
  // Раунди 1
// Бигузор навишти [abcd k s i] табдилдихии зеринро ифода кунад:
// a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s)
// 16 табдилдихии зерин ичро карда мешавад
[ABCD  0 7  1] [DABC  1 12  2] [CDAB  2 17  3] [BCDA  3 22 4]
[ABCD  4 7  5] [DABC  5 12  6] [CDAB  6 17  7] [BCDA  7 22 8]
[ABCD  8 7  9] [DABC  9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]
  // Раунди 2
 // Бигузор навишти [abcd k s i] табдилдихии зеринро ифода кунад:
// a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s)
// 16 табдилдихии зерин ичро карда мешавад
[ABCD  1 5 17] [DABC  6 9 18] [CDAB 11 14 19] [BCDA  0 20 20]
[ABCD  5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA  4 20 24]
[ABCD  9 5 25] [DABC 14 9 26] [CDAB  3 14 27] [BCDA  8 20 28]
[ABCD 13 5 29] [DABC  2 9 30] [CDAB  7 14 31] [BCDA 12 20 32]
  // Раунди 3
// Бигузор навишти [abcd k s i] табдилдихии зеринро
```

```
ифода кунад:
// a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s)
 //онгоҳ 16 табдилдиҳии зерин иҷро карда мешавад
[ABCD  5 4 33] [DABC  8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD  1 4 37] [DABC  4 11 38] [CDAB  7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC  0 11 42] [CDAB  3 16 43] [BCDA  6 23 44]
[ABCD  9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA  2 23 48]
  // Раунд 4
// Бигузор навишти [abcd k s i] табдилдихии зеринро ифода кунад:
// a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s)
// онгоҳ 16 табдилдиҳии зерин иҷро карда мешавад
[ABCD  0 6 49] [DABC  7 10 50] [CDAB 14 15 51] [BCDA  5 21 52]
[ABCD 12 6 53] [DABC  3 10 54] [CDAB 10 15 55] [BCDA  1 21 56]
[ABCD  8 6 57] [DABC 15 10 58] [CDAB  6 15 59] [BCDA 13 21 60]
[ABCD  4 6 61] [DABC 11 10 62] [CDAB  2 15 63] [BCDA  9 21 64]
  // Ба қимати буфери ҷорӣ қимати буфер ҳамроҳ карда мешавад
//Блоки ҷории пайғом дар ибтидоӣ коркард сабт карда мешавад
```

```
A = A + AA
B = B + BB
C = C + CC
D = D + DD
End.
```

Қадами 5. Қимати ҳисобкунии ҳэш-функсия битҳои калимаҳои A, B, C, D мебошанд, яъне битҳои натиҷа ки аз битҳои хурди байти A оғоз гардида, ба битҳои калони калимаи D ба охир мерасад.

Алгоритми коркарди пайғом ба намуди псевдокод шакли зеринро дорад:

```
var int[64] s, K
//s specifies the per-round shift amounts
s[ 0..15] := { 7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22,
7, 12, 17, 22 }
s[16..31] := { 5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20,  5,
9, 14, 20 }
s[32..47] := { 4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23,
4, 11, 16, 23 }
s[48..63] := { 6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21,
6, 10, 15, 21 }
//Use binary integer part of the sines of integers
(Radians) as constants:
for i from 0 to 63
   K[i] := floor(232 × abs(sin(i + 1)))
end for
//(Or just use the following precomputed table):
K[ 0.. 3] := { 0xd76aa478, 0xe8c7b756, 0x242070db,
```

0xc1bdceee }
K[4.. 7] := { 0xf57c0faf, 0x4787c62a, 0xa8304613, 0xfd469501 }
K[8..11] := { 0x698098d8, 0x8b44f7af, 0xffff5bb1, 0x895cd7be }
K[12..15] := { 0x6b901122, 0xfd987193, 0xa679438e, 0x49b40821 }
K[16..19] := { 0xf61e2562, 0xc040b340, 0x265e5a51, 0xe9b6c7aa }
K[20..23] := { 0xd62f105d, 0x02441453, 0xd8a1e681, 0xe7d3fbc8 }
K[24..27] := { 0x21e1cde6, 0xc33707d6, 0xf4d50d87, 0x455a14ed }
K[28..31] := { 0xa9e3e905, 0xfcefa3f8, 0x676f02d9, 0x8d2a4c8a }
K[32..35] := { 0xfffa3942, 0x8771f681, 0x6d9d6122, 0xfde5380c }
K[36..39] := { 0xa4beea44, 0x4bdecfa9, 0xf6bb4b60, 0xbebfbc70 }
K[40..43] := { 0x289b7ec6, 0xeaa127fa, 0xd4ef3085, 0x04881d05 }
K[44..47] := { 0xd9d4d039, 0xe6db99e5, 0x1fa27cf8, 0xc4ac5665 }
K[48..51] := { 0xf4292244, 0x432aff97, 0xab9423a7, 0xfc93a039 }
K[52..55] := { 0x655b59c3, 0x8f0ccc92, 0xffeff47d, 0x85845dd1 }
K[56..59] := { 0x6fa87e4f, 0xfe2ce6e0, 0xa3014314,

```
0x4e0811a1 }
K[60..63] := { 0xf7537e82, 0xbd3af235, 0x2ad7d2bb,
0xeb86d391 }
//Initialize variables:
var int a0 := 0x67452301   //A
var int b0 := 0xefcdab89   //B
var int c0 := 0x98badcfe   //C
var int d0 := 0x10325476   //D
//Pre-processing: adding a single 1 bit
append "1" bit to message
//Pre-processing: padding with zeros
append "0" bit until message length in bits ≡ 448
(mod 512)
append original length in bits mod (2 pow 64) to
message
//Process the message in successive 512-bit chunks:
for each 512-bit chunk of message
   break chunk into sixteen 32-bit words M[j], 0 ≤ j ≤
15
//Initialize hash value for this chunk:
   var int A := a0
   var int B := b0
   var int C := c0
   var int D := d0
  //Main loop:
   for i from 0 to 63
      if 0 ≤ i ≤ 15 then
         F := (B and C) or ((not B) and D)
```

```
        g := i
    else if 16 ≤ i ≤ 31
        F := (D and B) or ((not D) and C)
        g := (5·i + 1) mod 16
    else if 32 ≤ i ≤ 47
        F := B xor C xor D
        g := (3·i + 5) mod 16
    else if 48 ≤ i ≤ 63
        F := C xor (B or (not D))
        g := (7×i) mod 16
//Be wary of the below definitions of a,b,c,d
    dTemp := D
    D := C
    C := B
    B := B + leftrotate((A + F + K[i] + M[g]), s[i])
    A := dTemp
  end for
//Add this chunk's hash to result so far:
  a0 := a0 + A
  b0 := b0 + B
  c0 := c0 + C
  d0 := d0 + D
end for
var char digest[16] := a0 append b0 append c0 append
d0 //(Output is in little-endian)
//leftrotate function definition
leftrotate (x, c)
  return (x << c) binary or (x >> (32-c));
```

Барномаи ҳисобкунии қимати ҳэш-функсияи пайғоми додашуда тавассути алгоритми MD5 дар забони Java шакли зеринро дорад:

```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
public static String md5Custom(String st) {
  MessageDigest messageDigest = null;
  byte[] digest = new byte[0];
    try {
       messageDigest =
MessageDigest.getInstance("MD5");
       messageDigest.reset();
       messageDigest.update(st.getBytes());
       digest = messageDigest.digest();
      } catch (NoSuchAlgorithmException e) {
         e.printStackTrace();
    BigInteger bigInt = new BigInteger(1, digest);
    String md5Hex = bigInt.toString(16);
    while( md5Hex.length() < 32 ){
     md5Hex = "0" + md5Hex;
    }
    return md5Hex;
public static void main(String[] args) {
  String st = "abc";
  System.out.println("Custom MD5:");
  System.out.println(md5Custom(st));
}
```

Мисоли қиматҳои ҳэш-функсия (ба намуди шонздаҳӣ):

1) MD5 ("") = d41d8cd9 8f00b204 e9800998 ecf8427e 2)
2) MD5 ("abc") = 90015098 3cd24fb0 d6963f7d 28e17f72
3) MD5("12345678901234567890123456789012345678901234567890123456789012 34567890123456789012345678901234567890") = 57edf4a2 2be3c955 ac49da2e 2107b67a

3. Оилаи алгоритмҳои SHA

Оилаи алгоритмҳои *SHA* (Secure hash standard) дорои 5 алгоритми ҳисобкунии ҳэш-функсия мебошад: SHA—1, SHA-224, SHA-256, SHA-384, SHA—512. Чор ҳэш-функсияи охирон зеролаи SHA—2-ро ташкил мекунанд. Алгоритми SHA-1-ро соли 1995 хадамоти (агентии) милии бехатарии *ИМА* (NSA) кор кард кардааст. Алгоритмҳои зеролаи *SHA-2* низ аз ҷониби NSA сохта шуда, дуюми августи соли 2002 институти миллии стандартҳо ва технологияҳо дар стандарти федералии коркарди иттилоот FIPS PUB 180-2 мунташир (чоп карда) шудааст. Ин алгоритмҳо дар *SSL, SSH, S/MIME,* DNSSEC, *X.509, PGP* ва IPSec барои мубоилаи (равон кардани) файлҳо бо шабака (BitTorrent) истифода бурда мешаванд.

Алгоритмҳои оилаи *SHA* байниҳам танҳо аз рӯйи устувории криптографие, ки ҳэширонидани додаҳоро таъмин мекунад ва андозаи блок ва калимаи додаҳое, ки ҳангоми ҳэширронӣ истифода мешаванд, фарқ

мекунанд. Фарқияти асосии байни ин алгоритмҳо дар ҷадвали зерин оварда шудааст.

Алгоритм	Дарозии дейджести пайғом (бит)	Дарозии ҳолати дохилии пайғом (бит)	Дарозии блок (бит)	Дарозии пайғом (бит)	Дарозии калима (бит)	Миқдори итератсияҳо дар давр
SHA-1	160	160	512	$< 2^{64}$	32	80
SHA-224	224	256	512	$< 2^{64}$	32	64
SHA-256	256	256	512	$< 2^{64}$	32	64
SHA-384	384	512	1024	$< 2^{128}$	64	80
SHA-512	512	512	1024	$< 2^{128}$	64	80

Барои табдилдиҳии пайдарпайии битҳо ба байт ва калима аз тартиби ҷойгиршавии битҳо big-endian (монанди MD5) истифода бурда мешавад.

Хосияти алгоритмҳои SHA

Ҳоло алгоритми SHA-1-ро дида мебароем. Дар ин алгоритм (умуман дар ҳамаи алгоритмҳои оидаи SHA) аз амалҳои битии $'\wedge'$, $'\vee'$, $'\neg'$, $'\oplus'$, $\gg'$ ва $'\ll'$ истифода бурда мешавад. Зери мафҳуми + амали ҷамъ аз рӯйи модули 2^{32} фаҳмида мешавад, яъне $(x + y)\ (mod\ 2^{32})$.

Илова бар ин, аз ишораҳои зерин барои амали лағжиш (кӯчиш) истифода бурда мешавад.

- ✓ лағжиш ба рост $SHR^n \equiv x \gg n$;
- ✓ лағжиши даврӣ ба рост $ROTR^n(x) \equiv (x \gg n) \vee (x \ll w - n)$, дар ин ҷо w–дарозии калима;
- ✓ лағжиши даврӣ ба чап $ROTL^n(x) \equiv (x \ll n) \vee (x \gg w - n)$, дар ин ҷо w–дарозии калима;

Дар алгоритм аз функсияи зерин низ истифода бурда мешавад:

- $Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$,
- $Parity(x, y, z) = x \oplus y \oplus z$,
- $Parity(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$.
- $f(x, y, z) = \begin{cases} Ch(x, y, z), & 0 \le t \le 19, \\ Parity(x, y, z), & 20 \le t \le 39, \\ Maj(x, y, z), & 40 \le t \le 59, \\ Parity(x, y, z), & 60 \le t \le 79, \end{cases}$

Шарҳи алгоритм

Мисол. Бигузор пайғоми M, ки дарозиаш ба l бит баробар аст, дода шуда бошад, ва ҳисобкунии ҳэш-функсияи он талаб карда шавад.

Барои ҳисобкунии ҳэш-функсияи қадамҳои зеринро иҷро мекунем:

Қадами 1. Ҳамроҳкунии битҳои иловагӣ. Дар охири пайғом бити '1' илова карда, пас аз он то замоне, ки дарозии пайғоми ҳосилшуда L шарти $L \equiv 448 (mod\ 512)$–ро қаноат кунонидан бити сифрӣ ('0')

ҳамроҳ карда мешавад. Ҳамин тариқ, метавон аз 1 то 512 бит ҳамроҳ кард.

Қадами 2. Иловакунии дарозии пайғоми ибтидоӣ. Дар охири натиҷаи аз қадами 1 ҳосилшуда 64 бити хурд, ки дар охири он шакли дӯии дарозии пайғоми асл низ иштирок мекунад, ҳамроҳ карда мешавад. Масалан, агар дарозии калима ба 32 бит баробар бошад, он гоҳ пайғоми "abc", ки дарозиаш ба 24 бит баробар аст, ба сурати зерин пурра карда мешавад.

$$\underbrace{01100001}_{"a"}\ \underbrace{01100010}_{"b"}\ \underbrace{01100011}_{"c"}\ 1\ \overbrace{00\ldots00}^{423}\ \overbrace{00..0\ \underbrace{11000}_{i=24}}^{64}$$

Пайғоми ҳосилшуда ба блокҳои дарозиашон ба 512 бит баробар, ки бо $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$ ишора шудаанд, тақсим карда мешавад. Ҳар як блок ба 16-то блоки калимаи 32-битӣ, ки ишораи $M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)}$–ро доранд тақсим карда мешавад.

Қадами 3. Муайянкунии доимӣ. Алгоритми SHA-1 80-то пайдарпайии калимаҳои 32 бити $(K_0, K_1, \ldots, K_{79})$ -ро истифода мебарад, ки шакли 16-даҳии онҳо чунин аст:

$$K_t = \begin{cases} 5a827999, & 0 \le t \le 19, \\ 6ed9eba1, & 20 \le t \le 39, \\ 8f1bbcdc, & 40 \le t \le 59, \\ ca62c1d6, & 60 \le t \le 79. \end{cases}$$

Ба сифати қимати ибтидоии ҳэш-функсия доимиҳои зерин истифода бурда мешаванд.

$$H_0^{(0)} = 6745201, \quad H_1^{(0)} = efcdab89,$$
$$H_2^{(0)} = 98badcfe, \quad H_3^{(0)} = 10325476,$$
$$H_4^{(0)} = c3d2e1f0.$$

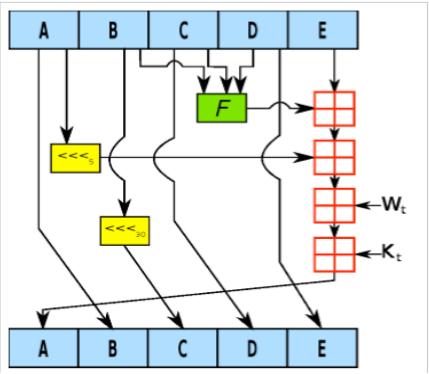
Қадами 4. Даврӣ асосӣ. Дар даври зерин пайдарпай ҳамаи блокҳои пайғоми иловакардашуда ҳисоб карда мешаванд.

For i = 1 to N
{
//1. Тайёркунии руйхати табдилдиҳии калимаҳои пайғом
$W_t = \begin{cases} M_t, & 0 \le t \le 15, \\ ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}, & 16 \le t \le 79. \end{cases}$
// 2. Қимати аввала бахшидан ба тағйирёбандаҳои корӣ
$a = H_0^{(i-1)} \quad b = H_1^{(i-1)} \quad c = H_2^{(i-1)} \quad d = H_3^{(i-1)} \quad e = H_3^{(i-1)}$
// 3. Даври дохилӣ
For t = 0 to 79
{
$T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_t$
e = d
d = c
$c = ROTL^{30}(b)$
b = a
a = T
}
// 4. Ҳисобкунии қиматҳои фосиавии ҳэш-функсияи
$H_0^{(i)} = a + H_0^{(i-1)} \quad H_1^{(i)} = b + H_1^{(i-1)}$
$H_2^{(i)} = c + H_2^{(i-1)} \quad H_3^{(i)} = d + H_3^{(i-1)}$
$H_4^{(i)} = e + H_4^{(i-1)}$
}

Қадами 5. Натиҷа. Дар охир қимати ҳэш-функсияи ҳамаи пайғом чунин шаклро мегирад:

$$H_0^{(N)} || H_1^{(N)} || H_2^{(N)} || H_3^{(N)} || H_4^{(N)}$$

Ба намуди схематики алгоритми SHA1 шакли зеринро дорад:



Шакли пурраи псевдокоди алгоритми шакли зеринро дорад:

```
//Initialize variables:
h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0
ml = message length in bits (always a multiple of the number of bits in a character).
Pre-processing:
append the bit '1' to the message e.g. by adding 0x80 if message length is a multiple of 8 bits.
append 0 ≤ k < 512 bits '0', such that the resulting message length in bits
   is congruent to −64 ≡ 448 (mod 512)
append ml, the original message length, as a 64-
```

```
bit big-endian integer. Thus, the total length is a
multiple of 512 bits.
//Process the message in successive 512-bit chunks:
break message into 512-bit chunks
for each chunk
   break chunk into sixteen 32-bit big-endian
words w[i], 0 ≤ i ≤ 15
 // Extend the sixteen 32-bit words into eighty 32-bit
words:
   for i from 16 to 79
      w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-
16]) leftrotate 1
  // Initialize hash value for this chunk:
   a = h0
   b = h1
   c = h2
   d = h3
   e = h4
  // Main loop:
   for i from 0 to 79
      if 0 ≤ i ≤ 19 then
         f = (b and c) or ((not b) and d)
         k = 0x5A827999
      else if 20 ≤ i ≤ 39
         f = b xor c xor d
         k = 0x6ED9EBA1
      else if 40 ≤ i ≤ 59
         f = (b and c) or (b and d) or (c and d)
         k = 0x8F1BBCDC
```

```
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6
        temp = (a leftrotate 5) + f + e + k + w[i]
        e = d
        d = c
        c = b leftrotate 30
        b = a
        a = temp
    //Add this chunk's hash to result so far:
    h0 = h0 + a
    h1 = h1 + b
    h2 = h2 + c
    h3 = h3 + d
    h4 = h4 + e
//Produce the final hash value (big-endian) as a 160
bit number:
hh = (h0 leftshift 128) or (h1 leftshift 96) or (h2
leftshift 64) or (h3 leftshift 32) or h4
```

Барои ҳисобкунии ҳэш-функсияи пайғоми додашуда, тавассути алгоритми SHA-1 метавон аз барномаи зерин, ки дар забони Java навишта шудааст, истифода кард.

```
public static void main(String[] args) throws
NoSuchAlgorithmException {
  String str = "abc";
  MessageDigest md = MessageDigest.getInstance("SHA-1");
  md.update(str.getBytes());
```

```
  byte byteData[] = md.digest();
  //convert the byte to hex format method 1
  StringBuffer sb = new StringBuffer();
  for (int i = 0; i < byteData.length; i++) {
    sb.append(Integer.toString((byteData[i] & 0xff) + 0x100,
16).substring(1));
    }
  System.out.println("Hex format : " + sb.toString());
   //convert the byte to hex format method 2
  StringBuffer hexString = new StringBuffer();
  for (int i=0;i<byteData.length;i++) {
     String hex=Integer.toHexString(0xff & byteData[i]);
     if(hex.length()==1) hexString.append('0');
           hexString.append(hex);
        }
  System.out.println("Hex format : " + hexString.toString());
 }
```

Мисолҳои ҳисобкунии ҳэш-функсия дар системаи ҳисоби шонздаҳӣ.

1) SHA1 ("") = da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709
2) SHA1 ("abc") = a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
3) SHA1("abcdbcdecdefdefgefghfghighijhijkijkljklmklmn lmnomnopnopq") =84983e44 1c3bd26e baae4aa1 f95129e5 e54670f1

4. Алгоритми DSA

DSA (англ. Digital Signature Algorithm – алгоритми имзои электронӣ-рақамӣ) — алгоритми криптографӣ буда, барои сохтани имзои электронӣ-рақамӣ тавассути калиди кушода истифода бурда мешавад. Имзо махфиёна сохта мешавад, аммо онро метавон ошкоро тафтиш кард. Ин маънои онро дорад, ки дилхоҳ кас метавонад бо истифода аз параметрщои ошкор дурустиии имзоро санҷад. Қайд кардан ба маврид аст, ки DSA танҳо барои сохтани имзои-электронӣ-рақамӣ пешбини шудааст, на барои рамзгузорӣ монанди системаҳои RSA ва ал-Ҷамол.

DSA-ро моҳи августи соли 1991 институти Милии стандартҳо ва технологияҳо (NIST)-и ИМА сохта, патент кунонидааст. Муаллифи патент David W. Kravitz ба ҳисоб меравад. NIST - барои истифодабарии ин патентро бе литсензия дастрас гузошт (ройгон). DSA ҳамчун як бахши DSS (англ. Digital Signature Standard – стандарти имзои электронӣ-рақамӣ, нахустин маротиба 15-уми декабри соли 1998 интишор шудааст (ҳуҷҷати FIPS-186 (англ. Federal Information Processing Standards – стандарти федералии коркарди иттилоот)) ба ҳисоб меравад.

DSA дорои ду алгоритм (S, V): сохтани имзои пайғоми (S) ва тафтиши он (V) мебошад. Ҳарду алгоритмҳо ибтидо ҳеш-пайғомро бо истифода аз ҳэш функсияҳо ҳисоб мекунанд. Алгоритми S ҳэш ва калиди махфиро барои сохтани имзо истифода мебарад, Алгоритми V бошад, ҳэш пайғомро (хэш сообщения),

имзо ва калиди кушодаро барои тафтиши имзо истифода мебарад.

Дар версисяи нахустини алгоритм истифодаи ҳэш-функсияи SHA-1 (англ. Secure Hash Algorithm – алгоритми бехатар ҳэширонӣ) маслиҳат дода мешуд, дар версияиҳои баъдина бошад, метавон дилхоҳ алгоритми оилаи SHA-2-ро истифода кард

Параметрҳои схемаи имзои –электронӣ рақамӣ

Барои сохтани системаи имзоӣ рақамӣ бояд амалҳои зерин ичро карда шаванд:

1) Интихоби ҳэш-функсияи криптографӣ $H(x)$.
2) Интихоби ададди содаи q, ки андозаи (дарозии) он ба N бит баробар буда, аз рӯи андоза (дарозӣ) ба андозаи қимати ҳэш-функсия $H(x)$ баробар мебошад.
3) Интихоби ададди содаи p, тавре ки $(p-1)$ ба q тақсим шавад. Дарозии битии ададди p тавассути L ($2^{L-1} < p < 2^L$) ишора карда мешавад.
4) Интихоби ададди g тавре ки тартиби мултипликативии он аз рӯӣ модули p ба q баробар бошад. Барои ҳисобкунӣ метавон аз формулаи $g = h^{\frac{p-1}{q}} (mod\ p)$ истифода кард. Дар ин ҷо $h \in (1, p-1)$ — ягон ададди тасодуфӣ мебошад, ки зимнан $g \neq 1$ аст. Дар аксар ҳолатҳо қимати $h = 2$ ин талаботро қонеъ мегардонад.

Тавре ки қайд кардем, параметрҳои ибтидоии схемаи имзои рақамӣ истифодаи ҳэш-функсияи криптографӣ мебошанд, ки барои матни пайғомро (ки барои он имзо

ҳисоб карда мешавад (гузошта мешавад)) ба адади қайдкардашуда табдил додан истифода мешаванд. Яке аз хосиятҳои муҳими ин функсия дарозии битии пайдарпайии хуручӣ, ки бо ҳарфи N ишора карда мешавад, ба ҳисоб меравад. Дар версияи нахустини стандарти DSS истифодаи функсияи SHA-1 маслиҳат дода шуда буд, ки мувофиқан дарозии битии адади имзогузошташуда 160 битро ташкил мекард. Дар айни ҳол SHA-1 ба қадри кифоя бехатар намебошад, бинобар ин, дар стандарт истифодаи ҷуфтҳои зерин пешниҳод шудааст:

1) L = 1024, N = 160
2) L = 2048, N = 224
3) L = 2048, N = 256
4) L = 3072, N = 256

Бо мувофиқа бо ин истифодаи ҳэш-функсияи SHA-2 маслиҳат дода шудааст.

Калидҳои кушода ва махфӣ

1. Калиди махфӣ, адади $x \in (0, q)$ ба ҳисоб меравад;
2. Калиди кушода бошад тавассути формулаи $y = g^x (mod\ p)$ ҳисоб карда мешавад.

Параметрҳои кушода ададҳои (p, q, g, y) ба ҳисоб мераванд. Параметри махфӣ бошад, танҳо адади x мебошад. Ҳамин тариқ, параметрҳои (p, q, g) метавонанд

барои ҳамаи гурӯҳи истифодабарандагон умумӣ бошанд, вале ададҳои x ва y мувофиқан калиди пушида ва кушодаи истифодабарандаи мушаххас мебошанд. Ҳангоми имзогузорӣ ададҳои махфии x ва k истифода мешаванд, ки ададди k ба таври тасодуфӣ ё псевдотасодуфӣ интихоб карда мешавад.

Гузоштани имзо

Тавассути алгоритми зерин ба пайғом имзо гузошта мешавад:

1) Интихоби ададди тасодуфии $x \in (0, q)$;
2) Ҳисобкунии $r = (g^x \ mod \ p)(mod \ q)$;
3) Интихоби k –и дигар, агар $r = 0$ бошад;
4) Ҳисобкунии $s = k^{-1}(H(m) + x \cdot r)(mod \ q)$;
5) Интихобкунии k –и дигар, агар $s = 0$ шавад;
6) Ҷуфти (r, s) имзоро ташкил медиҳанд, ки дарозиашон ба $2N$ баробар аст.

Амали душвори ҳисобкунии – ин ба дараҷабардорӣ аз рӯӣ модул (ҳисобкунии $g^x \ mod \ p$), ҳисобкунии ҳэш-функсия, яъне $H(m)$ ва ёфтани элементи баръакс, яъне $k^{-1} \ mod \ q$ ба ҳисоб мераванд.

Тафтиши имзо

Тавассути алгоритми зерин имзо тафтиш карда мешавад:

1) Ҳисобкунии $\omega = s^{-1} \ mod \ q$;
2) Ҳисобкунии $u_1 = H(m) \cdot \omega \ mod \ q$;
3) Ҳисобкунии $u_2 = r \cdot \omega \ mod \ \ q$;

4) Ҳисобкунии $v = (g^{u_1} \cdot y^{u_2} \ mod \ p) mod \ q$;

5) Имзо ҳаққонӣ аст, агар $v = r$ шавад.

Ҳангоми тафтиш амали мураккаб, ин ду амали бадарачабардорӣ g^{u_1} ва y^{u_2}, ҳисобкунии ҳэш-функсия $H(m)$ ва ёфтани элементи баръакс $s^{-1} \ mod \ q$ мебошанд.

Дурустии схемаҳо

Схемаи имзои рақамии мавриди баҳс қарордодаамон, ба он дарачае дақиқ аст, ки ҳар хоҳишманде, ки мехоҳад аслияти имзоро санҷад, ҳама вақт натиҷаи мусбат ба даст меорад. Ҳоло инро нишон медиҳем:

Аввалан, агар $g = h^{\frac{p-1}{q}} \ mod \ p$ бошад, пас аз рӯӣ теоремаи кучаки Ферма бармеояд, ки $g^q = h^{p-1} = 1$ аст. Азбаски $g > 1$ буда, q – адади сода аст, пас g дорои тартиби мултипликативии q аз рӯи модули p мебошад.

Барои гузоштани имзо ба пайғом ҳисоб карда мешавад:

$$s = k^{-1}(H(m) + x \cdot r)(mod \ q).$$

Аз ин ҷо бармеояд, ки

$k = H(m) \cdot s^{-1} + x \cdot r \cdot s^{-1} = H(m) \cdot \omega + x \cdot r \cdot \omega \ mod \ q$ аст.

Азбаски g дорои тартиби q аст, пас ҳосил мекунем.

$$g^k = g^{H(m)\cdot\omega \ mod \ q} g^{x\cdot r\cdot\omega \ mod \ q} = g^{H(m)\cdot\omega \ mod \ q} y^{r\cdot\omega \ \ mod \ q}$$
$$= g^{u_1} y^{u_2} \ mod \ p.$$

Сониян, дурустии схемаи DSA аз муносибати зерин бармеояд.

$$r \ = \ (\ g^k \ mod \ p \ ) mod \ q \ = \ (\ g^{u_1} \ y^{u_1} \ \ mod \ p \ ) mod \ q \ = \ v.$$

Ҳоло дар мисоле истифодаи схемаи DSA-ро барои ададӣ наонқадар калон дида мебароем. Бигузор қимати ҳэш-функсияи пайғом $H = 9$ бошад.

Интихоби параметрҳо

1) $H = 9_{10} = 1001_2$.
2) Дарозии ҳэш ба 4 баробар аст, аз инҷо метавон $q = 11_{10} = 1011_2$ гирифт.
3) p = 23 интихоб мекунем, чунки $23 - 1 = 22 = 2 \cdot q$ аст.
4) $g = 2^2 = 4$ интихоб мекунем.

Сохтани калид

Ба сифати калидии махфи $x = 7$ интихоб мекунем, он гоҳ калиди кушода $y = g^x \, mod \, p = 4^7 \, mod \, 23 = 8$ мешавад.

Гузоштани имзо

1) Интихоби $k = 3$.
2) Он гоҳ $r = (g^k \, mod \, p) mod \, q = (4^3 \, mod \, 23) mod \, 11 = 7$ мешавад.
3) Азбаски $r \neq 0$ аст, пас давом медиҳем.
4) $s = k^{-1} (H(m) + x \cdot r) mod \, q = 4 \cdot (9 + 7 \cdot 7) mod \, 11 = 1$, дар ин ҷо $3^{-1} \, mod \, 11 = 4$ аст.
5) $s \neq 0$ аст, давом медиҳем.
6) Ҷуфти ададҳои (r , s) = (7 , 1) имзоро ташкил мекунанд.

Тафтиши имзо

1) $\omega = s^{-1} \ mod \ q \ = \ 1^{-1} \ mod \ 11 \ = \ 1.$

2) $u_1 \ = \ H \ (\ m \ ) \ \cdot \ \omega \ mod \ q \ = \ 9 \ \cdot \ 1 \ mod \ 11 \ = \ 9.$

3) $u_2 = \ r \ \cdot \ \omega \ mod \ q \ = \ 7 \ \cdot \ 1 \ mod \ 11 \ = \ 7.$

4) $v \ = \ (\ g^{u_1} \ \cdot \ y^{u_2} \ mod \ p \ ) \ mod \ q \ =$
$(\ 4^9 \ \cdot \ 8^7 \ mod \ 23 \ ) \ mod \ 11 \ = \ 7.$

5) Ҳосил мекунем, ки $v \ = \ r$, яъне имзо дуруст будааст.

5. Имзои электрони дар RSA

Имзоҳои электрони-рақамиро дар схемаи RSA дида мебароем.

Масалан, агар Алӣ хоҳад, ки ҳуҷҷатеро имзо гузорад, барои иҷрои ин амал, параметрҳои RSA – ро интихоб мекунад. Тарзи интихоби параметрҳои RSA дар боби 8 оварда шудааст. Ибтидо Алӣ ду ададиkалони соддаи P ва Q – ро интихоб карда, қимати $N = PQ$ ва $\varphi = (P - 1)(Q - 1)$ – ро ҳисоб мекунад. Пас аз ин, ададии d – ро, ки бо φ байнан сода мебошанд, интихоб карда, қимати $c = d^{-1} \ mod \ \varphi -$ ро ҳисоб мекунад. Дар охир Алӣ ададҳои N ва d - ро интишор мекунад. Масалан, дар сайти худ мегузорад. Дар ин ҳангом ададии c – ро махфӣ нигоҳ медорад. Алӣ метавонад, ададҳои P, Q ва φ- ро ҳатто фаромӯш кунад, чунки дигар онҳо талаб карда намешаванд. Ҳамин тариқ Алӣ барои гузоштани имзо омода гашта, метавонад имзои худро ба ҳуҷҷатҳо ва мактубҳо гузорад.

Бигузор Алӣ мехоҳад пайғоми $\bar{m} = m_1, \dots, m_n$ – ро имзо гузорад. Барои иҷрои ин амал ибтидо ҳэш – функсияи $y = h(m_1, \dots m_n)$ – ро ҳисоб мекунад, ки он пайғоми $\bar{m}$ - ро ба адади y мувофиқ мегузорад. Тарзи ҳисобкунии ҳэш – функсия дар ибтидои ин боб оварда шудааст, бинобар ин, дар ин ҷо тарзи ҳисобкунии онро пурра мавриди баҳс қарор надода, танҳо баъзе хосиятҳои муҳими онро меорем: бе тағйирдиҳии y дар амалия тағйир додани матни асосии $m_1, m_2, \dots, m_n$ ғайриимкон аст. Аз ин рӯ, дар қадами оянда Алӣ танҳо имзо гузоштан ба y – ро таъмин мекунад, ки ин имзо ҳамаи матни $\bar{m}$ – ро дар бар мегирад.

Ибтидо Алӣ адади

$$s = y^c \ mod\ n \qquad (1)$$

-ро ҳисоб мекунад, яъне он адади y - ро ба дараҷаи адади махфии c мебардорад. Дар ин ҷо адади s – ин имзои электронӣ мебошад. Имзои электронӣ ба пайғоми $\bar{m}$ ҳамроҳ карда мешавад. Ҳамин тариқ Алӣ мактуби имзогузоштаро ба сурати зерин ҳосил мекунад.

$$\langle \bar{m}\ , s \rangle. \qquad (2)$$

Акнун ҳамаи он касоне, ки параметрҳои кушодаи Алӣ – ро медонанд, метавонанд, соҳибияти имзои ӯро тасдиқ кунанд. Барои иҷрои ин амал мактуби имзогузошташуда (2) – ро гирифта қимати ҳэш – функсияи $h(\bar{m})$ ва

$$\omega = s^d \ mod\ N \qquad (3)$$

– ро ҳисоб карда, иҷроиши шарти $\omega = h(\bar{m})$ – ро месанҷад.

Бе душворӣ дидан мумкин аст, ки агар имзо ҳаққонӣ бошад, он гоҳ $\omega = h(\bar{m})$ мешавад.

Дар ҳақиқат, аз формулаҳои (1) , (3) ва хосияти схемаи RSA дурустии ин тасдиқот бармеояд,

$$\omega = s^d \bmod N = y^{cd} \bmod N = h(m)$$

Қайд кардан ба маврид аст, ки имзои электронии дидабаромада ҳамаи талаботҳои имзоҳои оддиро қаноат мекунонанд.

Хосияти якуми имзоро месанҷем. Ҳангоме, ки тартиби N аз 1024 бит калон будан, ҳеҷ кас наметавонад, онро ба зарбкунандаҳои сода ҷудо кунад. Ин масъала то соли 2005 тамоман ҳалнашаванда буд. Аз ин рӯ бо донистани N ва d ёфтани c ғайриимкон мебошад. Дар ҳақиқат, барои ҳисоб намудани $c = d^{-1} \bmod \varphi$, бояд адади $\varphi = (P-1)(Q-1)$ маълум бошад, аммо барои донистани P ва зарбшавандаи Q зарур аст. Ҳамин тариқ, хосияти якум иҷро гардид – ҳеҷ кас ба ғайр аз Алӣ наметавонад адади c – ро ҳисоб кунад, аз ин рӯ мактубро наметавонад имзо гузорад.

Аз хосияти якум иҷроиши хосияти дуюм бармеояд. Муаллифи имзо наметавонад, аз он даст кашад, чунки шахси дигар наметавонад аз номи ӯ имзо гузорад.

Хосияти сеюм ҳам аён мебошад – дар ҳолати пайдо шудани баҳс, шахсони кунҷков метавонанд барои тафтиш он ва фаҳмидани ҳақ ба судя мурочиат кунанд.

Мисоли 1. Бигузор $P = 5,\ Q = 11$ бошад. Он гоҳ $N = 5 \cdot 11 = 55,\ \varphi = 4 \cdot 10 = 40$ мешавад. Бигузор $d = 3$ бошад. Чунин интихоб намудани d имкон дорад, чунки

КТУ(40,3)=1 аст. Барои ҳисобкунии $c = 3^{-1} \, mod \, 40$ аз алгоритми васеъкардашудаи Евклид (АВЕ) истифода намуда, ҳосил мекунем $c = 27$.

Бигузор Алӣ мехоҳад пайғоми $\overline{m} = abbbaa$ – ро, ки барои он қимати ҳэш – функсия ба 13 баробар аст, имзо гузорад.

$$y = h(abbbaa) = 13$$

Дар ин ҳолат Алӣ аз рӯйи (1) қимати

$$s = 13^{27} \; mod \; 55 = 7$$

-ро ҳисоб карда, пайғоми имзогузошташудаи зеринро ҳосил мекунад.

$$\langle abbbaa, 7 \rangle$$

Акнун касоне, ки калиди кушодаи Алӣ $N=55$ ва $d=3$ – ро медонад, метавонад ҳаққонияти (соҳибияти) имзоро санҷанд.

Баъди ба даст овардани пайғоми имзогузошта, Валӣ аз сари нав қимати ҳэш – функсияро

$$h(abbbaa) = 13$$

-ро ҳисоб карда (агар таркиби мактуб иваз карда нашуда бошад, он гоҳ қиммати ҳэш – функсия ба қимати ҳэш – функсияе, ки Алӣ ҳисоб карда буд мувофиқат мекунад), сипас қимати ифодаи (3)

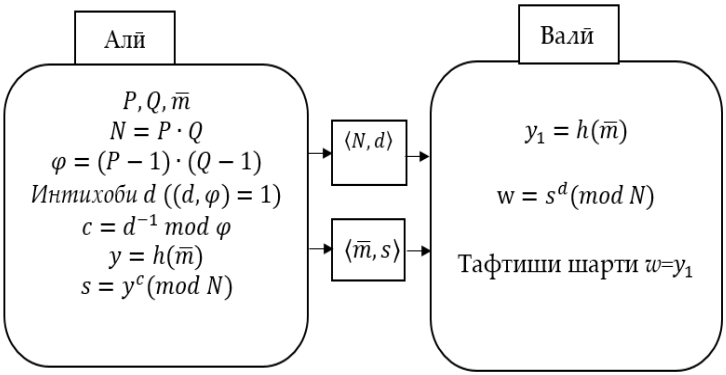
$$\omega = 7^3 \; mod \; 55 = 13$$

-ро ҳисоб мекунад.

Тавре ки дида мешавад, қимати ω ва қимати ҳэш – функсия мувофиқат мекунанд, бинобар ин, метавон ба дурустии имзо боварӣ ҳосил кард.

Қайд. *Диққат дошта бошед, ки як схемаи RSA – ро Алӣ барои ҳалли ду масъала истифода кард. Аввал Алӣ метавонад мактубро бо истифода аз калиди махфии с имзо гузорад. Дуюм ҳар кас мехоҳад бо Алӣ мактуби рамзгузошташуда (адад) равон кунад, ки рамзкушоӣ кардани он танҳо бо истифодаи калиди d имкон дошта бошад.*

Ба намуди схематикӣ ин алгоритм шакли зеринро дорад:



6. Имзоҳои электронӣ дар базаи рамзи Ал – Ҷамол

Бигузор Алӣ мехоҳад, ки ҳуҷҷатеро имзо гузорад. Барои иҷрои ин амал адади калони содаи p ва адади g – ро интихоб мекунад Тарзи интихоби ин параметрҳо дар боби 8 оварда шудааст. Ин ададҳо метавонад барои дигар муштариён низ дастрас бошанд. Илова бар ин, Алӣ адади тасодуфии (ихтиёрии) x $(1 < x < p-1)$ – ро интихоб карда, онро махфӣ нигоҳ медорад. Пас аз ин, қимати адади зеринро ҳисоб мекунад.

$$y = g^x \ mod \ p \qquad (1)$$

Ин ададҳоро Алӣ ҳамчун калиди кушодаи худ интишор мекунад. Тавре, ки аён (маълум) аст, ҳангоми бениҳоят калон будани p, аз рӯйи y ёфтани x ғайриимкон мебошад (масъалаи логарифми дискретӣ).

Акнун Алӣ метавонад мактубро имзо гузорад. Фарз мекунем, ки Алӣ мехоҳад мактуби $\overline{m} = m_1, \dots, m_n$ – ро имзо гузорад. Алгоритми сохтани имзоро меорем.

Алӣ қимати ҳэш – функсия $h = h(\overline{m})$ – ро, ки бояд, ки шарти $1 < h < p$ – ро қаноат мекунонад, ҳисоб карда, сипас ададди тасодуфии k $(1 < k < p - 1)$ – ро ки бо $(p - 1)$ байнан сода мебошанд, интихоб карда, қимати ададди зеринро ҳисоб мекунад.

$$r = g^k \ mod \ p \qquad (2)$$

Дар қадами оянда Алӣ қимати ададҳои зеринро ҳисоб мекунад.

$$u = (h - xr) \ mod \ (p - 1), \qquad (3)$$
$$s = k^{-1} \ u \ mod \ (p - 1) \ , \qquad (4)$$

Дар охир Алӣ пайғоми рамзгузошташударо имзо мегузорад.

$$\langle m; r, s \rangle \qquad (5)$$

Қабулкунандаи иттилооти имзошуда (5) пеш аз ҳама қимати ҳэш функсияи $h = h(\overline{m})$ – ро аз нав ҳисоб мекунад. Баъд аз ин, бо истифода аз баробарии зерин имзоро тафтиш мекунад:

$$y^r \ r^s = g^h mod \ p \qquad (6)$$

Бе душворӣ дидан мумкин аст, ки дар сурати ҳаққонӣ будани имзо шарти (6) иҷро мегардад.

Дар ҳақиқат

$$y^r r^s = (g^x)^r (g^k)^s = g^{xr} q^{k(k-1(h-xr))} = g^{xr} g^h g^{-xr} = q^n mod p$$

Мисол. Бигузор параметрҳои ошкор $P = 23$ ва $g = 5$ бошанд. Алӣ калиди махфӣ $x = 7$-ро интихоб карда, калиди кушодаи y– ро бо истифода аз (1) ҳисоб мекунад.

$$y = 5^7 \ mod \ 23 = 17$$

Бигузор Алӣ мехоҳад пайғоми $\bar{m} = baaaab$ – ро имзо гузорад. Барои иҷрои ин чунин амал мекунад:

Пеш аз ҳама қимати ҳэш – функсияро ҳисоб мекунем. Бигузор қимати $h(\bar{m}) = 3$ бошад. Пас аз ин Алӣ адади тасодуфии k (масалан k = 5) – ро интихоб карда, қимати ифодаҳои (2) ва (3) – ро ҳисоб мекунад.

$$r = 5^5 \ mod \ 23 = 20,$$

$$v = (3 - 7 \cdot 20) \ mod \ 22 = 17$$

Пас аз ин, Алӣ қимати $k^{-1} \ mod \ 22$ – ро ҳисоб мекунад.

$$k^{-1} \ mod \ 22 = 5^{-1} \ mod \ 22 = 9.$$

Қимати (4) бошад, ба $s = 9 \cdot 17 \ mod \ 22 = 21$ баробар мешавад.

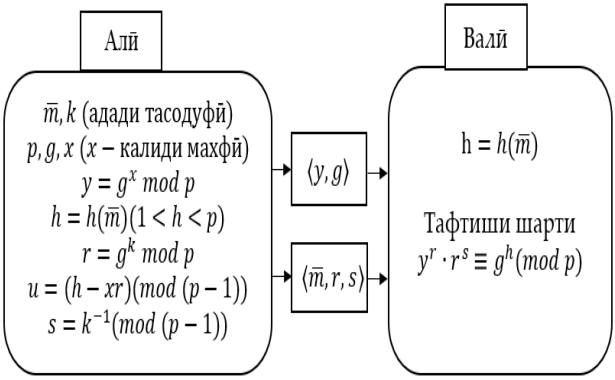
Дар охир пайғоми имзогузошташударо ба сурати (5) $(baaaab, 20, 21)$ ҳосил мекунад. Акнун Алӣ онро ба Валӣ равон мекунад. Валӣ онро ба даст оварда, ибтидо соҳибияти имзоро месанҷад. Бирои ин аввал қимати ҳэш – функсия $h(baaaab) = 3$ ва баъд тарафи чапи (6) $17^{20} \cdot 20^{21} \ mod \ 23 = 16 \cdot 15 \ mod \ 23 = 10$ ва дар охир тарафи рости (6) – ро ҳисоб мекунад

$$5^3 \ mod \ 23 = 10$$

Валӣ боварӣ ҳосил мекунад, ки имзо дуруст (ҳақиқӣ) аст.

Дар асоси ин алгоритми Ал-Ҷамол дигар алгоритмҳои эффективӣ сохта шудаанд.

Ба намуди схематикӣ ин алгоритм шакли зеринро дорад:



7. Стандартҳо дар имзои электронӣ (рақамӣ)

Дар бисёр кишварҳои ҷаҳон стандартҳо дар имзоҳои электронӣ (ИЭ) ё рақамӣ вуҷуд дорад. Дар ин ҷо мо стандарти давлатии Россия ГОСТ Р34.10 – 94 ва стандарти ИМА FIPS 186 – ро мавриди баҳс қарор медиҳем. Тавре ки аз ишорааш бармеояд стандарти Россия соли 1994 ва стандарти амрикоӣ соли 1991 қабул карда шудааст. Ҳарду стандартҳо дар асоси як алгоритм, ки DSA (Digital Signature Algorithm) ном дорад асос ёфта, вариатсияи имзои Ал – Ҷамол мебошанд. Ҳоло алгоритми Россияро мавриди баҳс қарор дода, дар охир фарқияти алгоритми амрикоиро меорем.

Ибтидо барои як гурӯҳ истифодабарандагон параметрҳои ошкор интихоб карда мешаванд. Пеш аз ҳама, бояд ду ададиі содаи p ва q, ки барои онҳо баробарии зерин иҷро мегардад, интихоб карда шавад.

$$p = bq + r \qquad (1)$$

Дар ин ҷо b ягон ададиі бутун мебошад. Битҳои калони (старшие биты) p ва q бояд ба як баробар бошанд. Пас аз ин, чунин ададиі $a > 1$ тавре интихоб карда мешавад, ки барои он баробарии зерин иҷро гардад.

$$a^q \bmod p = 1. \qquad (2)$$

Дар натиҷа се параметри умумии – p, q ва a – ро ҳосил карда мешаванд.

Қайд. *Баробарии (2) маънои онро дорад, ки ҳангоми ададиі a – ро аз рӯйи модули p ба дараҷа бардоштан, дараҷа ба модули q оварда мешавад, яъне* $a^b \bmod p = a^{b \bmod q} \bmod p$.

Дар қадами оянда ҳар як истифодабаранда ададиі ихтиёрии x – ро ки шарти $0 < x < q$ – ро қаноат мекунад, интихоб карда, қимати

$$y = a^x \bmod p \qquad (3)$$

– ро ҳисоб мекунанд. Дар онҷо x – калиди махфӣ ва y – калиди ошкор (кушода) мебошад. Барои истифодабарандагон ададиі x ҳамчун калиди махфӣ ва ададиі y калиди кушода ба ҳисоб меравад. Фарз карда мешавад, ки калиди кушодаи ҳамаи истифода-барандагон ба ҳамдигар муайян мебошад, то он ки онҳо тавонанд имзоро тафтиш кунанд.

Қайд мекунем, ки дар айни ҳол ёфтани x аз рӯйи y дар амалия ғайриимкон мебошад. Пас аз интихоби параметрҳо ба имзогузорӣ оғоз мекунем.

Бигузор пайғоми $\bar{m}$ мавҷуд аст, ки бояд имзо гузошта шавад. Алгоритми гузоштани имзо чунин аст:

1) Ибтидо барои пайғоми $\bar{m}$ ҳэш – функсия $h = h(\bar{m})$ – ро ҳисоб мекунем. Қимати ҳэш – функсия бояд дар фосилаи $0 < h < q$ хобад (дар варианти руссия ҳэш – функсияе, ки ГОСТ Р34.11 – 94 муайян кардааст).
2) Ададӣ тасодуфии k $(0 < k < q)$ – ро интихоб мекунем.
3) Қимати $r = (a^k \ mod \ p) mod \ q$ – ро ҳисоб мекунем. Агар рафту $r = 0$ бошад, он гоҳ ба қадами 2 бар мегардем.
4) Қимати $s = (kh + xr) \ mod \ q$ – ро ҳисоб мекунем, агар рафту $s = 0$ шавад, ба қадами 2 бар мегардем.
5) Пайғоми имзогузошташудаи $\langle \bar{m}; r, s \rangle$ – ро ҳосил мекунем.

Барои тафтиши имзо амалҳои зерин иҷро карда мешаванд.

1) Барои пайғоми $\bar{m}$ қимати ҳэш-функсия, яъне $h = h(\bar{m})$ – ро ҳисоб мекунем.
2) Дурустии шартҳои $0 < r < q$, $0 < s < q$ – ро месанҷем.
3) Қимати $u_1 = s \cdot h^{-1} \ mod \ q$, $u_2 = -r \cdot h^{-1} \ mod \ q$ – ро ҳисоб мекунем.
4) Қимати $v = (a^{u_1} y^{u_2} \ mod \ p) \ mod \ q$ – ро ҳисоб мекунем.
5) Иҷроиши шарти $v = r$ – ро месанҷем.

Агар ақалан яке аз тафтишҳо (санҷишҳо) дар қадами 2 ва 5 қимати ҳақ надиҳанд, имзо ғайриҳақиқӣ

дониста мешавад. Агар ҳамаи тафтишҳо иҷро гарданд, пас имзо дуруст ба ҳисоб меравад.

Бе душворӣ дидан мумкин аст, ки агар имзо бо пайғом қонунӣ бошад (яъне агар калиди махфии x – ро соҳиб бошад), он гоҳ $v = r$ мешавад.

Дар ҳақиқат

$$v = \left(a^{sh^{-1}}\, y^{-rh^{-1}} \bmod p\right) \bmod q =$$
$$= (a^{(kh+xr)h^{-1}}\, a^{-xrh^{-1}} \bmod p) \bmod q =$$
$$= \left(a^{k+xrh^{-1}-xrh^{-1}} \bmod p\right) \bmod q =$$
$$= (a^k \bmod p) \bmod q = r.$$

Қайд. *Барои ёфтани қимати параметри a, ки шарти (2) – ро қаноат мекунонад, аз методи зерин истифода бурда мешавад. Ибтидо адади тасодуфии q >1 – ро интихоб карда, қимати*

$$a = q^{(p-1)/q} \bmod p \qquad (4)$$

- ро ҳисоб мекунем. Дар ҳақиқат, дар асоси (4) ва теоремаи Ферма ҳосил мекунем.

$$a^q \bmod p = g^{((p-1)/q)q} \bmod p = g^{p-1} \bmod p = 1,$$

яъне баробарии (3) иҷро мешавад. Агар ҳангоми ҳисобкунии (4) қимати $a = 1$ шавад, он гоҳ зарурияти интихоби қимати дигар барои g пеш меояд.

***Мисоли* 2.** Параметрҳои умумии ошкор (ғайримахфӣ) – и $q = 11$, $p = 6q + 1 = 67$ – ро интихоб карда, қимати $g = 10$ гирифта, $a = 10^6 \bmod 67 = 25$ – ро ҳисоб мекунем. Сипас, калиди махфии $x = 6$ – ро интихоб карда, калиди кушодаи $y = 25^6 \bmod 67 = 62$ – ро ҳисоб мекунем.

Барои пайғоми $\bar{m} = baaaab -$ ро имзо гузоштан, чунин амал карда мешавад. Бигузор ҳэш – функсияи ин пайғом $h(\bar{m}) = 3$ бошад. Адади тасодуфии $k = 8$ – ро интихоб карда, қимати ададҳои зеринро ҳисоб мекунем.

$$r = (25^8 \ mod \ 67) mod \ 11 = 24 \ mod \ 11 = 2,$$
$$s = (8 \cdot 3 + 6 \cdot 2) \ mod \ 11 = 36 \ mod \ 11 = 3.$$

Пайғоми имзогузошташудаи $\langle baaaab; 2{,}3 \rangle$ – ро ба даст меорем.

Акнун имзоро тафтиш мекунем. Агар пайғом тағйир дода нашуда бошад, $h = 3$ мешавад. Ҳисоб мекунем,

$$h^{-1} = 3^{-1} \ mod \ 11 = 4,$$
$$u_1 = 3 \cdot 4 \ mod \ 11 = 1,$$
$$u_2 = -2 \cdot 4 \ mod \ 11 = -8 \ mod \ 11 = 3,$$
$$v = (25^1 \cdot 62^3 \ mod \ 67) \ mod \ 11 =$$
$$= (25 \cdot 9 \ mod \ 67) \ mod \ 11 = 24 \ mod \ 11 = 2.$$

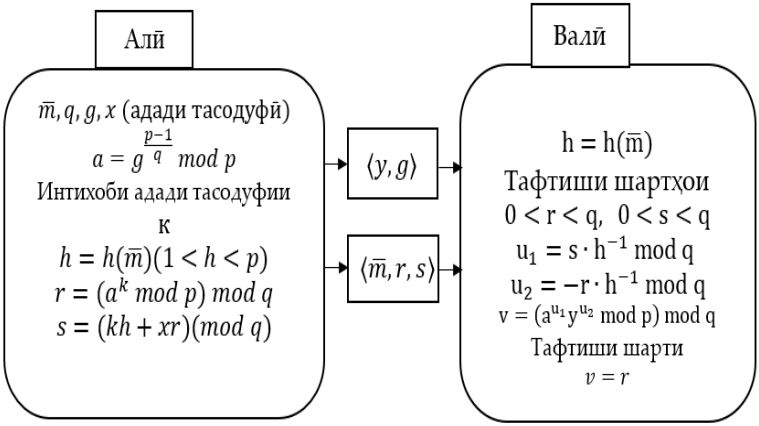
Тавре ки аён гашт, шарти $v = r$ ичро мегардад, яъне имзо дуруст будааст.

Акнун фарқияти стандарти амрикоиро аз стандарти русӣ дида мебароем.

1) Дарозии q ба 160 бит баробар гирифта мешавад.
2) Ба сифати ҳэш – функсия аз алгоритми SHA – 1 истифода бурда мешавад.
3) Ҳангоми сохтани имзо дар қадами 4 параметри s тавассути формулаи $s = k^{-1}(h + xr) \ mod \ q$ ҳисоб карда мешавад.
4) Ҳангоми тафтиши имзо дар қадами 3 u_1 ва u_2 аз рӯйи формулаҳои $u_1 = h \cdot s^{-1} \ mod \ q$, $u_2 = r \cdot s^{-1} \ mod \ q$ ҳисоб карда мешавад.

Бо назардошти ин фарқиятҳо метавон схемаи имзоро бо услуби амрикоӣ навишт. Исботи дурусти алгоритм айнан гузаронида мешавад.

Ба намуди схематикӣ алгоритми мазкур шакли зеринро дорад:



Саволҳо барои мустаҳкамкунӣ

1. Ҳэш-функсия чист ва чӣ тавр ҳисоб карда мешавад?
2. Кадом алгоритмҳои ҳисобкунии ҳэш-функсияро медонед?
3. Имзои электронӣ чист?
4. Алгоритми SHA-1 аз MD5 чӣ фарқ драд?
5. Имзоҳои электронӣ аз имзоҳои муқаррарӣ чӣ фарқ доранд?
6. DSA чист ва кай сохта шудааст?
7. Оё авассути DSA метавон рамгузорӣ кард?

8. Чи тавр параметрҳои ошкори DSA интихоб карда мешаванд?
9. Тавассути алгоритми DSA чӣ тавр имзои электронӣ гузошта мешавад?
10. Тавассути алгоритми RSA чӣ тавр имзои электронӣ гузошта мешавад?
11. Тавассути алгоритми Ал-Ҷамол чӣ тавр имзои электронӣ гузошта мешавад?
12. Оё метавон барои гузоштани имзои электронӣ аз рамзи Шамир истифода кард?
13. Алгоритми ГОСТ Р34.10 – 94 чӣ гуна алгоритм аст ва кай сохта шудааст?
14. Барои гузоштани имзои электронӣ оё метавон аз алгоритми ГОСТ Р34.10 – 94 истифода кард?
15. Стандарти ГОСТ Р34.10 – 94 аз сатдартӣ амрикоии FIPS 186 чӣ фарқ дорад?

Боби 10. Методҳои муосири рамзгузорӣ бо калидҳои пушида

1. Рамз ё шабакаи Фейстел


Горст Фейстел

Сеть ё шабакаи Фейстел (англ. Feistel network, Feistel cipher) —яке аз методҳои сохтани рамзҳои блокӣ ба ҳисоб меравад. Шабакаи мазкур аз катакчаҳо иборат мебошад, ки онҳоро катакчаҳои Фейстел меноманд. Дар вуруди ҳар як катакча итилоот ва калид ворид гардида, дар хуруҷ итилоот ва калиди тағйирёфа ба даст оварда мешавад. Ҳамаи катакчаҳои мазкур аз рӯйи тип якхела мебошанд. Вобаста аз алгоритми рамзгузорӣ/рамзкушоӣ калид интихоб гардида, ҳангоми аз гузариш аз як катакча ба катакчаи дигар тағйир меёбад. Дар вақти рамзгузорӣ ва рамзкушоӣ айнан як амал иҷро карда мешавад, фарқияти асосӣ тартиби калидҳо ба ҳисоб мераванд, аз рӯйи содагӣ метавон ба осонӣ барномаи методи мазкурро таҳия кард. Аксар методҳои муосири рамзгузории блоки ба монанди: DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA ва ғайра ба сифати асос аз шабакаи Фейстел истифода мебаранд. Алтернативи шабакаи Фейстел алгоритми AES ба ҳисоб меравад, ки баъдтар онро мавриди баҳс қарор медиҳем.

Соли 1971 Хорст Фейстел[1] (англ. Horst Feistel) ду воситае, ки дар онҳо алгоритмҳои гуногун амали карда мешуданд, патент кард. Баъдан ин восита номи Lucifer-ро гирифт. Яке аз ин воситаҳо конструксияеро истифода кард, ки баъдан он дар шабакаи Фейстел («Feistel cipher», «Feistel network») истифода шуд. Аз ин ҷо Фейстел якҷоя бо Дон Копперсмит (англ. Don Coppersmith) дар системи криптогарфии нав дар IBM кор кард. Соли 1973 газетаи «Scientific American» мақолаи Фейстелро таҳти унвони «Cryptography and computer privacy» чоп кард, ки дар он ҷанбаҳои муҳими рамзгузорӣ мавриди баҳс қарор дода шуда, шарҳи версияи нахустини Lucifer оварда шудааст. Дар версияи нахустини лоиҳаи Lucifer шабакаи Фейстел истифода нашуда буд.

Дар асои шабакаи Фейстел соли 1977 алгоритми DES сохта шуд.

Акун алгоритми рамзгузорӣ ва рамзкушоиро тавасути шабакаи Фейстел дида мебароем. Бигузор талаб карда шавад, ки ягон итилооте, ки ба намуди дӯӣ дода

[1] Хорст Фейстел (англ. Horst Feistel) 30-юми январи соли 1915 дар шаҳри Берлин (Олмон) ба дунё омадааст. Аз хурдсоли Олмонро тарк гуфта ба Тсюрих (Швейтсария) рафт. Хорст олими бузурги соҳаи ҳифзи итилоот ва яке аз асосгузорони криптографияи замони муосир ҳамчун илм ба ҳисоб рафта, дар ширкати IBM дар соҳаи коркарди алгоритмҳои рамзгузорӣ кор кардааст. Саҳми Ӯ дар сохтани алгоритми DES хело калон мебошад. 14-уми ноябри соли 1990 дар штати Массачусетс аз олам чашм пушид.

шудааст (дар хотираи компютер, файл ё ягон барандаи дигари итилоот), рамзгузорӣ карда шавад. Алгоритми рамзгузорӣ чунин аст:

Итилооти додашуда ба блокҳои якхела (қайдкардашуда) тақсим карда мешавад. Блокҳои ҳосилшуда вурӯди номида мешаванд, чунки ба вуруди алгоритм равон карда мешаванд. Агар андозаи блоки вурудӣ, аз дарозии дар алгоритм муайяншуда, хурд бошад, он гоҳ бо ягон усул дароз карда мешавад (масалан бо илова намудани ягон символ ё ҳарф, баъзан рамзи хати поён истифода мешавад). аз рӯйи қоида дарозии блок бояд, ягон адади дараҷаи ду бошад, масалан, 64 бит ё 128 бит.

Акнун амалеро дида мебароем, ки танҳо бо як блок ба амал омада, дар ҷараёни рамзгузорӣ бо дигар блок айнан ҳамин хел ба амал меояд.

1) Блоки интихобшуда ба ду зербloки дорои дарозии якхела ҷудо карда мешавад: L_0 – зербloки чап ва R_0 –зербloки рост.
2) Зербloки чап L_0 – тавассути функсияи f бо истифода аз калиди раундиии (даврии) K_0 тағйир дода мешавад.

$$x = f(L_0, K_0).$$

Натиҷаи ҳосилшуда бо истифода аз амали амали xor $(\oplus)$ бо зербloки тарафи рост R_0 ҷамъ карда мешавад.

$$x = x\ xor\ R_0.$$

Дар раунди навбати ин натиҷа ҳамчун зербloки чап истифода бурда мешавад L_1:

$$L_1 = x.$$

Зерблоки чапи L_0 раунди ҷорӣ дар раунди баъди ҳамчун зерблоки рост истифода бурда мешавад R_1:

$$R_1 = L_0.$$

Аз рӯйи баъзе қоидаҳои математикӣ калиди раунди K_1 ҳисоб карда мешавад, ки дар раунди баъдӣ истифода бурда мешавад. Умуман барои рамзгузорӣ/рамзкушоӣ метавон як чанд калид истифода кард, яъне дар ҳар раунд аз калиди мувофиқ истифода кард.

Амалҳои мазкур $N-1$ маротиба иҷро карда мешаванд, дар ин ҷо N — миқдори раундҳоро дар алгоритми интихобшуда ифода мекунад. Дар ин ҳангом гузариш аз як раунд ба раунди дигар калид K_0 ба K_1, K_1 ба K_2 ва ҳоказо иваз карда мешаванд.

Амали рамзкушоӣ айнан амали рамзгузорӣ иҷро карда мешавад, ба истиснои истифода калид ба тартиби баръакс, яъне аввал калиди $N-$ум, сипас $N-1$-ум ва ҳоказо калиди якум истифода бурда мешавад.

Акнун ба намуди математикӣ алгоритми Фейстелро дида мебароем, ки чунин шакл дорад:

Блоки матни кушод ба ду зерблок чап ва рост тақсим карда мешавад: L_0 — зерблоки чап ва R_0 —зерблоки рост.

Дар ҳар як раунд, қимати ифодаҳои зерин ҳисоб карда мешаванд:

$$L_i = R_{i-1} \oplus f(L_{i-1}, K_{i-1});$$
$$R_i = L_{i-1}.$$

Дар ин ҷо

i — рақами тартибии раунд, i=1…N;

N — миқдори раундҳои алгоритми интихобшуда;

f —ягон фунсия;

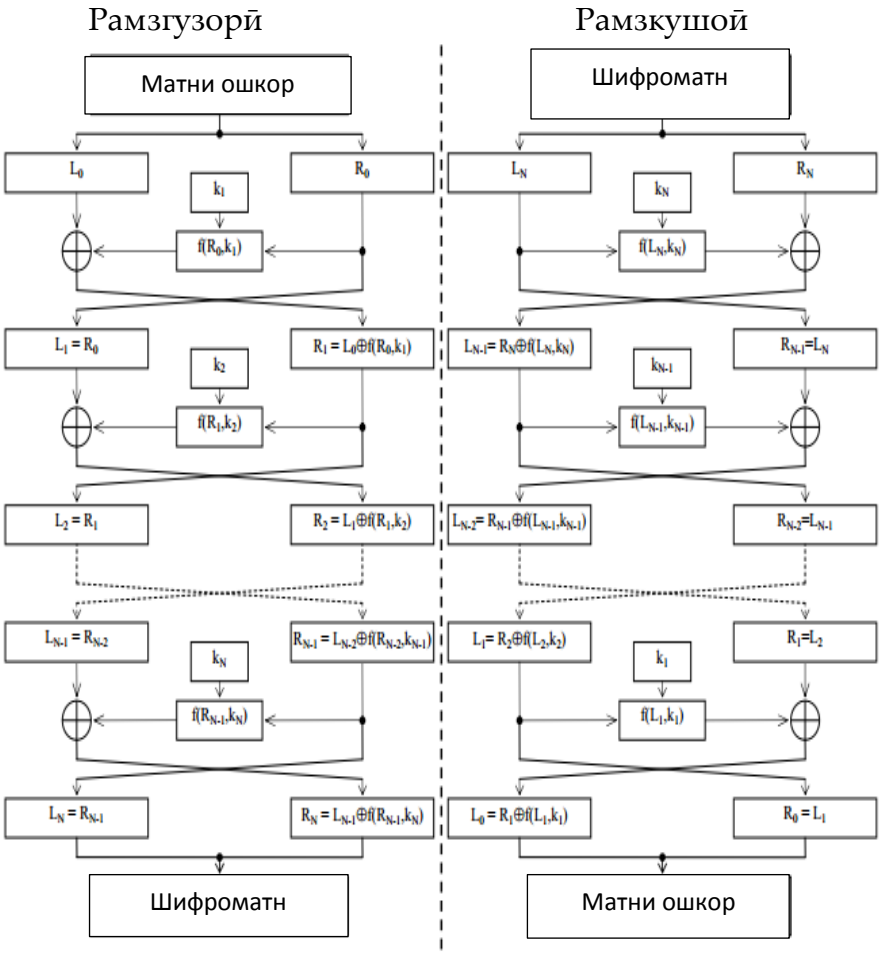
K_{i-1} —калиди раунди $i-1$ —ум;

Натиҷаи иҷроиши раунди N-ум (L_N, R_N) мебошад. Дар раунди N-ум ҷойивазкунии L_N ва R_N ба амал намеояд, барои онки ҷараёни рамзкушоӣ осон бошад, яъне амали рамзкушоӣ калидҳо ба тартиби баръакс истифода бурда мешаванд. Масалан, ба ҷойи калидҳои K_0 , $K_1,..,K_N$ аз калидҳои K_N , $K_{N-1},..,K_0$. Аз ин ҷо барои рамзкушоӣ кардан аз форрмулаҳои зерин истифода бурда мешавад:

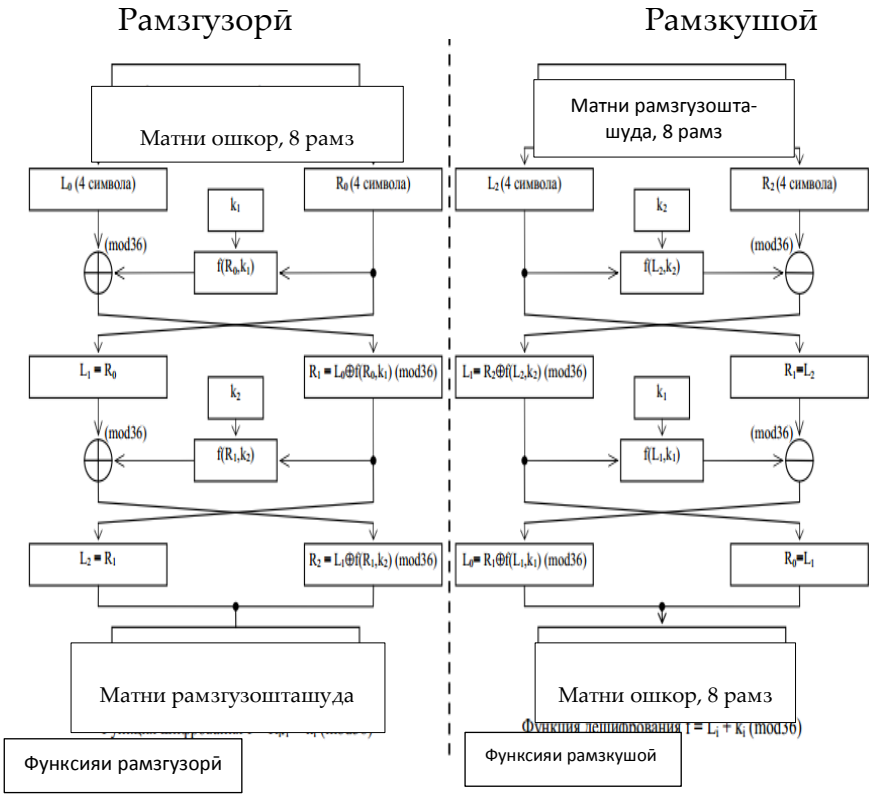
$$L_{i-1} = R_i \oplus f(L_i, K_{i-1});$$

$$R_{i-1} = L_i.$$

Ба намуди графикӣ шакли умумии алгоритми рамзгузорӣ ва рамзкушоӣ шабакаи Фейстел шакли зайлро дорад.



Алгоритми Фейстелро метавон бо дилхоҳ миқдори раундҳо истифода кард. Масалан, дар расми зерин бо ду раунд алгоритми рамзгузорӣ ва рамзкушоӣ шабакаи Фейстел оварда шудааст.



Функсиҳои дар шабаки Фейстел истифода шаванда

Дар кори худ «Cryptography and computer privacy» Хорст Фейстел ду блоки табдилдиҳӣ: блоки ҷойгузорӣ (s-блок, англ. s-box) ва блоки ҷойивазкунӣ (p-блок, англ. p-box) (дар функсияи $f(L_i, K_i)$)-ро шарҳу тавзеҳ додааст.

Метавон нишон дод, ки дилхоҳ табдилдиҳии дӯиро дар блокҳои додаҳои қайдкардашуда ба сурати s-блокҳо

табдил дод. Дар мақолаи асл ба ҷойи мафҳуми функсия мафҳуми блок истифода шудааст. Аз ин ҷост, ки сухан дар бораи рамзҳои блокӣ меравад.

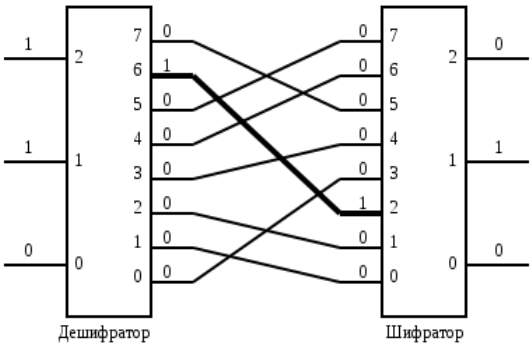
Ҳоло ин блокҳоро мухтасар мавриди баҳс қарор медиҳем.

S-блок

S-блок (англ. s-box аз substitution-box) аз қисматҳои зерин иборат мебошад:

1) дешифратор — табдилдиҳандаи n-разрядии сигнали дӯӣ ба сигнали якразрияди аз рӯйи асоси 2^n;
2) системаи комутаторҳо-алоқакунандаҳои дохилӣ (имконияти 2n! лоқакунанда мавҷуд аст);
3) шифратор - табдилдиҳандаи сигнал аз блоки якразриядаи 2^n ба блоки n-разриядаи дӯӣ;

Шакли умумии ин блок чунин аст:



Ҳангоми калон будани n таҳлили S-блоки n –разряда хело душвор мебошад. Дар ҳолати умумӣ S-блок метавонад, миқдори ғаримувофиқӣ вуруд/хуруҷ дошта бошад. Дар ин ҳолат дар системаи комутатсия аз ҳар як баромади дешифратор метавонад, натанҳо як

алоқакунанда барояд, балки метавонад, ягонто баромад надошта бошад. Барои вурудии шифратор низ айнан ҳамин хел мебошад.

Амалкарди ин блок чунин аст: аз сутуни дешифратор, ягон адад интихоб карда шуда, ба сутуни шифратор аз рӯйи схемаи овардашуда мувофиқ гузошта мешавад, масалан адади 6 аз сутуни дешифратор ба адади 2-и сутуни шифратор мувофиқат мекунед, адаи 0 бошад ба адади 3 ва ҳоказо.

Ҳамин тариқ метавон, барои блоки се разриядаи ҷадвали зеринро ҳосил кард:

№ комбинатсия	0	1	2	3	4	5	6	7
Вуруд	000	001	010	011	100	101	110	111
Хуруҷ	011	000	001	100	110	111	010	101

Қайд кардан ба маврид аст, ки ин блок барои алгоритмҳои гуногуни рамзгузории симметрӣ татбиқ карда мешавад, ба монанди:

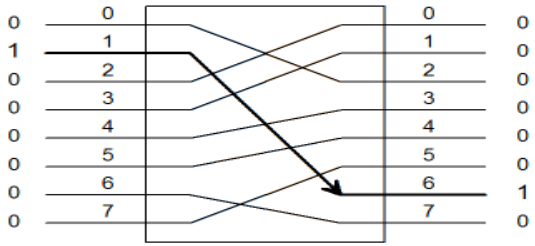
1) AES (англ. Advanced Encryption Standard) - стандарт рамзгузории амрикоӣ;
2) ГОСТ 28147-89 —стандарти давлатии рамзгузории Росия;
3) DES (англ. Data Encryption Standard) – стандарти рамзгузории додаҳо дар ИМА то пайдошавии AES;
4) Twofish.

P-блок

Блоки ҷойгузорӣ (p-блок, англ. p-box) ҳамаи ҳолати (положение) рамзро иваз карда, воситаи хаттӣ мебошад. Ин блок метавонад, миқдори бисёри вурудӣ ва хуруҷӣ дошта бошад. Аммо бо назардошти хаттӣ будани система наметавон онро крипто-устувор номид.

Криптоанализи калид барои p-блоки n-разряда бо равон кардани n-1-пайғоми гуногун ба вурудӣ, ки ҳар кадомаш аз n-1 сифр («0») ва воҳид («1») иборат мебошанд амалӣ карда мешавад.

Шакли схематикии амалкарди блоки мазкур чунин аст:



Истифодаи P-блокро баъдан дар рамзи DES пурра мавриди баҳс қарор медиҳем.

Барои хубтар дарк кардани алгоритми Фейстел мисолеро дида мебароем.

Мисоли 1. Матни “донишгоҳ”-ро бо истифода аз калиди $K = [k_1, k_2]$ =[дарс, хонӣ] рамзгузорӣ мекунем.

Ҳал. Ибтидо матни ошкор ба қисматҳои 8-рамзӣ (символӣ) ҷудо карда мешавад.

Д	о	н	и	ш	г	о	ҳ
Блок							

Акнун бо истифода аз алгоритми ду раундаи Фейстел (нақшаи 2) ба рамзгузорӣ оғоз мекунем.

Раунди 1.

$L_0 =$ дони $R_0 =$ шгоҳ

$k_1 =$ дарс

	$f(R_0,k_1) = R_0 + +k_1 (mod 35)$					$R_1 = L_0 + +f(R_0,k_1)(mod 35)$			
R_0	ш	г	о	ҳ	L_0	д	о	н	и
	30	3	18	27		5	18	17	10
k_1	д	а	р	с	$f(R_0,k_1)$	а	г	г	к
	5	0	20	21		0	3	3	13
$R_0 + k_1$	0	3	3	13	$L_0 + f(R_0,k_1)$	5	21	20	23
$f(R_0,k_1)$	а	г	г	к	R_1	д	с	р	у

Раунди 2.

$L_1 = R_0 =$ шгоҳ $R_1 =$ дсру

$k_2 =$ хонӣ

	$f(R_1,k_2) = R_1 + +k_2 (mod 35)$					$R_2 = L_1 + +f(R_1,k_2)(mod 35)$			
R_1	д	с	р	у	L_1	ш	г	о	ҳ
	5	21	20	23		30	3	18	27
k_2	х	о	н	й	$f(R_1,k_2)$	ъ	ғ	в	я
	26	18	17	11		31	4	2	34
$R_1 + k_2$	31	4	2	34	$L_1 + f(R_1,k_2)$	26	7	20	26
$f(R_0,k_1)$	ъ	ғ	в	я	R_2	х	ё	р	х

$L_2 = R_1 =$дсру $R_2 =$ хёрх

Ҳамин тариқ, матни додашуда ба сурати $L_2 + R_2 =$ дсрухёрх рамзгузорӣ карда шуд.

Ҷавоб: дсрухёрх

Акнун матни рамзгузошташударо рамзкушоӣ мекунем. Тавре, ки қайд кардем, барои рамзкушоӣ калид ба тартиби баръакс истифода бурда мешавад.

Раунди 1.

$L_2 = R_1 =$ дсру $R_2 =$ хёрх

$k_2 =$ хонӣ

	$f(L_2,k_2)=L_2+$ $+k_2(mod35)$					$L_1=R_2-$ $-f(L_2,k_2)(mod35)$			
L_2	д	с	р	у	R_2	х	ё	р	х
	5	21	20	23		26	7	20	26
k_2	х	о	Н	ӣ	$f(L_2,k_2)$	ъ	ғ	в	я
	26	18	17	11		31	4	2	34
L_2+k_2	31	4	2	34	$R_2-f(L_2,k_2)$	30	3	18	27
$f(L_2,k_2)$	ъ	ғ	В	я	L_1	ш	г	о	ҳ

$L_1 =$ъғвя $R_1 = L_2 =$ шгоҳ

Раунди 2.

$L_1 =$ ъюоч $R_1 =$ шғвю

$k_1 =$ дарс

	$f(L_1,k_1)=L_1+$ $+k_1(mod35)$					$L_0=R_1-$ $-f(L_1,k_1)(mod35)$			
L_1	ш	г	о	ҳ	R_1	д	с	р	у
	30	3	18	27		5	21	20	23
k_1	д	а	Р	с	$f(L_1,k_1)$	а	г	г	к
	5	0	20	21		0	3	3	13
L_1+k_1	0	3	3	13	$R_1+f(L_1,k_1)$	5	18	17	10
$f(L_1,k_1)$	а	г	Г	к	L_0	д	о	н	и

$L_0 = дони$ $R_0 = L_1 =$*шгоҳ*

Ҳамин тариқ, матни рамзгузошташуда рамзкушоӣ карда шуд.

Қайд. *Дар схемаи овардашуда, алифбоӣ тоҷикӣ истифода бурда шуд, ки ҳарфҳои он чунин рақамгузорӣ карда шудаанд.*

А а	Б б	В в	Г г	Ғ ғ
0	1	2	3	4
Д д	Е е	Ё ё	Ж ж	З з
5	6	7	8	9
И и	Ӣ ӣ	Й й	К к	Қ қ

10	11	12	13	14
Л л	М м	Н н	О о	П п
15	16	17	18	19
Р р	С с	Т т	У у	Ӯ ӯ
20	21	22	23	24
Ф ф	Х х	Ҳ ҳ	Ч ч	Ҷ ҷ
25	26	27	28	29
Ш ш	Ъ ъ	Э э	Ю ю	Я я
30	31	32	33	34

Қайд. *Азбаски калиди мо аз 8 символ (ду қисм) иборат буд бинобар ин, дар раунди якум қисмати якум (4 ҳарфи аввала) ва дар раунди дуюм қисмати дуюм (чор ҳарфи боқимонда) истифода карда шуд. Ба ҳамин монанд, агар калид аз як қисм иборат бошад, пас дар раунди дуюм метавон ҳарфҳои онро аз рӯйи ягон қоида ҷойгардони карда, истифода бурд.*

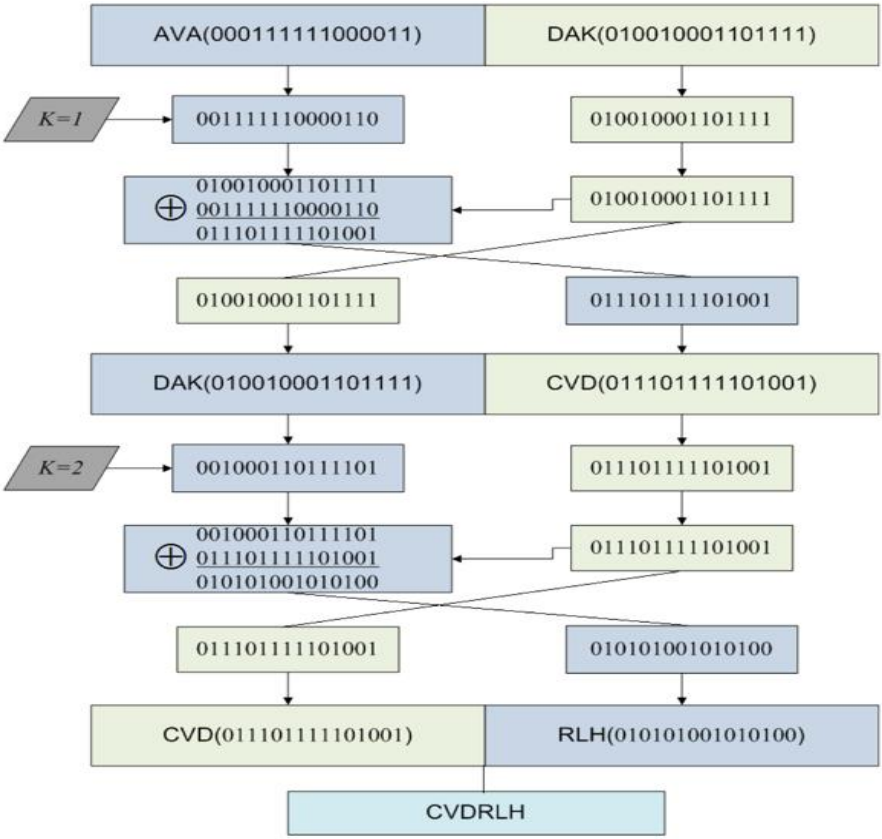
Метавон қайд кард, ки дар рамзи мазкур матн натанҳо ба блокҳои иборат аз 8 рамзӣ тақсим карда мешавад, балки метавонад ба 4 ё шаш рамзӣ низ тақсим карда шавад.

Мисоли 2. Калимаи AVADAKEDAVRA рамзгузорӣ карда шавад. Матни мазкурро ба ду қисми шашсимволӣ тақсим мекунем — AVADAK | EDAVRA. Барои осонии кор аз рӯйи ягон қоида коди дӯии ҳар як ҳарфро менависем.

A	V	A	D	A	K	E	D	A	V	R	A
00011	11110	00011	01001	00011	01111	00001	01001	00011	11110	01010	00011

Акнун бо ёрии шабакаи ду раундаи Фейстел блоки якуми матни додашударо бо истифода аз калиди K, ки ба намуди дӯӣ додашудааст рамзгузорӣ мекунем:

$$K = [001111110000110, 001000110111101]$$



Ба ҳамин монанд, агар қисми дуюм рамзгузорӣ кунем, чунин натиҷа MOSSTR ҳосил мешавад.

Қайд. *Ба сифати функсияи f дар рамзи Фейстел метавон дилхоҳ функсияи мувофиқро истифода кард. Устувории криптографӣ аз ин функсия вобаста мебошад.*

Барои рамзгузорӣ ва рамзкушой кардан тавассути методи Фейстел метавон аз барномаи зерин, ки дар забони C# навишта шудааст, истифода кард.

```
using System;
using System.Text;
using System.Threading.Tasks;
namespace FEISTEL
{
   class Program
   {
      //str - сатри додашуда, key - калид (на камтар аз 8 
символ (рамз))
      public static string feistel_crypt(string str, string key)
      {
         if (key.Length < 8)
            throw new ArgumentException("Калид бениҳоят 
хурд аст! (бояд min = 8 символ бошад)");

         byte[] str_arr = Encoding.Default.GetBytes(str);
         byte[] key_arr = Encoding.Default.GetBytes(key);

         //агар дарозӣ каратии 84 набошад(8 байт)
         int diff = str_arr.Length % 8;
         if (diff != 0)
         {
```

```
            byte[] temp = new byte[str_arr.Length + (8 - diff)];
            Array.Copy(str_arr, temp, str_arr.Length);
            str_arr = temp;
        }
        byte[] res_arr = new byte[str_arr.Length];
        //рамзгузорӣ мекунем.
        for (int i = 0; i < str_arr.Length; i = i + 8)
        {
            byte[] block = new byte[8];
            Array.Copy(str_arr, i, block, 0, 8);

            for (int j = 0; j <= 9; j++)
            {
                //2 зерблок месозем
                byte[] subblock_left_arr = new byte[4];
                Array.Copy(block, subblock_left_arr, 4);
                byte[] subblock_right_arr = new byte[4];
                Array.Copy(block, 4, subblock_right_arr, 0, 4);

                //калиди раунди месозем
                byte[] subblock_key_arr = new byte[4];
                Array.Copy(key_arr, subblock_key_arr, 4);
                subblock_key_arr = shift_key_left(key_arr, j);

                if (j != 9)//агар j = 9 бошад, ҷойи зерблокҳо иваз
карда намешаванд.
                    block = crypt_block(subblock_left_arr,
subblock_right_arr, subblock_key_arr, false);
```

```
                else
                    block = crypt_block(subblock_left_arr,
subblock_right_arr, subblock_key_arr, true);
                }
                //скидываем блок в результирующий массив
                Array.Copy(block, 0, res_arr, i, block.Length);
            }
            return Encoding.Default.GetString(res_arr);
        }

        private static byte[] crypt_block(byte[] subblock_left_arr,
byte[] subblock_right_arr, byte[] subblock_key_arr, bool
isLast)
        {
         int subblock_left =
BitConverter.ToInt32(subblock_left_arr, 0);
            int subblock_right =
BitConverter.ToInt32(subblock_right_arr, 0);
        int subblock_key =
BitConverter.ToInt32(subblock_key_arr, 0);

            //xor
            subblock_left = subblock_left ^ subblock_key;
            subblock_left_arr =
BitConverter.GetBytes(subblock_left);

            byte[] tmp = new byte[2];
            Array.Copy(subblock_left_arr, tmp, 2);
```

```
            Int16 left = BitConverter.ToInt16(tmp, 0);
            Array.Copy(subblock_left_arr, 2, tmp, 0, 2);
            Int16 right = BitConverter.ToInt16(subblock_left_arr, 2);

            //xor
            subblock_right = f(left, right) ^ subblock_right;
            subblock_right_arr =
BitConverter.GetBytes(subblock_right);

            //ҷойи зерблокҳоро иваз мекунем ё намекунем
            byte[] res_arr = new byte[8];
            if (!isLast)
            {
                Array.Copy(subblock_right_arr, res_arr, 4);
                Array.Copy(subblock_left_arr, 0, res_arr, 4, 4);
            }
            else
            {
                Array.Copy(subblock_left_arr, res_arr, 4);
                Array.Copy(subblock_right_arr, 0, res_arr, 4, 4);
            }
            return res_arr;
        }

        public static string feistel_decrypt(string str, string key)
        {
            if (key.Length < 8)
                throw new ArgumentException("Калид бениҳоят
```

```
хурд аст! (бояд min = 8 символ бошад)");

            byte[] str_arr = Encoding.Default.GetBytes(str);
            byte[] key_arr = Encoding.Default.GetBytes(key);
            byte[] res_arr = new byte[str_arr.Length];

            //агар дарозӣ бо 64 (8байт) карати набошад
            int diff = str_arr.Length % 8;
            if (diff != 0)
                throw new ArgumentException("Сатр нодуруст
дохил карда шудааст!");
            //аз охир сар мекунем
            for (int i = str_arr.Length - 8; i >= 0; i = i - 8)
            {
                byte[] block = new byte[8];
                Array.Copy(str_arr, i, block, 0, 8);
                //калиди раундирро бо тартиби баръакс истифода
мекунем.
                for (int j = 9; j >= 0; j--)
                {
                    //2 зерблок месозем
                    byte[] subblock_left_arr = new byte[4];
                    Array.Copy(block, subblock_left_arr, 4);
                    byte[] subblock_right_arr = new byte[4];
                    Array.Copy(block, 4, subblock_right_arr, 0, 4);

                    //калиди раундӣ месозем
                    byte[] subblock_key_arr = new byte[4];
```

```
                Array.Copy(key_arr, subblock_key_arr, 4);
                subblock_key_arr = shift_key_left(key_arr, j);

                if (j != 0)//агар j = 0 бошад, онгоҳ ҷойи
зерблокҳоро иваз кардан лозим намешавад
                    block = decrypt_block(subblock_left_arr,
subblock_right_arr, subblock_key_arr, false);
                else
                    block = decrypt_block(subblock_left_arr,
subblock_right_arr, subblock_key_arr, true);
            }
            //блокҳои натиҷавиро ба массив илова мекунем
            Array.Copy(block, 0, res_arr, i, block.Length);
        }
        return Encoding.Default.GetString(res_arr);
    }

    private static byte[] decrypt_block(byte[]
subblock_left_arr, byte[] subblock_right_arr, byte[]
subblock_key_arr, bool isLast)
    {
     int subblock_left =
BitConverter.ToInt32(subblock_left_arr, 0);
        int subblock_right =
BitConverter.ToInt32(subblock_right_arr, 0);
    int subblock_key =
BitConverter.ToInt32(subblock_key_arr, 0);
```

```
            byte[] tmp = new byte[2];
            Array.Copy(subblock_left_arr, tmp, 2);
            Int16 left = BitConverter.ToInt16(tmp, 0);
            Array.Copy(subblock_left_arr, 2, tmp, 0, 2);
            Int16 right = BitConverter.ToInt16(subblock_left_arr, 2);

            //xor
            subblock_right = f(left, right) ^ subblock_right;

            //xor
            subblock_left = subblock_left ^ subblock_key;
            subblock_left_arr =
BitConverter.GetBytes(subblock_left);

            subblock_right_arr =
BitConverter.GetBytes(subblock_right);

            //ҷойи зерблокҳоро иваз мекунем ё намекунем
            byte[] res_arr = new byte[8];
            if (!isLast)
            {
                Array.Copy(subblock_right_arr, res_arr, 4);
                Array.Copy(subblock_left_arr, 0, res_arr, 4, 4);
            }
            else
            {
                Array.Copy(subblock_left_arr, res_arr, 4);
                Array.Copy(subblock_right_arr, 0, res_arr, 4, 4);
```

```
        }
        return res_arr;
    }
    private static int f(Int16 left, Int16 right)
    {
        //7 мавқеъ кучиш ба чап
        int l = left << 7;
        int r = l >> 16;
        left = (Int16)(l + r);

        // 5 мавқеъ кучиш ба рост
        l = right >> 5;
        r = l << 11;//16-5
        right = (Int16)(l + r);

        //Ҷои қисматҳоро иваз мекунад
        int res = (int)left << 16;
        return res + right;
    }

    //Қисми чапи зеркалидро бармегардонад
    private static byte[] shift_key_left(byte[] key_arr, int i)
    {
        byte[] tmp = new byte[4];
        Array.Copy(key_arr, tmp, 4);
        int left = BitConverter.ToInt32(tmp, 0);
        Array.Copy(key_arr, 4, tmp, 0, 4);
        int right = BitConverter.ToInt32(tmp, 0);
```

```
            //i * 3 мавқеъ кучиши даври ба рост
            int l_l = left << (i * 3);
            int r_r = right >> (32 - i * 3);
            left = l_l + r_r;

            return BitConverter.GetBytes(left);
        }
        static void Main(string[] args)
        {
            String text, Key, Etext, Dtext;
            text = Console.ReadLine();
            Key = Console.ReadLine();
            Etext = feistel_crypt(text, Key);
            Console.WriteLine(Etext);
            //Рамзкушой
            Dtext = feistel_decrypt(Etext, Key);
            Console.WriteLine(Dtext);
            Console.ReadKey();
        }
    }
}
```

2. Алгоритм (рамз)-и DES

DES (англ. data encryption standard) — алгоритми симметрии рамзгузорӣ буда, соли 1977 аз тарафи ширкати

IBM[1] дар асоси сет ё шабакаи Фейстел бо 16 давр (раунд) ва калиди дарозиаш ба 56 бит сохта шуда, аз ҷониби ҳукумати ИМА ҳамчун стандарти расмии (FIPS 46-3) тасдиқ карда шудааст. Андозаи блокҳо барои DES ба 64 бит баробар буда, дар он комбинатсияи ғайрихатии S-блокҳо ва ҷойивазкунии хатии E, IP, IP^{-1} табдилдиҳиҳо истифода бурда мешаванд. Барои DES якчанд реҷаҳои корӣ мавҷуд аст:

1) ECB (англ. electronic code book) — реҷаи китоби электронии кодӣ;
2) CBC (англ. cipher block chaining) — реҷаи пайвасткунии блокҳо;
3) CFB (англ. cipher feed back) — реҷаи алоқаи баръакс бо шифротекст;
4) OFB (англ. output feed back) — реҷаи алоқаи баръакс баромад.

Дар замони муосир инкишофи DES алгоритми Triple DES (3DES) ба ҳисоб меравад. Дар 3DES

[1] IBM (International Business Machines) —ширкати амрикоӣ дар шаҳри Армонке (штат. Ню-Йорк) буда, яке аз бузургтарин истеҳсокунанда ва таъминкунандаи воситаҳои техникӣ, таъминоти барномавӣ ва инчунин IT-хизматрасониҳо ба ҳисоб меравад. Ширкати мазкур аз ҷониби соҳибкори амрикоӣ Чарлз Рэнлетт Флинт (24 январи 1850, Томастон, Мэн — 26 феврали 1934) соли соли 1911 бо номи C-T-R, сохта шуда, сипас соли 1924 номи IBM-ро гирифт.

рамзгузорӣ/рамзкушоӣ бо татбиқи секаратаи алгоритми DES иҷро карда мешавад.

Ин алгоритм дар корхонаҳои давлатии ИМА бо мақсади муҳофизати итилоот аз дастбурдҳои гуногун истифода бурда мешуд. Алгоритме, ки дар асоси ин стандарт ташкил шуд, зуд паҳн гардида, ҳатто соли 1980 аз тарафи ANSI стандартизатсия карда шуд.

Дар замони ҳозира DES яке аз алгоритмҳои паҳнгашта мебошад, ки дар системаи муҳофизати маълумотҳои тиҷорати истифода бурда мешавад.

Пеш аз мавриди баҳс қарор додани алгоритми мазкур хосиятҳои асосии онро меорем:

1) Танҳо 1 калиди 56 битаро истифода мебарад.
2) Пушидани маълумотро бо ёрии як пакет барои кушодан дигарашро истифода мебарад.
3) Нисбатан соддагии алгоритм метавонад бо суръати тез маълумотро дарёбад.
4) Ба қадри кифоя суръати баланди алгоритм

Алгоритми DES маълумотҳои рамзгузори-шудаи 64 битаро бо ёрии калиди 56 бита ба вуҷуд меорад. Барои рамзгузорӣ аз формулаи зерин истифода бурда мешавад.

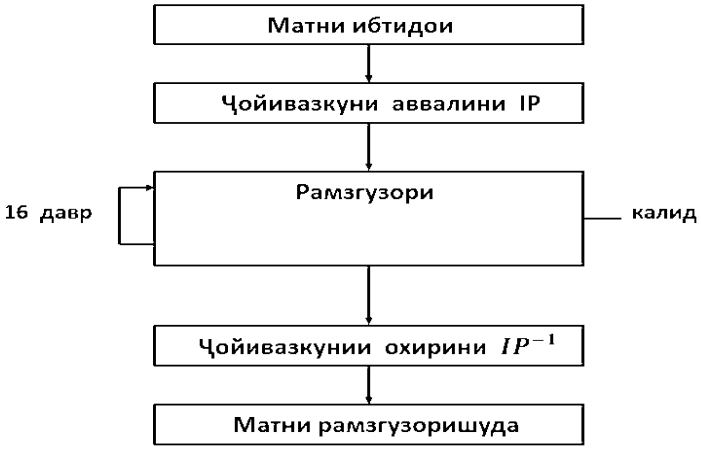
$$L_i = R_{i-1},$$
$$R_i = L_{i-1}\ xor\ f(R_{i-1}, K_i), i = 1,2,\dots,16; \qquad (1)$$

дар инчо xor –амали ҷамъ аз рӯи модули 2 мебошад. Функсияи f-функсияи рамзгузорӣ номида мешавад. Баъдтар онро мавриди баҳс қарор медиҳем.

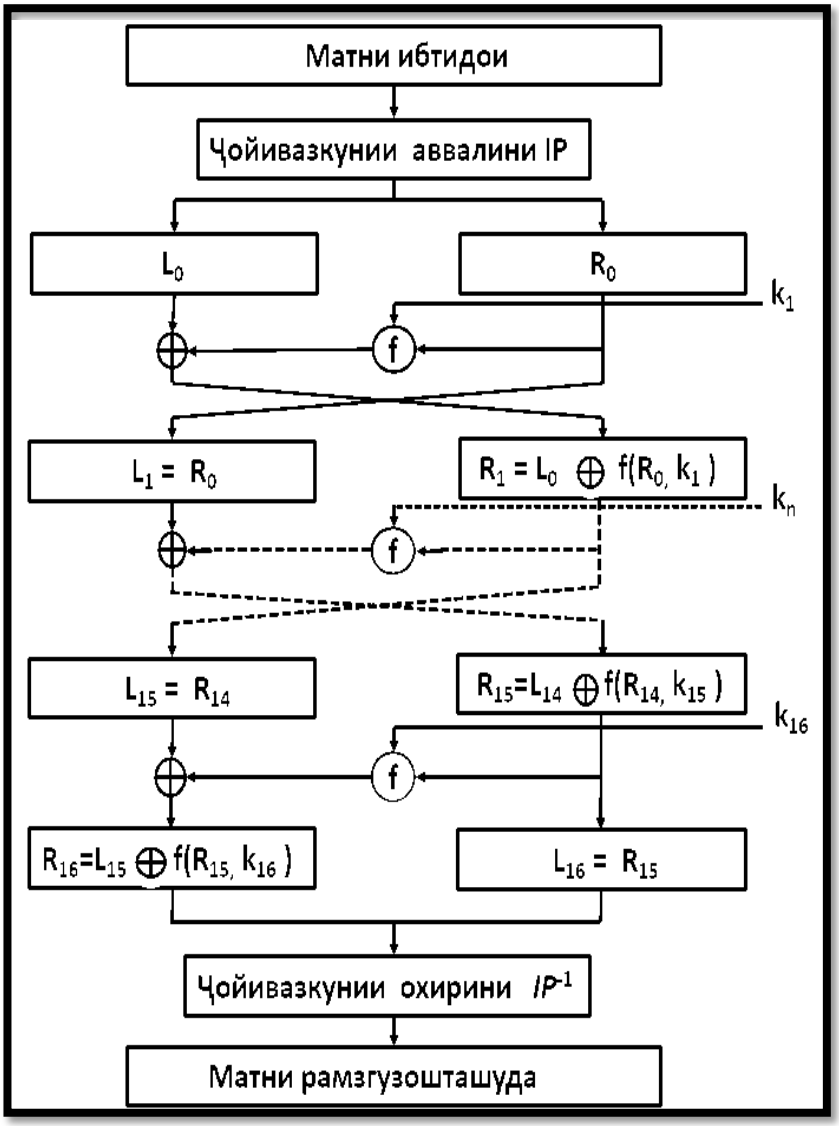
Рамзкушой бошад – ин амали баръакси рамгузорӣ буда, барои иҷрои он аз формулаи зерин истифода бурда мешавад:

$$R_{i-1} = L_i,$$
$$L_{i-1} = R_i xor\, f(L_i, K_i), i = 1,2, \dots ,16. \qquad (2)$$

Нақшаи умумии алгоритми DES чунин шаклро дорад:



Сохтори умумии алгоритми DES ба намуди графикӣ шакли зеринро дорад.



Алгоритми мазкур аз ду қисм иборат аст:

1) Сохтани калид ва зеркалидҳо.
2) Рамзгузорӣ

Ҳоло ҳарду ин қадамҳоро дида мебароем.

Қадами 1. Сохтани калид ва зеркалидҳо.

Бигузор калиди К-и 64 бита бо сурати зерин дода шуда бошад.

$$К = i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8 i_9 i_{10} i_{11} i_{12} i_{13} i_{14} i_{15} i_{16} i_{17} i_{18} i_{19} i_{20} i_{21} i_{22} i_{23} i_{24} i_{25} i_{26} i_{27} i_{28} i_{29} i_{30} i_{31} i_{32} i_{33} i_{34} i_{35} i_{36} i_{37} i_{38} i_{39} i_{40} i_{41} i_{42} i_{43} i_{44} i_{45} i_{46} i_{47} i_{48} i_{49} i_{50} i_{51} i_{52} i_{53} i_{54} i_{55} i_{56} i_{57} i_{58} i_{59} i_{60} i_{61} i_{62} i_{63} i_{64}.$$

Матритсаи тайёрии калиди ибтидоӣ G

57	**49**	**41**	**33**	**25**	**17**	**09**
01	**58**	**50**	**42**	**34**	**26**	**18**
10	**02**	**59**	**51**	**43**	**35**	**27**
19	**11**	**03**	**60**	**52**	**44**	**36**
63	**55**	**47**	**39**	**31**	**23**	**15**
07	**62**	**54**	**46**	**38**	**30**	**22**
14	**06**	**61**	**53**	**45**	**37**	**29**
21	**13**	**05**	**28**	**20**	**12**	**04**

Ҷадвали 1. Матритсаи тайёрии калиди ибтидоӣ G

-ро ки татбиқ карда, калиди 56 битаи K^+ -ро ҳосил мекунем.

$$K^+ = i_{57} i_{49} i_{41} i_{33} i_{25} i_{17} i_9 i_1 i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 i_{59} i_{51} i_{43} i_{35} i_{27} i_{19} i_{11} i_3 i_{60} i_{52} i_{44} i_{36} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7 i_{62} i_{54} i_{46} i_{38} i_{30} i_{22} i_{14} i_6 i_{61} i_{53} i_{45} i_{37} i_{29} i_{21} i_{13} i_5 i_{28} i_{20} i_{12} i_4$$

Қайд. *Матритсаи K^+ аз марисаи К чунин ҳосил шудааст: ба сифати элементи якуми матритсаи K^+*

элементи 57-уми матритсаи K ба сифати элементи дуюм бошад, элементи 49-ум ва гайра гирифта шудааст.

Натиҷаи табдилдиҳии K^+ ба 2 блоки 28 бита: C_0 ва D_0 тақсим карда мешавад, аз он ҷумла C_0 битҳои i_{57}, i_{49},…, i_{36} –уми калиди K^+ ва D_0 битҳои i_{63}, i_{55} ,…, i_4 –уми калиди K^+ мебошад.

Акнун барои ба тарафи чап даврӣ кучонидани битҳои C_0 ва D_0 аз рақамҳои итератсия, ки дар ҷадвали зерин оварда шудаанд, истифода бурда мешавад.

рақами итерасия	кучонидан (бит)
01	1
02	1
03	2
04	2
05	2
06	2
07	2
08	2
09	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Ҷадвали 2. Ҷадвали ҳеҷиш (ба чап) додан ва муаянкунии калид

Пас аз татбиқи ҷадвали 2 16 ҷуфти C_i ва D_i ($i = 1 \dots 16$) ҳосил карда мешаванд, ки шакли зеринро доранд:

		C_0: $i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}$ $i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}$
		D_0: $i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}$ $i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4$
1	1	C_1: $i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}$ $i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}$
		D_1: $i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}$ $i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}$
2	1	C_2: $i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}$ $i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}$
		D_2: $i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}$ $i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}$
3	2	C_3: $i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}$ $i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}$
		D_3: $i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}$ $i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}$
4	2	C_4: $i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}$ $i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}$
		D_4: $i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}$ $i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}$
5	2	C_5: $i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}$ $i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1$
		D_5: $i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}$ $i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7$

6	2	$C_6:\ i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}$ $i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}$
		$D_6:\ i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}$ $i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}$
7	2	$C_7:\ i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}$ $i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}$
		$D_7:\ i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}$ $i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}$
8	2	$C_8:\ i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}$ $i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}$
		$D_8:\ i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}$ $i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}$
9	1	$C_9:\ i_2i_{59}i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}i_9$ $i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}$
		$D_9:\ i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}$ $i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}$
10	2	$C_{10}:\ i_{51}i_{43}i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}$ $i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}$
		$D_{10}:\ i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7$ $i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}$
11	2	$C_{11}:\ i_{35}i_{27}i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1$ $i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}$
		$D_{11}:\ i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}$ $i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}$
12	2	$C_{12}:\ i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}$ $i_{42}i_{34}i_{26}i_{18}i_{10}\ i_2i_{59}i_{51}i_{43}i_{35}i_{27}$
		$D_{12}:\ i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}$ $i_{38}i_{30}i_{22}i_{14}i_6i_{61}i_{53}i_{45}i_{37}i_{29}$

13	2	$C_{13}: i_3 i_{60} i_{52} i_{44} i_{36} i_{57} i_{49} i_{41} i_{33} i_{25} i_{17} i_9 i_1 i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 i_{59} i_{51} i_{43} i_{35} i_{27} i_{19} i_{11}$
		$D_{13}: i_5 i_{28} i_{20} i_{12} i_4 i_{63} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7 i_{62} i_{54} i_{46} i_{38} i_{30} i_{22} i_{14} i_6 i_{61} i_{53} i_{45} i_{37} i_{29} i_{21} i_{13}$
14	2	$C_{14}: i_{52} i_{44} i_{36} i_{57} i_{49} i_{41} i_{33} i_{25} i_{17} i_9 i_1 i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 i_{59} i_{51} i_{43} i_{35} i_{27} i_{19} i_{11} i_3 i_{60}$
		$D_{14}: i_{20} i_{12} i_4 i_{63} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7 i_{62} i_{54} i_{46} i_{38} i_{30} i_{22} i_{14} i_6 i_{61} i_{53} i_{45} i_{37} i_{29} i_{21} i_{13} i_5 i_{28}$
15	2	$C_{15}: i_{36} i_{57} i_{49} i_{41} i_{33} i_{25} i_{17} i_9 i_1 i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 i_{59} i_{51} i_{43} i_{35} i_{27} i_{19} i_{11} i_3 i_{60} i_{52} i_{44}$
		$D_{15}: i_4 i_{63} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7 i_{62} i_{54} i_{46} i_{38} i_{30} i_{22} i_{14} i_6 i_{61} i_{53} i_{45} i_{37} i_{29} i_{21} i_{13} i_5 i_{28} i_{20} i_{12}$
16	1	$C_{16}: i_{57} i_{49} i_{41} i_{33} i_{25} i_{17} i_9 i_1 i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 i_{59} i_{51} i_{43} i_{35} i_{27} i_{19} i_{11} i_3 i_{60} i_{52} i_{44} i_{36}$
		$D_{16}: i_{63} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7 i_{62} i_{54} i_{46} i_{38} i_{30} i_{22} i_{14} i_6 i_{61} i_{53} i_{45} i_{37} i_{29} i_{21} i_{13} i_5 i_{28} i_{20} i_{12} i_4$

Акнун ҷуфти C_i ва D_i $(i = 1 \dots 16)$ – ҳоро пайваст карда (дар бари ҳам навишта), барои онҳо матритсаи H, ки шакли зеринро дорад, татбиқ мекунем.

14	**17**	**11**	**24**	**01**	**05**
03	**28**	**15**	**06**	**21**	**10**
23	**19**	**12**	**04**	**26**	**08**
16	**07**	**27**	**20**	**13**	**02**
41	**52**	**31**	**37**	**47**	**55**
30	**40**	**51**	**45**	**33**	**48**
44	**49**	**39**	**56**	**34**	**53**

46 42 50 36 29 32

Ҷадвали 3. Матритсаи H коркарди охирини калид.

Пас аз татбиқи матритсаи охирон (Ҷадвали 3) 16-то зеркалиди $K_1, K_2, \dots, K_{16}$, ки ҳар кадомашон 48 битӣ мебошанд, сохта мешаванд, яъне $K_i =$ H(C_i, D_i) $i = 1 \dots 16$. Барои содаги ин амалро барои ҷуфти C_1D_1 дида мебароем, ки шакли зеринро доранд:

C_1D_1: $i_{49}i_{41}i_{33}i_{25}i_{17}i_9i_1i_{58}i_{50}i_{42}i_{34}i_{26}i_{18}i_{10}i_2i_{59}i_{51}i_{43}i_{35}i_{27}$
$i_{19}i_{11}i_3i_{60}i_{52}i_{44}i_{36}i_{57}i_{55}i_{47}i_{39}i_{31}i_{23}i_{15}i_7i_{62}i_{54}i_{46}i_{38}i_{30}i_{22}i_{14}$
$i_6i_{61}i_{53}i_{45}i_{37}i_{29}i_{21}i_{13}i_5i_{28}i_{20}i_{12}i_4i_{63}$

Пас аз татбиқи матритсаи H барои ҷуфти C_1D_1 калиди K_1 ба сурати зерин ҳосил мешавад.

K_1=$i_{10}i_{51}i_{34}i_{60}i_{49}i_{17}i_{33}i_{57}i_2i_9i_{19}i_{42}i_3i_{35}i_{26}i_{25}i_{44}i_{58}$
$i_{59}i_1i_{36}$ $i_{27}i_{18}i_{41}i_{22}i_{53}i_{23}i_{29}$ $i_{61}i_{21}i_{38}i_{63}i_{15}i_{20}i_{45}i_{14}i_{13}$
$i_{62}i_{55}i_{31}$

Ба ҳамин монанд H$(C_2D_2), \dots,$ H$(C_{16}D_{16})$ – ҳо сохта мешаванд, ки дар натиҷа 16 зеркалидҳои калиди K^+ (56 бита) пайдо мешаванд. Дар ҳар як даври рамзгузории алгоритми DES ин зеркалидҳо мувофиқ ба даври рамзгузорӣ истифода бурда мешаванд.

Мисол. Бигузор калиди K ба сурати дӯӣ чунин дода шуда бошад.

K: 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

Матритаи (Ҷадвали) калиди ибтидои G-ро (ҷадвали 1) татбиқ карда, калиди 56 битаи K^+ −ро ҳосил мекунем, ки шакли зеринро дорад:

K^+: **1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111**

Калиди K^+ −чунин ҳосил шудааст: бити 57-умини калиди K дар ҷойи аввал, бити 49-умини калиди K дар ҷойи дуюм, бити 41-умини калиди K дар ҷойи сеюм ва ҳоказо навишта шудаанд.

Қайд. *Барои ҳисоб намудани қимати K^+ метавон аз зербарномаи зерин истифода кард:*

```
#include <iostream>
using namespace std;
int main(int argc, char** argv) {
  int
G[]={57,49,41,33,25,17,9,1,58,50,42,34,26,18,10,2,59,51,43,35,2,19,
11,3,60,52,44,36,63,55,47,39,31,23,15,7,62,54,46,38,30,22,14,6,61,5
3,45,37,29,21,13,5,28,20,12,4};
 string  S="00001001100110100010101110111100110011011011100110111111110001";
 int i, n;
 n=S.length();
 for (i=0; i<n; i++)
 {
        if (i%7==0)
   cout<<" ";
```

```
  cout<<S[G[i]];
}
 return 0;
}
```

Пас аз ин, калиди K^+ ба 2 қисми баробари C_0 ва D_0, ки ҳар кадомашон 28 битӣ мебошанд, ҷудо карда мешавад.

C_0: **1111000 0110011 0010101 0101111**

D_0: **0101010 1011001 1001111 0001111**

Бо истифода аз ҷадвали ҷойивазкунии ба тарафи чап (ҷадвали 2) ҳамаи C_i ва D_i ($i = 1 \ldots 16$)-ҳо сохта мешаванд, ки шакли зеринро доранд:

		C_0: : **11110000110011001010101011111**
		D_0,: **01010101011001100111100011111**
1	**1**	C_1:: **11100001100110010101010111111**
		D_1: **10101010110011001111000111110**
2	**1**	C_2: **11000011001100101010101111111**
		D_2: **01010101100110011111000111101**
3	**2**	C_3: **00001100110010101010111111111**
		D_3: **01010110011001111000111110101**
4	**2**	C_4: **00110011001010101011111111100**
		D_4: **01011001100111100011111010101**

5	**2**	C_5**: 11001100101010101111111110000**
		D_5**: 01100110011110001111010101010101**
6	**2**	C_6**: 00110010101010111111111000011**
		D_6**: 10011001111000111110101010101**
7	**2**	C_7**: 11001010101011111111100001100**
		D_7**: 01100111100011111010101010110**
8	**2**	C_8**: 00101010101111111110000110011**
		D_8**: 10011110001111010101011001**
9	**1**	C_9**: 01010101011111111100001100110**
		D_9**: 00111100011110101010110011**
10	**2**	C_{10}**: 01010101111111100001100110011**
		D_{10}**: 11110001111010101011001100**
11	**2**	C_{11}**: 01010111111110000110011001011**
		D_{11}**: 11000111101010101100110011**
12	**2**	C_{12}**: 01011111111000011001100101011**
		D_{12}**: 00011110101010101100110011111**
13	**2**	C_{13}**: 01111111100001100110010101011**
		D_{13}**: 01111010101010110011001111100**

14	**2**	C_{14}**: 11111110000110011001010101**
		D_{14}**: 11101010101011001100111110001**
15	**2**	C_{15}**: 11111000011001100101010101111**
		D_{15}**: 10101010101100110011111000111**
16	**1**	C_{16}**: 11110000110011001010101011111**
		D_{16}**: 01010101011001100111100011111**

Қайд. *Барои як мавқеъ ба тарафи чап кучонидани элементҳои ягон сатр метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст истифода кард:*

```
#include <iostream>
using namespace std;
string kuchish(string S)
{
 int i, n;
 n=S.length();
 char c=S[0];
 for (i=0; i<n-1; i++)
   S[i]=S[i+1];
   S[i+1]=c;
 return S;
}
int main(int argc, char** argv) {
 string S="11110000110011001010101011111";
 string S1=kuchish(S);
```

```
 cout<<S1;
 return 0;
}
```

Ду мавқеъ кучонидан низ айнан ичро карда мешавад.

Дар ин қадам бошад, ҳар як ҷуфти C_i ва D_i $(i = 1 \dots 16)$ – ҳоро дар паҳлуи ҳам навишта, бо истифода аз ҷадвали H (ҷадвали 5) зеркалидҳои $K_1, \dots, K_{16}$ –ро ҳосил мекунем.

K_1: **000110 110000 001011 101111 111111 000111 000001 110010**

K_2: **011110 011010 111011 011001 110110 111100 100111 100101**

K_3: **010101 011111 110010 001010 010000 101100 111110 011001**

K_4: **011100 101010 110111 010110 110110 110011 010100 011101**

K_5: **011111 001110 110000 000111 111010 110101 001110 101000**

K_6: **011000 111010 010100 111110 010100 000111 101100 101111**

K_7: **111011 001000 010010 110111 111101 100001 100010 111100**

K_8: **111101 111000 101000 111010 110000 010011 101111 111011**

K_9: **111000 001101 101111 101011 111011 011110 011110 000001**

K_{10}: **101100 011111 001101 000111 101110 100100 011001 001111**

K_{11}: **001000 010101 111111 010011 110111 101101 001110 000110**

K_{12}: **011101 010111 000111 110101 100101 000110 011111 101001**

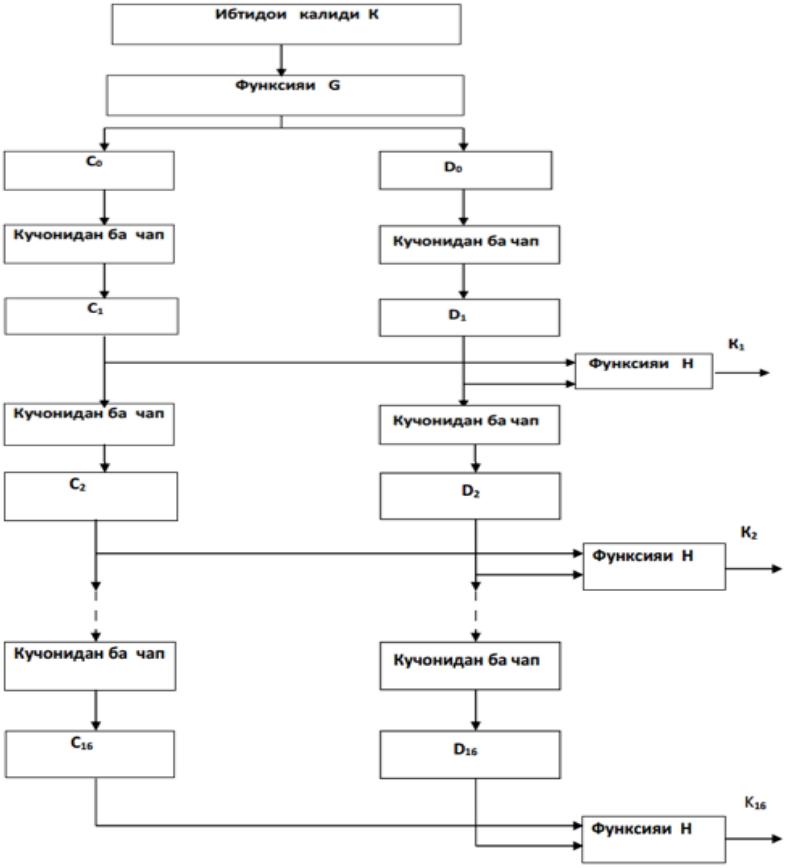
K_{13}: **100101 111100 010111 010001 111110 101011 101001 000001**

K_{14}: **010111 110100 001110 110111 111100 101110 011100 111010**

K_{15}: **101111 111001 000110 001101 001111 010011 111100 001010**

K_{16}: **110010 110011 110110 001011 000011 100001 011111 110101**

Алгоритми муайянкунии калид ва зеркалидҳо ба намуди графикӣ шакли зеринро дорад:



Қадами 2. Рамзгузорӣ.

Бигузор матни M (64 бит) бо чунин шакл дода шуда бошад:

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}

M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Дар ин ҷо ҳар як $M_i(i = 1, \dots, 64)$ қимати 0 ё 1-ро доро мебошад. Барои матни додашуда, матритсаи IP

58	**50**	**42**	**34**	**26**	**18**	**10**	**02**
60	**52**	**44**	**36**	**28**	**20**	**12**	**04**
62	**54**	**46**	**38**	**30**	**22**	**14**	**06**
64	**56**	**48**	**40**	**32**	**24**	**16**	**08**
57	**49**	**41**	**33**	**25**	**17**	**09**	**01**
59	**51**	**43**	**35**	**27**	**19**	**11**	**03**
61	**53**	**45**	**37**	**29**	**21**	**13**	**05**
63	**55**	**47**	**39**	**31**	**23**	**15**	**07**

Ҷадвали 4: Матритсаи ҷойивазкунии аввалини IP -ро татбиқ карда, матни ибтидоиро ба сурати зерин менависем.

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5

M_{63} M_{55} M_{47} M_{39} M_{31} M_{23} M_{15} M_7

Қайд.*Тавре ки аён аст, дар ин ҷадвал бити 58-уми матни ибтидоӣ дар ҷойи якум, бити 50-ум дар ҷойи дуюм ва ҳоказо навишта мешаванд.*

Баъд аз ин амал матритсаи (ҷадвали) охирон ба ду қисми баробар қисми чап L_0 ва рост R_0 тақсим карда мешавад. Дар ин ҷо L_0 ва R_0 шакли зеринро доранд:

$$L_0: \mathrm{M}_{58} \dots \mathrm{M}_8 ;$$

$$R_0: = \mathrm{M}_{57} \dots \mathrm{M}_7 ;$$

Пас аз ин тавассути формулаи (1) ба рамзгузорӣ оғоз мекунем.

Пеш аз оғози рамзгузорӣ қимати функсияи $f(R_{n-1}, K_n)$ -ро ҳисоб мекунем. Ҳисобкунии қимати функсияи f аз 4 қадами зерин иборат мебошад.

1) $E(R_{n-1})$;

2) $E(R_{n-1})\ xor\ \ K_n\ = B_1, B_2, \dots, B_8$ ($B_1, B_2, \dots, B_8$ ҳар яки онҳо 6 битӣ мебошанд*);*

3) $S_1(B_1), S_2(B_2), \dots, S_8(B_8)$;

4) $P(S_1(B_1), S_2(B_2), \dots, S_8(B_8))$;

Ҳар яке аз ин қадамҳоро дида мебароем.

1) $E(R_{n-1})$;

Матритсаи

32 01 02 03 04 05

04 05 06 07 08 09

08 09 10 11 12 13

12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 01

Ҷадвали 5. Матритсаи E коркарди охирини калид.

-ро татбиқ карда, қимати $E(R_{n-1})$-ҳоро ҳисоб мекунем. Ҳоло ба сифати намуна тарзи ҳисобкунии $E(R_0)$-ро дида мебароем, ки натиҷаи он шакли зеринро дорад:

$$E(R_0): \mathrm{M_7M_{57}M_{49}M_{41}M_{33}M_{25}}$$
$$\mathrm{M_{33}M_{25}M_{17}M_9M_1M_{59}}$$
$$\mathrm{M_1M_{59}M_{51}M_{43}M_{35}M_{27}}$$
$$\mathrm{M_{35}M_{27}M_{19}M_{11}M_3M_{61}}$$
$$\mathrm{M_3M_{61}M_{53}M_{45}M_{37}M_{29}}$$
$$\mathrm{M_{37}M_{29}M_{21}M_{13}M_5M_{63}}$$
$$\mathrm{M_5M_{63}M_{55}M_{47}M_{39}M_{31}}$$
$$\mathrm{M_{39}M_{31}M_{23}M_{15}M_7M_{57}}$$

2) $E(R_{n-1})$ xor K_n:

Дар ин қадам, бо истифода аз амали xor қимати $E(R_{n-1})$ xor K_n ҳисоб карда мешавад. Бигузор натиҷаи ин амал барои $E(R_0)$ ва K_1 шакли зеринро дошта бошад:

$E(R_0)\ xor\ K_1$: $b_1^1 b_2^1 b_3^1 b_4^1 b_5^1 b_6^1\ \ b_1^2 b_2^2 b_3^2 b_4^2 b_5^2 b_6^2\ \ b_1^3 b_2^3 b_3^3 b_4^3 b_5^3 b_6^3$
$b_1^4 b_2^4 b_3^4 b_4^4 b_5^4 b_6^4\ \ b_1^5 b_2^5 b_3^5 b_4^5 b_5^5 b_6^5\ \ b_1^6 b_2^6 b_3^6 b_4^6 b_5^6 b_6^6\ \ b_1^7 b_2^7 b_3^7 b_4^7 b_5^7 b_6^7$
$b_1^8 b_2^8 b_3^8 b_4^8 b_5^8 b_6^8$

Аз инҷо $B_i (i = 1 \ldots 8)$ – ҳо шакли шакли зеринро мегиранд:

$$B_1 = b_1^1 b_2^1 b_3^1 b_4^1 b_5^1 b_6^1$$
$$B_2 = b_1^2 b_2^2 b_3^2 b_4^2 b_5^2 b_6^2$$
$$B_3 = b_1^3 b_2^3 b_3^3 b_4^3 b_5^3 b_6^3$$
$$B_4 = b_1^4 b_2^4 b_3^4 b_4^4 b_5^4 b_6^4$$
$$B_5 = b_1^5 b_2^5 b_3^5 b_4^5 b_5^5 b_6^5$$
$$B_6 = b_1^6 b_2^6 b_3^6 b_4^6 b_5^6 b_6^6$$
$$B_7 = b_1^7 b_2^7 b_3^7 b_4^7 b_5^7 b_6^7$$
$$B_8 = b_1^8 b_2^8 b_3^8 b_4^8 b_5^8 b_6^8$$

3) $S_1(B_1), S_2(B_2),\ldots, S_8(B_8)$

Барои ҳисобкунии $S_1(B_1), S_2(B_2),\ldots,S_8(B_8)$ аз ҷадвали зерин истифода бурда мешавад.

		Рақами сутун 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
Р а қ	0	**14 04 13 01 02 15 11 08 03 10 06 12 05 09 0 07**	S_1
	1	**0 15 07 04 14 02 13 01 10 06 12 11 09 05 03 08**	
	2	**04 01 14 08 13 06 02 11 15 12 09 07 03 10 05 0**	
	3	**15 12 08 02 04 09 01 07 05 11 03 14 10 0 06 13**	
	0	**15 01 08 14 06 11 03 04 09 07 02 13 12 0 05 10**	
	1	**03 13 04 07 15 02 08 14 12 0 01 10 06 09 11 05**	S_2

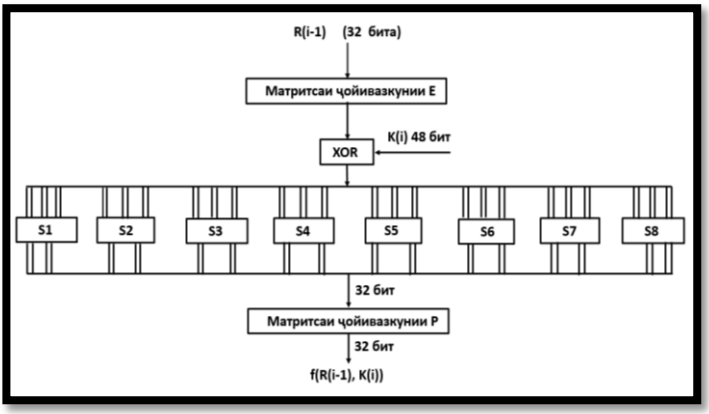
а	2	**0 14 07 11 10 04 13 01 05 08 12 06 09 03 02 15**	
	3	**13 08 10 01 03 15 04 02 11 06 07 12 0 05 14 09**	
м	0	**10 0 09 14 06 03 15 05 01 13 12 07 11 04 02 08**	S_3
	1	**13 07 0 09 03 04 06 10 02 08 05 14 12 11 15 01**	
и	2	**13 06 04 09 08 15 03 0 11 01 02 12 05 10 14 07**	
	3	**01 10 13 0 06 09 08 07 04 15 14 03 11 05 02 12**	
с	0	07 **13 14 03 0 06 09 10 01 02 08 05 11 12 04 15**	
	1	**13 08 11 05 06 15 0 03 04 07 02 12 01 10 14 09**	
а	2	**10 06 09 0 12 11 07 13 15 01 03 14 05 02 08 04**	S_4
т	3	**03 15 0 06 10 01 13 08 09 04 05 11 12 07 02 14**	
р	0	**02 12 04 01 07 10 11 06 08 05 03 15 13 0 14 09**	
	1	**14 11 02 12 04 07 13 01 05 0 15 10 03 09 08 06**	
	2	**04 02 01 11 10 13 07 08 15 09 12 05 06 03 0 14**	S_5
	3	**11 08 12 07 01 14 02 13 06 15 0 09 10 04 05 03**	
	0	**12 01 10 15 09 02 06 08 0 13 03 04 14 07 05 11**	
	1	**10 15 04 02 07 12 09 05 06 01 13 14 0 11 03 08**	
	2	**09 14 15 05 02 08 12 03 07 0 04 10 01 13 11 06**	S_6
	3	**04 03 02 12 09 05 15 10 11 14 01 07 06 0 08 13**	

	0	**04 11 02 14 15 0 08 13 03 12 09 07 05 10 06 01**	
	1	**13 0 11 07 04 09 01 10 14 03 05 12 02 15 08 06**	
	2	**01 04 11 13 12 03 07 14 10 15 06 08 0 05 09 02**	S_7
	3	**06 11 13 08 01 04 10 07 09 05 0 15 14 02 03 12**	
	0	**13 02 08 04 06 15 11 01 10 09 03 14 05 0 12 07**	
	1	**01 15 13 08 10 03 07 04 12 05 06 11 0 14 09 02**	
	2	**07 11 04 01 09 12 14 02 0 06 10 13 15 03 05 08**	S_8
	3	**02 01 14 07 04 10 08 13 15 12 09 0 03 05 06 11**	

Ҷадвали 6. Функсияи ҳосилшавии $S_1, S_2, \ldots, S_8$

Қайд. *Бигузор дар даромади функсияи матритсаи S_i блоки 6 битаи $B_1 = b_1^1 b_2^1 b_3^1 b_4^1 b_5^1 b_6^1$, дохил шавад. Бити дугонаи шумораи $b_1^1 b_6^1$ рақами сатр ва чор бити боқимонад $b_2^1 b_3^1 b_4^1 b_5^1$– рақами сутуни матритсаро нишон медиҳанд, яъне натиҷаи функсияи $S_i(B_i)$ элементи 4 битӣ мебошад, ки дар сатри $b_1^1 b_6^1$ (ба намуди даҳӣ) ва сутуни $b_2^1 b_3^1 b_4^1 b_5^1$ (ба намуди даҳӣ) ҷойгир аст.*

Шакли графикии функсияи $f(R_{i-1}, K_i)$ чунин аст:



Ҳамин тариқ, бо истифода аз калид 16 раундӣ (даврӣ) рамзгузорӣ иҷро карда мешавад. Баъди даври 16-ум матритсаи IP^{-1}, ки бо матритсаи IP баръакс мебошад, ба натиҷаи охирон татбиқ карда мешавад.

40	**08**	**48**	**16**	**56**	**24**	**64**	**32**
39	**07**	**47**	**15**	**55**	**23**	**63**	**31**
38	**06**	**46**	**14**	**54**	**22**	**62**	**30**
37	**05**	**45**	**13**	**53**	**21**	**61**	**29**
36	**04**	**44**	**12**	**52**	**20**	**60**	**28**
35	**03**	**43**	**11**	**51**	**19**	**59**	**27**
34	**02**	**42**	**10**	**50**	**18**	**58**	**26**
33	**01**	**41**	**09**	**49**	**17**	**57**	**25**

Ҷадвали 7. Матритсаи ҷойивазкунии баръакс IP^{-1}

Қайд. *Ҷойивазкунии матритсаи IP^{-1} ба ҷойивазкунии матритсаи IP монанд гузаронида мешавад.*

Мисол. Бигузор матни 64 битаи М, ки шакли дӯии он чунин аст, дода шуда бошад.

M = 00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111

Матритсаи IP-ро (ҷадвали 4) татбиқ карда, қимати IP(M)-ро ҳисоб мекунем, ки шакли зеринро мегирад.

IP(M): 11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010

Натиҷаи IP(M)-ро ба ду қисми баробар чап L_0 ва рост R_0 ҷудо мекунем:

L_0**: 11001100 00000000 11001100 11111111**

R_0**: 11110000 10101010 11110000 10101010**

Матритсаи Е-ро (ҷадвали 5) татбиқ карда, қимати $E(L_0)$ ҳисоб карда мешавад.

$\boldsymbol{E}(L_0)$: **011110 100001 010101 010101 011110 100001 010101 010101**

2) E(R_{n-1}**)** $\boldsymbol{xor}$ K_n**:**

Дар ин қадам, бо истифода аз амали xor қимати E(R_{n-1}) xor K_n-ро ҳисоб мекунем, ибтидо E(R_0) xor K_1 ҳисоб карда мешавад, ки K_1 ва E(R_0) шакли зеринро доранд:

K_1**: 00110 110000 001011 101111 111111 000111 000001 110010**

E(R_0): 011110 100001 010101 010101 011110 100001 010101 010101.

Аз инҷо

E(R_0) xor K_1: 011000 010001 011110 111010 100001 100110 010100 100111

Ҳамин тариқ

$$B_1 = 011000$$
$$B_2 = 010001$$
$$B_3 = 011110$$
$$B_4 = 111010$$
$$B_5 = 100001$$
$$B_6 = 100110$$
$$B_7 = 010100$$
$$B_8 = 100111$$

3) $S_1(B_1), S_2(B_2),\ldots, S_8(B_8)$

Барои ҳисобкунии $S_1(B_1), S_2(B_2),\ldots, S_8(B_8)$ аз ҷадвали 6 истифода бурда мешавад.

Бигзор B=″011011″ бошад. Ҷадвали 6-ро табиқ карда қимати $S_1(B)$-ро меёбем. Азбаски шакли даҳии бити аввал ва охири B_1 ба 1 (01_2) ва чор бити боқимонда 1101_2 ба 13 баробар аст, бинобар ин қимати матлуб дар бурриши сатри 1 ва сутуни 13 ҷойгир аст. Элементе ки дар сатр ва сутунҳои мазкури матритсаи S_1 мехобад-ин 5 мебошад.

Пас S_1 (011011)=0101 (шакли дӯии адади 5) мешавад. Ба ҳамин монанд, $S_i(B_i)$ $(i = 2…8)$ – ҳо низ ҳисоб карда мешаванд.

$S_1(B_1)$	$S_2(B_2)$	$S_3(B_3)$	$S_4(B_4)$	$S_5(B_5)$	$S_6(B_6)$	$S_7(B_7)$	$S_8(B_8)$
0101	**1100**	**1000**	**0010**	**1011**	**0101**	**1001**	**0111**

Барои муайян намудани мавқеи $S_i(B_i)$ метавон аз зербарномаи зерин, ки дар забони C++ навишта шудааст, истифода кард.

```
#include <iostream>
#include <cmath>
using namespace std;
int main(int argc, char** argv) {
 string S="011011";
 int n,c,r;
 n=S.length();
 c=2*((int)S[0]-48)+((int)S[n-1]-48);
 r=0;
 for (int i=1; i<n-1; i++){
   r+=pow(2,(n-2-i))*((int)S[i]-48);
 }
cout<<"satr:"<<r<<" sutun:"<<c;
 return 0;
}
```

4) $f(R_0, K_1) = P(S_1(B_1), S_2(B_2), \dots, S_8(B_8))$

Барои ҳисоб намудани қимати $P(S_1(B_1), S_2(B_2), \dots, S_8(B_8))$ барои ҳар як блок матритсаи Р татбиқ карда мешавад.

16	**07**	**20**	**21**
29	**12**	**28**	**17**
01	**15**	**23**	**26**
05	**18**	**31**	**10**
02	**08**	**24**	**14**
32	**27**	**03**	**09**
19	**13**	**30**	**06**
22	**11**	**04**	**25**

Ҷадвали 8. Матритсаи Р

Пас аз як давр (бо татбиқи ҷадвали 8) натиҷаи зерин ба даст меояд:

$\boldsymbol{f(R_0, K_1)}$**: 0010 0011 0100 1010 1010 1001 1011 1011**

Акнун қимати $R_1 = L_0 \ xor \ f(R_0, K_1)$ -ро ҳисоб мекунем, ки чунин шаклро соҳиб мешавад:

$R_1 = L_0 \ xor \ f(R_0, K_1)$**: 1110 1111 0100 1010 0110 0101 0100 0100**

Ҳамин тариқ пас аз 16 давр чунин натиҷа ба даст меояд:

$\boldsymbol{R_1 = L_0}$**: 1111 0000 1010 1010 1111 0000 1010 1010**

$\boldsymbol{R_1}$**: 1110 1111 0100 1010 0110 0101 0100 0100**

⋮

$\boldsymbol{L_{16}}$**: 0100 0011 0100 0010 0011 0010 0011 0100**

$\boldsymbol{R_{16}}$**: 0000 1010 0100 1100 1101 1001 1001 0101**

Баъд аз 16 давр ҷойҳои $\boldsymbol{L_{16}}$ ва $\boldsymbol{R_{16}}$–ро бо ҳамдигар иваз карда чунин натиҷаро ба даст меорем:

$\boldsymbol{L_{16}R_{16}}$**:00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100**

Дар охир қимати $IP^{-1}\,(R_{16}, L_{16})$-ро ҳисоб мекунем, яъне матритсаи IP^{-1} (ҷадвали 7)-ро барои $R_{16}\,L_{16}$ татбиқ карда чунин натиҷаро ба даст меорем:

$\boldsymbol{IP^{-1}(R_{16}, L_{16})}$**: 1000 0101 1110 1000 0001 0011 0101 0100 0000 1111 0000 1010 1011 0100 0000 0101**

Ҳамин тариқ матни додашуда рамзгузорӣ карда мешавад, агар қимати $IP^{-1}\,(R_{16}, L_{16})$-ро аз дӯи ба даҳӣ гардонем матни рамзгузошташуда ҳосил мегардад.

Рамзкушоӣ бошад, ба монанди рамзгузорӣ буда, фақат зеркалидҳо ба тартибӣ баръакс истифода бурда мешаванд, яъне $K_{16}, K_{15}, K_{14}, \dots, K_1$

Просесси рамзкушоӣ бошад, тавасути формулаи (2) иҷро карда мешавад.

Дар 16-ум давр (итерасия) пайдарпаии L_0 ва R_0 ҳосил мегарданд. Онҳоро бо ҳамдигар пайваст карда, пайдарпаии 64 бита ҳосил мекунем.

Баъдан мавқеи пайдарпаии ин битҳоро бо ёрии матритсаи IP иваз мекунем. Натиҷаи чунин ҷойивазкунӣ пайдарпаии 64 бита мебошад.

Ба ҳамин минвол рамзи DES истифода бурда мешавад.

3) Алгоритми AES ва таърихи пайдоиши он

Соли 1998 NIST (National Institute of Standards and Technology) оиди сохтани алгоритми рамзгузории симметрӣ конкурс эълон кард. Алгоритми сохташуда номи AES (Advanced Encryption Standard)-ро соҳиб шуд. Дар нақша гирифта шуда буд, ки алгоритм ҳамчун стандарди ИМА дар ивази стандарди DES (Digital Encryption Standard), ки соли 1997 стандарди Амрико қабул шуда буд, истифода шавад. Зарурати қабули алгоритми нав дар кутоҳии калиди DES (56 бит) мебошад, ки бо усули азназаргузаронии ростаи калид бо содаги DES рахна карда мешуд. Илова бар ин, архитектураи DES барои татбиқи аппаратӣ нигаронида шуда буд, аммо татбиқи платформавии он бо назардошти маҳдудияти манбаҳо на он қадар мувофиқ буд. Модификатсияи TripleDES дорои калиди ба қадри кифоя дароз буда, суръати корияш сустар (оҳистатар) буд.

Дуюми январи соли 1997 NIST қасди интихоби ҷойгузини DES-ро эълон кард. 12-уми сентябри соли 1997 конкурс эълон карда шуд. Дар ин конкурс дилхоҳ ташкилот ва гурӯҳҳои тадқиқотӣ метавонистанд алгоритми худро пешкаш намоянд. NIST ҳамаи

иттилотҳои лозимиро оиди санҷиши (тестирования) номзадҳо дар нақши AES мунташир карда, аз муаллифон принсипҳои базавии (истифодаи доимиҳо, ҷадвалҳо барои ивазкунӣ(S-box) ва ғайра) сохтани алгоритмро талаб кард. Талаботи асоси аз номзадҳо чунин буд:

1) рамзи блокӣ (блочный шифр) будани он;
2) дарозии блок ба 128 бит баробар будан;
3) истифодаи калидҳои дарозашон ба 128, 192 ва 256 бит баробар буда.

Иловатан аз номзадҳо талаб карда шуда буд:

1) истифодаи амалҳое, ки ба содагӣ пиёдасоии (амалисозии) апаратӣ (дар микрочипҳо), ва барномави (дар КФ ва серверҳо)-и онҳо мавҷуд бошад;
2) ба протсессҳои 32 бита нигаронидани он;
3) бе зарурат душвор нагардонидани сохтори рамз, барои он ки ҳар як истифодабаранда тавонад мустақилона ва новобаста алгоритмро таҳлили криптографӣ гузаронида, боварӣ ҳосил кунад, дар он ягон имконияти ғайриҳуҷҷатӣ гузошта нашудааст.

Илова бар ин, аз алгоритме ки ба сифати номзади стандард мехост баромад кунад, талаб карда шуд, ки ба тамоми ҷаҳон мунташир карда шавад ва барои истифодаи патент ягон хел маблағ талаб накунад.

Алгоритми бояд пеш аз ҳама дараҷаи баланди ҳифзро пешниҳод карда, дорои сохтори сода ва маҳсулнокии бештар бошад. Аз нуқтаи назари архитектураи дохилӣ бояд чунон боваринок бошад, ки ба зидди ҳар гуна ҳуҷумҳо тоқат карда тавонад.

Дар байни ҳамаи алгоритмҳо конкурс гузаронида шуда, дуюми октябри соли 2000 ғолиби конкурси AES алгоритми Rijndael ([rɛinda:l] (Рэндал) эълон гардад. Сар карда аз ҳамон вақт ба стандартизатсия кардани он шурӯъ карданд. Бистуҳаштуми феврали соли 2001 лоиҳа (проект) чоп карда шуда, 26-уми ноябри соли 2001 AES ҳамчун стандартӣ FIPS 197 қабул гардид.


Joan Daemen

Таҳиякунандагони алгоритми Rijndael криптографҳои белгиявӣ Ҷоан Дамен[1] ва Винсент Реймен[2] ба ҳисоб мераванд.

AES айнан Rijndael намебошад, чунки алгоритми аслии Rijndael калид ва блоки дорои фосилаи калонро пуштибонӣ мекард, аммо дар AES дарозии калид қайдкардашуда буда ба 128 бит баробар мебошад. Дар Rijndael метавон калидҳои дарози-ашон аз 128 то 256 бит баробарро бо қадами 32 бит истифода кард. AES блоки додаҳои дарозиашон ба 16 байт баробарро истифода мекунад, аммо дар Rijndael истифодабаранда метавонад худаш дарозии калидро интихоб кунад.


Vincent Rijmen

Rijndael – алгоритми муҷаз (компактный) бо сохтори математикии сода буда, дорои устуворӣ хуб ба муқобили ҳар гуна ҳамла дар вақти истифодабарӣ

[1] https://en.wikipedia.org/wiki/Joan_Daemen
[2] https://en.wikipedia.org/wiki/Vincent_Rijmen

мебошад. Умуман AES –ро метавон ҳамчун Rijndael бо калиди дарозиаш ба 128 бит ва блоки дарозиаш ба 16 байт баробар дар назар гирифт.

Дар ин боб бе назардошти асосҳои математикиаш алгоритми AES-ро дида мебароем.

Ишораҳои дар алгоритми AES истифодашаванда

Пеш аз мавриди баҳс қарор додани алгоритми AES ибтидо ишораҳои асосии дар он истифодашавандаро дида мебароем

Ишора	Маъно ва мафҳум
AddRoundKey()	Табдилдиҳи дар рамзгузорӣ ва рамзкушоӣ, дар он калиди раундӣ тавассути амали XOR ба матритсаи state ҷамъ карда мешавад.
InvMixColumns()	Инверсияи MixColumns буда, ҳамчун табдилдиҳи дар рамзкушоӣ истифода бурда мешавад.
InvShiftRows()	Инверсияи ShiftRows буда, ҳамчун табдилдиҳи дар рамзкушоӣ истифода бурда мешавад.
InvSubBytes()	Инверсияи SubBytes буда, ҳамчун табдилдиҳи дар рамзкушоӣ истифода бурда мешавад.
K	Калиди рамгузорӣ — массиви иборат аз 128 бит ё 16 байт.
MixColumns()	Табдилдиҳи дар ҷараёни рамзгузорӣ буда, барои ба даст овардани сутуни нав, ҳамаи сутунҳои ҷадвали *state* гирифта додаҳои онҳоро кучиш мекунонад
Rcon()	Массиви калимаҳои доимии раундӣ.

RotWord()	Функсияи дар амали калиди васеъшуда истифодашаванда буда, калимаи 4 байтарои гирифта онро ҷойгардонӣ мекунад.
ShiftRows()	Табдилдиҳӣ дар ҷараёни рамзгузорӣ буда, се сутуни охирини матритсаи state –ро бо мавқеъҳои гуногун даврӣ мекучонад.
SubBytes()	Табдилдиҳӣ дар ҷараёни рамзгузорӣ буда, бо истифода аз ҷадвали ивазкунӣ (*S*-box) байтҳои матритсаи state иваз мекунад.
N_k	Дарозии калид дар AES - 4 калима.
N_b	Дарозии блок дар калима барои AES - 4 калима.
N_r	Миқдори рундҳо дар рамзгузорӣ – 10.
XOR	Амали даврии («ё») кор бо битҳо.
⊗	Амали даврии («ё») кор бо битҳо.
•	Амали зарб дар майдони охирнок.

Рамзгузорӣ тавассути AES

Барои рамзгузорӣ кардан, ибтидо калид лозим мешавад. Дар алгоритми AES дарозии калид ба 128 бит баробар буда, одатан ҳамчун матрисаи 4×4 байт дода мешавад.

Input*Key*

k_0	k_4	k_0	k_0
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

Додаҳои вурудӣ барои амали рамзгузорӣ массиви 16 байтаи $in_0, in_1, \dots, in_{15}$ мебошад. Дар ибтидои рамзгузорӣ додаҳои вурудӣ ба ба блокҳои андозаашон ба 16 байт ё 128 бит баробар тақсим карда мешаванд. Агар андозаи умумии итилоотӣ вурудӣ ба 16 каратӣ набошад, онгоҳ дар охири он байтҳои иловагӣ (то замоне, ки андозаи пайғоми ҳосилшуда ба карати 16 нашавад) илова карда мешаванд. Сипас байтҳои ин массив пайдарпай ба сутунҳои матритсаи *InputBlock* (аз боло ба поён) навишта мешаванд. Дар дохили алгоритм бо байтҳои матритсаи ҳолат (State) амали ҷамъ ичро карда мешавад. Қиматҳои охирини матритсаи ҳолатро OutputBlock меноманд, ки баромади алгоритм ба ҳисоб меравад. Ба ҳамин монанд элементҳои матрисаи калид InputKey (K) $k_0, k_1, \dots, k_{15}$ дода мешаванд. Андозаи ҳамаи матритсаҳо 4×4 мебошанд.
Шакли схематикии додаҳо чунин аст:

in_0	in_4	in_0	in_0
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

→

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

=

out_0	out_4	out_0	out_0
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

Байтҳои вурудӣ InputBlock — Матритсаи *state* — Байтҳои хуруҷӣ OutputBlock

Input*Key*

k_0	k_4	k_0	k_0
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

Чор байти дар ҳар як сутуни матритсаи ҳолат ё калид-ро метавон ҳамчун як калимаи 32 битӣ дар назар гирифт. Аз ин ҷост, ки матрисаи ҳолат –ин чор калимаи w_0, w_1, w_2, w_3 мебошад, дар инҷо

$$w_0 = s_{0,0}s_{1,0}s_{2,0}s_{3,0};$$
$$w_1 = s_{0,1}s_{1,1}s_{2,1}s_{3,1};$$
$$w_2 = s_{0,2}s_{1,2}s_{2,2}s_{3,2};$$
$$w_3 = s_{0,3}s_{1,3}s_{2,3}s_{3,3};$$

аст.

Матритсаеро ки дар вурудӣ ҳар як раунд иштирок мекунад InputState ва матритсаеро, ки дар хуруҷи ҳар як раунд иштирок мекунад OutputState меноманд. Маълум аст, ки дар вуруди раунди якум $InputState = InputBlock$ буда, дар хуруҷи раунди охирон $OutputState = OutputBlock$ мебошад.

Мисол. Матни зеринро ки ба намуди ададӣ (даҳӣ) дода шудааст ба шакли блоки $InputBlock$ менависем:

$(21\ 14\ 15\ 00\ 05\ 17\ 11\ 21\ 22\ 30\ 09\ 00\ 05\ 00\ 27\ 11)_{10} =$
$= (15\ 0E\ 0F\ 00\ 05\ 11\ 0B\ 15\ 16\ 1E\ 09\ 00\ 05\ 00\ 1B\ 0B)_{16};$

$$InputBlock = \begin{pmatrix} 15 & 05 & 16 & 05 \\ 0E & 11 & 1E & 00 \\ 0F & 0B & 09 & 1B \\ 00 & 15 & 00 & 0B \end{pmatrix}.$$

Амали рамзгузории ҳар як блок аз муҳтавои блоки дигар новобаста гузаронида мешавад. Бо охиррасии рамзгузории блок - матритса бо додаҳои қисми дигар пур карда шуда, ҷараён аз нав такрор карда меёбад. Бо назардошти новобаста будани рамзгузории як блок аз блоки дигар ҷараёни рамзгузорӣ хуб ба ҷудокунӣ меафтад.

Ҳар як блок дар якчанд қадам-раунд рамзгузорӣ карда мешавад. Схемаи крипто-табдилдиҳиро метавон ба сурати зерин навишт.

1. Калиди васеъшуда-*KeyExpansion*.
2. Ибтидои амали — *AddRoundKey* — сумаронӣ бо асоси калид.
3. Иҷроиши 9 раунд иборат аз 4 қадам ҳар кадомашон.
3.1. *SubBytes* — иваз кардани байтҳои *state* аз рӯӣ ҷадвали ивазкунӣ.
3.2. *ShiftRows* — лағжиши даврии сатрҳои *state*.
3.3. *MixColumns* — ҷойгардонии сутунҳои *state*.
3.4. *AddRoundKey* — суммирони бо калиди раундӣ.
4. Иҷроиши раунди ҷамъбасти 10-ум.
4.1. *SubBytes* — ивазкунии байтҳо *state* аз рӯи ҷадвали ивазкунӣ.
4.2. *ShiftRows* — лағжиши даврии сатрҳои *state*.
4.3. *AddRoundKey* — суммирони бо калиди раундӣ.

Ҳоло ҳар яке аз ин қадамҳоро муфассал дида мебароем.

Табдилдиҳии *SubBytes*

Табдилдиҳии *SubBytes* – ин ивазкунии байтии ғайрихатӣ буда, барои ҳар як байти state бо истифода аз ҷадвали ҷойивазкунии *S-box* гузаронида мешавад.

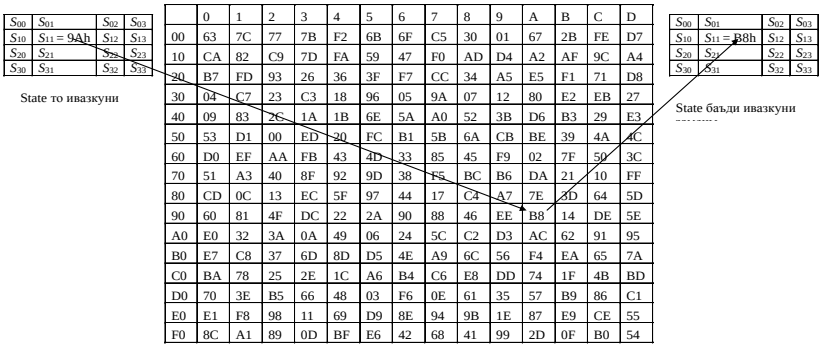
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	Ed	20	Fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	Fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	Bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Ҷадвали ивазкунии байтҳо *S-box* дар рамзи AES

Мақсади татбиқи ҷадвали ивазкунӣ — ин душвор гардонидани криптоанализи хаттӣ ва дифференсиалӣ мебошад. Дар алгоритми AES ҷадвали ивазкунӣ қайдкардашуда мебошад. Дар ҷадвали *S-box* ададҳо ба намуди системаи ҳисоби шонздаҳӣ навишта шудаанд. Дар ин система қимати дилхоҳ байт ба сурати на зиёда аз ду разрияди шонздаҳӣ тасвир карда мешавад.

Амали ивазкунии байти Z-ро аз рӯй ҷадвали *S*-box чунин иҷро кардан мумкин аст: байти z ба сурати системаи ҳисоби шонздаҳӣ табдил дода мешавад, масалан

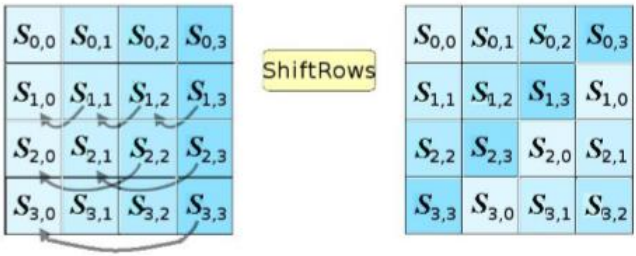
хy*h*. Дар инҷо *x* — разряди калонӣ ва *y* — разряди хурдӣ аст. Агар разряди калонӣ мавҷуд набошад, онгоҳ он ба сифр иваз карда мешавад. Дар ҷадвали *s-box* қимати катакчаи дар сатри *x* ва сутуни y-хобида интихоб карда мешавад. Қимати z', ки дар сатри x-ум ва сутуни y-уми ҷадвали s-box мехобад ҳамчун ивази z истифода бурда мешавад. Масалан, агар z = 9ah бошад, онгоҳ натиҷаи ивази ин байт, байтест, ки дар сатри 9-ум ва сутуни A-юм мехобад, яъне $Z' = SubBytes(9ah) = \{B8h\}$.



Қайд. Ҷадвали *S-box-ро* шарт нест, ки ба тартиби дар тавзеҳи AES оварда шуда, истифода кард, балки онро метавон ҳамчун массиви якченакае, ки индекси он қимати байт ва муҳтавояш қимати мувофиқи S-box аст, истифода кард. Масалан, S-arr = {63h, 7Ch, 77h, …}. Ҷараёни ивазкунӣ аз рӯй ин ҷадвал ба шакли $Z' = S\text{-}arr[Z]$ оварда мешавад, ки дар муқоиса тезтар мебошад. Дар ин вақт андозаи ҳофиза тағйир намеёбад.

Табдилдиҳии *ShiftRows*

Дар табдилдиҳии *ShiftRows* байтҳои се сатри охирони ҷадвали state мувофиқан ба миқдори 1,2 ва 3 байт даврӣ ба тарафи рост кучонида мешаванд.



Табдилдиҳии *MixColumns*

Дар табдилдиҳии MixColumns — сутунҳои матритсаи state ҳамчун бисёраъзогӣ дар майдони $F(2^8)$ дар назар гирифта шуда, аз рӯи модули $x^4 + 1$ ба бисёраъзогии доимии зерин зарб карда мешаванд:

$$a(x) = 3x^3 + 1x^2 + 1x^2 + 2 \qquad (2)$$

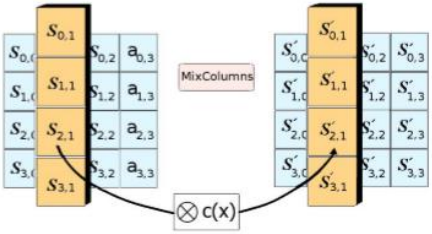
Ҷараёни зарби бисёраъзогиҳо бо зарбти матритсавии зерин баробарқувва аст:

$$\begin{bmatrix} S'_{0c} \\ S'_{1c} \\ S'_{2c} \\ S'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix},$$

дар инҷо c ($0 \le c \le 3$) – рақами сутунҳои матритсаи state-ро ифода мекунад. Дар натиҷаи чунин зарбкунӣ байтҳои сутуни c {S_{0c}, S_{1c}, S_{2c}, S_{3c}} мувофиқан ба байтҳои зерин иваз карда мешаванд.

$$S'_{0c} = (2 \bullet S_{0c}) \oplus (3 \bullet S_{1c}) \oplus S_{2c} \oplus S_{3c};$$
$$S'_{1c} = S_{0c} \oplus (2 \bullet S_{1c}) \oplus (3 \bullet S_{2c}) \oplus S_{3c}; \quad (2)$$
$$S'_{2c} = S_{0c} \oplus S_{1c} \oplus (2 \bullet S_{2c}) \oplus (3 \bullet S_{3c});$$
$$S'_{3c} = (3 \bullet S_{0c}) \oplus S_{1c} \oplus S_{2c} \oplus (2 \bullet S_{3c}).$$

Табдилдиҳии (2) барои ҳар як сутуни матритсаи *state* татбиқ карда мешавад.



Табдилдиҳии *AddRoundKey*

Дар табдилдиҳии *AddRoundKey*, калиди раундӣ *RK* тавассути амали XOR бо матритсаи state ҷамъ карда мешавад. Ҳар як калиди раундӣ аз 16 байти калиди васеъшуда иборат мебошад. Байтҳои калиди раундӣ дар матритсаи 4×4, монанди *state* навишта мешаванд. Ҳар як байти калиди раундӣ бо байти мувофиқи state ҷамъ карда мешавад.

AddRoundKey

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

State то суммирони

$\oplus$

K_{00}	K_{01}	K_{02}	K_{03}
K_{10}	K_{11}	K_{12}	K_{13}
K_{20}	K_{21}	K_{22}	K_{23}
K_{30}	K_{31}	K_{32}	K_{33}

Калиди раунди

$\rightarrow$

S'_{00}	S'_{01}	S'_{02}	S'_{03}
S'_{10}	S'_{11}	S'_{12}	S'_{13}
S'_{20}	S'_{21}	S'_{22}	S'_{23}
S'_{30}	S'_{31}	S'_{32}	S'_{33}

State баъди суммирони

Калиди васеъшуда KeyExpansion

Алгоритми AES калиди рамзгузорӣ *K*-ро гирифта, барои сохтани калидҳои раундӣ амали васеъкунии калидро иҷро мекунад. Калиди васеъшудаи *W* дорои 4×(10+1) калима мебошад — 4 калима аз калиди ибтидоӣ ва чортогӣ калима дар ҳар як раунд (10 раунд). Калиди васеъшудаи *W, ки* аз калимаҳо (калимаҳои чор байтӣ) таркиб ёфтааст, тавасути w_i ишора карда мешаванд, дар инҷо i аз фосилаи [0..44] муайян карда мешавад. Дарозии пурраи КВ ба 1048 бит баробар мебошад, яъне 128 битӣ дар ҳар як раунд.

Дар ҷараёни васеъкунии калид аз массиви доимии *Rcon* истифода бурда мешавад. Элементҳои массиви Rcon сар карда аз 1 то 256+3 рақамгузорӣ карда мешаванд. Қиматҳои матритсаи мазкурро аз рӯи қоидаи рекурсивии зерин муайян кардан мумкин аст:

$$\mathrm{Rcon}_1 = 1;$$

$$\mathrm{Rcon}_k = 2 \cdot \mathrm{Rcon}_{k-1} = 2^{k-1}, \text{для k} = 2, 3, \ldots 255;$$

$$\mathrm{Rcon}_k = 0, \text{барои k} = 256, 257, 258;$$

Калиди васеъшударо метавон тавассути пайдарпайии амалҳои зерин навишт

Чор калимаи калиди рамзгузорӣ *K* ба 4 калимаи нахустини КВ нусхабардорӣ карда мешаванд *W*: $w_i = k_i$ барои $i = 0, 1, 2, 3$.

Калимаҳои боқимондаи калид *W* барои $i = 4, 5, \ldots 44$ чунин таҳия карда мешаванд:

агар *i* бо 4 каратӣ бошад, онгоҳ

$w_i = SubBytes(RotByte(w_{i-1})) \oplus Rcon(i/4)$ мешавад;

агар i бо 4 каратӣ набошад, онгоҳ $w_i = w_{i-4} \oplus w_{i-1}$ мешавад.

Функсияи RotByte чор байти матни ибтидоӣ $\{a_0, a_1, a_2, a_3\}$ –ро тавассути амали даврии ҷойгардонӣ ба шакли $\{a_3, a_2, a_1, a_0\}$ бармегардонад. Функсияи *SubBytes* барои ҳар яке аз чор байти калимаи ивазкунӣ тавассути *S*-box татбиқ карда мешавад.

Ба намуди псевдокод алгоритми ҳисобкунии Калиди васеъшуда шакли зеринро дорад:

```
KeyExpansion(byte key[4 * Nk], word w[Nb * (Nr+1)], Nk)
begin
   word temp
   i = 0;
   while(i < Nk)
      w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
      i = i + 1
   end while
   i = Nk
   while(i < Nb * (Nr+1))
      temp = w[i - 1]
      if (i mod Nk = 0)
         temp = SubWord(RotWord(temp)) xor Rcon[i / Nk]
      else if (Nk > 6 and i mod Nk = 4)
         temp = SubWord(temp)
      end if
      w[i] = w[i - Nk] xor temp
      i = i + 1
   end while
```

end

Дар инҷо Nb миқдори калимаҳо дар ҳар раунд ва Nr миқдори раундҳо мебошад.

Калидҳои ҷадвалии AES

Калидҳои раундӣ аз калиди рамзгузорӣ K тавассути амали KeyExpansion сохта мешаванд.

Ҳар як калиди раундӣ дорои дарозии 128 бит (ё 4 калимаи 4 байтии $w_i, w_{i+1}, w_{i+2}, w_{i+3}$, ки дарозиии ҳамаашон ба 128 бит *(10 рунд+1)=1024 (ё 44 калимаи 4 байтӣ $w_0, w_2, \dots, w_{42}, w_{43}$) мебошад. Чор калимаи аввала w_0, w_1, w_2, w_3, аз калиди ибтидоӣ, ташкил карда шуда, 40 калимаи боқимонда 4-тогӣ аз ҳар як калиди раундӣ сохта мешаванд. Интихоби калима хело сода мебошад: чор калимаи нахустин (онҳо бо калиди рамз мувофиқат мекунанд) калиди рақами сифрум (0) буда, чор калимаи минбаъда w_4, w_5, w_6, w_7 –калиди раундӣ барои раунди пурраи якум ва ғайра ба ҳисоб меравад.

Калимаҳои нав $w_{i+4}, w_{i+5}, w_{i+6}, w_{i+7}$ калиди раундии минбаъда аз калимаҳои $w_i, w_{i+1}, w_{i+2}, w_{i+3}$ (калиди қаблӣ) дар асоси формулаҳои зерин сохта мешаванд:

$$w_{i+5} = w_{i+4} \oplus w_{i+1};$$
$$w_{i+6} = w_{i+5} \oplus w_{i+2};$$
$$w_{i+7} = w_{i+6} \oplus w_{i+3};$$

Калимаи нахустини w_{i+4} дар ҳар калиди раундӣ аз рӯӣ қоидаи зерин тағйир дода мешаванд.

$$w_{i+4} = w_i \oplus g(w_{i+3});$$

Дар инҷо функсияи g аз рӯй се қоидаи зерин амал мекунад:

Кӯчиши даврии калимаи 4 байта ба андозаи як байт ба тарафи чап (амали RotWord).

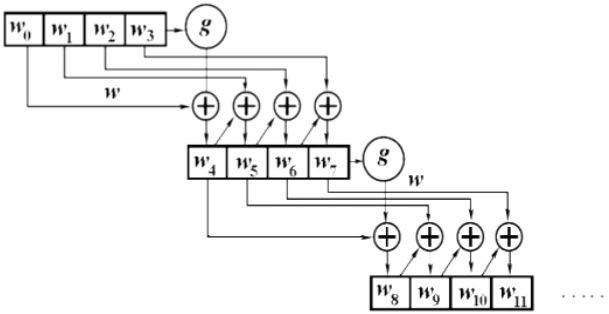
Мувофиқан аз рӯй ҷадвали SubBytes иваз кардани ҳар як байти калимае, ки аз қадами якум ҳосил шудааст (амали SubWord).

Аз рӯй модули 2 ҷамъ кардани байтҳои дар қадами 2 ҳосилшуда, бо доимии раундӣ $R_{con}[i] = (RC[i], 0,0,0)$ ки барои ҳар як калиди K_i ихтисорнашаванда ва ягона мебошад. Се байти тарафи рости ин доимӣ сифр буда, байти тарафи чапи ғайринулӣ аз рӯй қоидаи маъмули рекурсивӣ

$RC[1] = 1, RC[i] = 2 \cdot RC[i-1]$ $(i = 1,2, \dots ,10)$ иваз карда мешаванд.

Мақсади суммиронӣ бо доимии раундӣ-вайрон кардани дилхоҳ симметрия, ки дар қадамҳои гуногуни тобдиҳии (разворачивание) калид ба амал омада, сабаби суст шудани калид ҳамчун алгоритми DES мегардад.

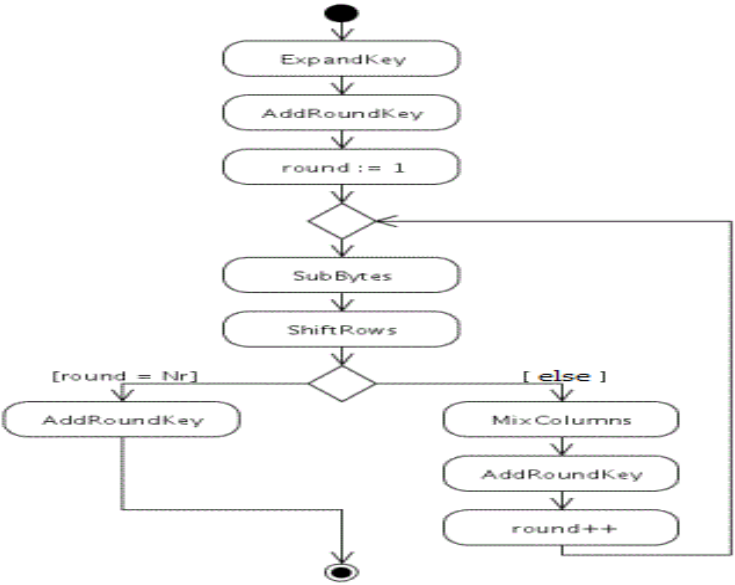
Дар расми зерин кори алгоритми калиди васеъшуда оварда шудааст:



Мисол. Бигзор калиди рамзгузорӣ OF 15 71 C9 47 D9 E8 59 0C B7 AD DF AF 7F 67 98 бошад. Онгоҳ қиматҳои калиди раундӣ ва фуксияи $g(w)$ чунин шаклро мегиранд.

Калидҳои раундӣ	Функсияи $g(w)$
$w_0 = 0F\ 15\ 71\ C9$ $w_1 = 47\ D9\ E8\ 59$ $w_2 = 0C\ B7\ AD\ DF$ $w_3 = AF\ 7F\ 67\ 98$	$RotWord(w_3) = 7F\ 67\ 98\ AF = x_1$ $RotWord(w_3) = D2\ 85\ 46\ 79 = y_1$ $R_{con}[1] = 01\ 00\ 00\ 00$ $y_1 + R_{con}[1] = D3\ 85\ 46\ 79 = z_1$
$w_4 = w_0 + z_1 = DC\ 90\ 37\ B0$ $w_5 = w_4 + w_1 = 9B\ 49\ DF\ E9$ $w_6 = w_5 + w_2 = 97\ FE\ 72\ 3F$ $w_7 = w_6 + w_3 = 38\ 81\ 15\ A7$	$RotWord(w_7) = 81\ 15\ A7\ 38 = x_2$ $SubWord(x_1) = 0C\ 59\ 5C\ 07 = y_2$ $R_{con}[2] = 02\ 00\ 00\ 00$ $y_2 + R_{con}[2] = 0E\ 59\ 5C\ 07 = z_2$
$w_8 = w_4 + z_2 = D2\ C9\ 6B\ B7$ $w_9 = w_8 + w_5 = 49\ 80\ B4\ 5E$ $w_{10} = w_9 + w_6 = DE\ 7E\ C6\ 61$ $w_{11} = w_{10} + w_7 = E6\ FF\ D3\ C6$	$RotWord(w_{11}) = FF\ D3\ C6\ E6 = x_3$ $SubWord(x_2) = 16\ 66\ B4\ 8E = y_3$ $R_{con}[3] = 04\ 00\ 00\ 00$ $y_3 + R_{con}[3] = 12\ 66\ B4\ 8E = z_3$

Ба намуди блок-схема амалкарди алгоритми AES чунин аст:



Рамзкушоӣ дар AES

Ҳамаи табдилдиҳиҳои рамзгузорӣ якқимата мебошанд, бинобар ин, ҳар яки онҳо дорои табдилдиҳии баръакс буда, (аз инҷо) онҳоро метавон инвертироват карда, ба тартиби баръакс барои амали рамзкушоии AES истифода кард.

Схемаи крипто-табдилдиҳиро метавон ба сурати зерин навишт:

1. Калиди васеъшудаи *KeyExpansion*.

3. Ичроиши 9 раунд, ки ҳар кадомаш дорои 4 қадам мебошанд.

3.1. *AddRoundKey* — суммиронӣ бо калиди раундӣ.

3.2. *InvMixColumns* — ҷойгардонии баръакси сутунҳои *state*.

3.3. *InvShiftRows* — лағжиши даврии баръакси сатрҳои *state*.

3.4. *InvSubBytes* — ивазкунии байтҳои *state* аз рӯӣ ҷадвали ивазкунӣ.
4. Раунди ҷамъбастӣ, раунди 10
4.1. *AddRoundKey* — суммиронӣ бо калиди раундӣ.
4.2. *InvShiftRows* — ҷойивазкунии баръакси сутунҳои *state*.
4.3. *InvSubBytes* — ивазкунии байтҳои *state* аз рӯӣ ҷадвали ивазкунӣ.

Ҳоло ҳар яке аз ин табдилдиҳиҳоро шарҳу тавзеҳ медиҳем:

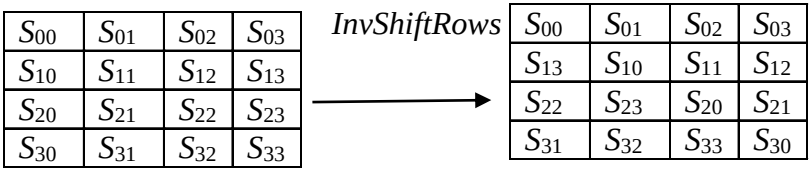
Табдилдиҳии *InvMixColumns*

Табдилдиҳии *InvMixColumns* барои табдилиҳии *MixColumns* баръакс мебошад. Дар табдилдиҳии *InvMixColumns*, сутунҳои матритсаи *state* ҳамчун бисёраъзогӣ дар майдони $F(2^8)$ дида баромада шуда, аз рӯи модули $x^4 + 1$ бо бисёраъзогии $d(x) = a^{-1}(x)$, дар майдони $F(2^8)$ зарб карда мешаванд:

$$d(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}. (4)$$

Табдилдиҳии *InvShiftRows*

Табдилдиҳии *InvShiftRows* баръакси табдилдиҳии *ShiftRows* мебошад. Байтҳои се сатри охирони массиви state ба таври даврӣ ба тарафи рост кӯчонида мешаванд. Сатри 1 (рақамгузорӣ аз 0 оғоз шудааст) –ба 1 байт, сатри 2 – ба 2 байт, сатри 3 – ба 3 байт кӯчонида мешавад.



State то лағжиш

State баъди лағжиш

Табдилдиҳии *InvSubBytes*

Табдилдиҳии *InvSubBytes*- баръакси амали SubBytes буда, байтҳои матритсаи *State*-ро тавассути ҷадвали ивазкунӣ (ки *InvS-box* ном дорад) ба қиматҳои нав иваз мекунад. Ҷадвали *InvS-box* дар поён оварда шудааст.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DE	6E
A	47	E1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	D	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7E	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	CB	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Табдилиҳии баръакси *AddRoundKey*

Табдилдиҳии *AddRoundKey*, барои худаш баръакс мебошад, чунки дар он амали *XOR* истифода мешавад.

Саволҳо барои мустаҳкамкунӣ

1. Рамзи Фейстел кай ва аз тарафи кӣ сохта шудааст?
2. Дар рамзи Фейстел кадом функсияҳо истифода бурда мешаванд?
3. S-блок чист ва чӣ тавр ҳисоб карда мешавад?
4. Алгоритми DES кай ва бо чи мақсад сохта шудааст?
5. Дар алгоритми DES чанд матритсаи стандартӣ истифода бурда мешавад?
6. Алгоритми DES дорои чанд давр мебошад?
7. Матн ва калиди ибтидоии методи DES чӣ тавр дода мешаванд?
8. Алгоритми AES дар куҷо ва аз тарафи кӣ сохта шудааст?
9. Маънои калимаи AES чист?
10. Дар алгоритми AES аз кадом табдилдиҳиҳо истифода карда мешавад?
11. Амали рамзкушоӣ чӣ тавр иҷро карда мешавад?
12. Калиди васеъшуда чи гуна калид аст?

Боби 11. Истифодаи хатҳои каҷи эллиптикӣ дар криптография

1. Каме аз таърих

Соли 1985 математикони машҳури амрикоӣ Нил Коблитс (англ. Koblitz Neal) [1] ва Виктор Миллер(англ. Victor Saul Miller)[2] новобаста аз ҳамдигар истифодаи хосияти алгебравии хатҳои каҷро дар криптография пешниҳод карданд. Сар карда аз ҳамон вақт дар криптография истифода-барии яке аз соҳаҳои назарияи ададҳо ва геометрияи алгебравӣ – назарияи хатҳои каҷи эллиптикӣ дар майдонҳои охирнок хело зиёд ба назар мерасад. Сабаби асоси дар он аст, ки хатҳои аҷи эллиптикӣ дар майдонҳои охирнок сарчашмаи тамомнаша-вандаи гурӯҳи абелиро ифода мекунанд. Гарчанде, ки онҳо калонанд, аммо барои истифода қулай ва шаклу сохти бою мураккаб доранд. Хатҳои каҷи эллиптикӣ дар бисёр ҷиҳатҳо аналоги ягонаи гурӯҳҳои мултипикативӣ мебошанд.


Нил Коблитс


Виктор Саул Миллер

2. Хатҳои каҷи эллиптикӣ ва хосиятҳои онҳо

Дар майдони G хати каҷи эллиптикии (ХКЭ) Е гуфта, маҷмӯи нуқтаҳои (x, y)–ро меноманд, ки координатаҳои он муодилаи зеринро қаноат мекунонанд.

[1] http://www.math.washington.edu/~koblitz
[2] http://www.ithistory.org/honor-roll/dr-victor-saul-miller

$$E: y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a_6, \quad a_i \in F \qquad (1)$$

Муодилаи хати кач (ХК) (1) аз мачмӯи нуқтаҳои $(x, y) \in G$ ва нуқтаи беохир дурӣ (бесконечно удалённой точки) О таркиб ёфтааст.

Ба ҷойи муодилаи (1) функсияи ду тағйирёбандаи зеринро дида мебароем.

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6. \qquad (2)$$

ХКЭ-и E сингулярӣ номида мешавад, агар дар он аққалан як нуқтаи махсуси (x_0, y_0) мавҷуд бошад, ки дар ин нуқта ҳосилаҳои хусусии функсияи (2) ба сифр баробар шаванд.

$$\begin{cases} \frac{\partial F(x_0,y_0)}{\partial x} = 0, \\ \frac{\partial F(x_0,y_0)}{\partial y} = 0. \end{cases}$$

Дар ҳолати акс ХК ғайрисунгулярӣ номида мешавад. Чунин ХК суфта ба ҳисоб мераванд, зеро дар он нуқтаи баргашт (возврата) ва худбурранда (самопересечений) мавҷуд набуда, дар дилхоҳ нуқтаи он метавон расанда гузаронид. Маҳз ҳамин хел хатҳои кач дар криптография мавриди таваҷҷуҳ қарор мегиранд.

Барои татбиқ дар криптография вобаста аз характеристикаи майдон, метавон ба усули гузориш муодилаи (1)-ро ба шаклҳои каноникии гуногун оварад. Масалан:

$$\begin{cases} y^2 = x^3 + ax + b, \text{агар } \ p \neq 2 \text{ ва } p \neq 3 \text{ бошад,} \\ y^2 = x^3 + a_2x^2 + a_4x + a_6, \text{агар } \ p = 3 \text{ бошад,} \\ \begin{cases} y^2 + y = x^3 + ax + b - \text{ХК} - \text{и суперсингулярӣ} \\ y^2 + xy = x^3 + ax + b - \text{ХК} - \text{и} - \text{ғайри суперсингулярӣ.} \end{cases} \\ \text{агар } \ p = 2 \text{ бошад.} \end{cases}$$

3. Шарти ғайрисингулярии ХК

Дар майдони охирноки характеристикааш аз 2 ва 3 фарқкунанда ХКЭ тавассути муодилаи зерин дода мешавад:

$$E_p(a,b): \ y^2 = x^3 + ax + b \ mod \ p. \qquad (3)$$

Дар ин ҷо $p-$ адади сода ва коэффитсиентҳои муодилаи (3) $a, b \in F_p$ буда, бояд шарти зеринро қаноат кунонанд.

$$4a^3 + 27b^2 \neq 0(mod \ p) \qquad (4)$$

Азбаски $y = \pm\sqrt{x^3 + ax + b}$ аст, пас графики ХК нисбат ба тири абтсисса симметрӣ мебошад. Барои ёфтани нуқтаи расандаи он ба тири абтсисса бояд муодилаи кубии зерин ҳал карда шавад.

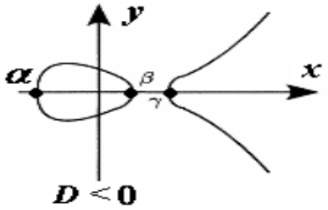
$$x^3 + ax + b = 0 \qquad (5$$

Тавре ки маълум аст барои ҳал намудани муодилаи (5) аз формулаи маъмули Кардано истифода бурда мешавад. Дискриминанти муодилаи (5) тавасси формулаи зерин муайян карда мешавад.

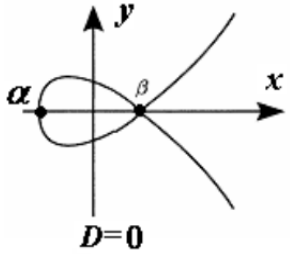
$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{108}.$$

Ҳамин тариқ:

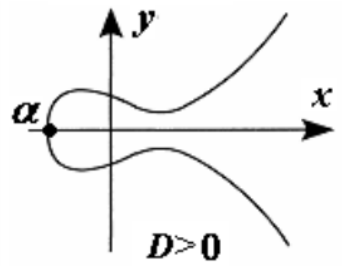
1) Агар $D<0$ бошад, он гоҳ (5) дорои се решаи ҳақиқии α, β, γ мебошад. Дар ин ҳолат графики муодилаи (10) аз ду қисм таркиб меёбад.



2) Агар $D = 0$ бошад, он гоҳ (10) дорои се решаи ҳақиқии α, β, γ мебошад, ки дутои онҳо якхела мебошанд. Графики муодилаи (10) дар ин ҳолат шакли зеринро дошта, нуқтаи $(\beta, 0)$–нуқтаи махсус ба ҳисоб меравад, зеро дар ин нуқта ду расанда мавҷуд мебошад. Дар ин ҳолат ХК-ро сингулярӣ меноманд. Чунин навъ хатҳои кач дар криптография истифода бурда намешаванд.



3) Агар $D > 0$ бошад, он гоҳ муодилаи (10) дорои як решаи ҳақиқии α ва ду решаи комплекии ҳамроҳшудаи $\beta \pm i\gamma$ мебошад. Графики муодилаи (10) дар ин ҳолат шакли зеринро дорад:



Ҳамин тариқ, ҳангоми характеристикаи майдон аз 2 ва 3 фарқкунанда будан, муодилаи (5) дар ҳолати иҷроиши шарти (4), ки ба $D \neq 0$ эквивалент аст, ғайрисингулярӣ ба ҳисоб меравад.

Яке аз хосиятҳои муҳими дигари ХКЭ инвариант $J(E)$ ба ҳисоб меравад.

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Коэффитсиентҳои ХКЭ $E_p(a,b) -$ро ҳангоми маълум будани инвариант $J(E)$ метавон чунин муайян кард:

$$\begin{cases} a = 3k \ (mod\ p), \\ b = 2k (mod\ p). \end{cases}$$

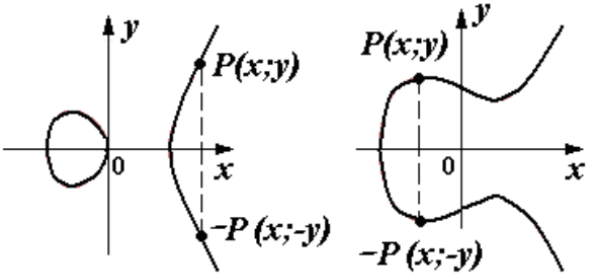
Дар ин ҷо k аз рӯйи инвариант ҳисоб (муайян) карда мешавад.

$$k = \frac{J(E)}{1728 - J(E)} \ (mod\ p), \ J(E) \neq 0, \quad J(E) \neq 1728.$$

Ҳангоми табдилдиҳии хаттии ХК инвариант $J(E)$ тағйир намеёбад. Агар инварианти $J(E)$ ду ХК якхела бошанд, он гоҳ онҳо бо ҳамдигар изоморфизм мебошанд.

4. Қонуни ҷамъ ва таҳияи гурӯҳи нуқтаҳои ХКЭ

Симметрияи ХК нисбати тири Ox имконияти ба таври аёни (наглядное) муайянкунии нуқтаи баръаксро фароҳам меорад. Барои нуқтаи додашудаи $P(x,y)$ дар ХКЭ нуқтаи баръакс гуфта, нуқтаи $-P(x,-y)$–ро мемонанд.



Яке аз хосиятҳои шоёни диққати ХК-и ғайрисингулярӣ дар он аст, ки дилхоҳ ХР-и аз ду нуқтаи он гузаранда, ХК-ро дар як нуқта (нуқтаи ягона) мебурад. Илова бар ин, расанда ба ХКЭ дар дилхоҳ нуқта (ба ғайр аз нуқтаи перегиба) ба як нуқтаи дигар низ расанда мебошад. Чунин хусусият имконияти муайянкунии амали ҷамъи нуқтаҳои ХКЭ-ро фароҳам меорад.

Бигузор ду нуқтаи ХКЭ $P(x_1,y_1)$ ва $Q(x_2,y_2)$ дода шуда бошанд. Тавассути ин нуқтаҳо расанда мегузаронем. Ин ХР ХК-ро дар нуқтаи сеюм R' ки ҳатман мавҷуд аст мебурад. Суммаи ду нуқтаи $P(x_1,y_1)$ ва $Q(x_2,y_2)$ гуфта, нуқтаи $R(x_3,y_3)=P(x_1,y_1)+Q(x_2,y_2)$ −ро мемонанд, ки ба нуқтаи сеюм, яъне нуқти расандаи ХКЭ ва ХР-и аз нуқтаҳои $P(x_1,y_1)$ ва $Q(x_2,y_2)$ гузаранда баръакс мебошад. Нуқтаи $R(x_3,y_3)$ тавасути амали муроҷиат $-(x,y)=(x,-y)$ ба даст оварда мешавад.

Агар ҳангоми ҷамъ нуқтаҳои $P(x_1, y_1)$ ва $Q(x_2, y_2)$ баробар бошанд, он гоҳ натиҷаи ҷамъ ба дучанди нуқтаи $P(x_1, y_1)$ баробар мешавад.

$$R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2) = P(x_1, y_1) + P(x_1, y_1) = 2P(x_1, y_1).$$

Дар ин ҳолат бурраидаи (секущая) PQ ба расандаи ХК мубаддал мегардад. Аз нуқтаи назари геометри дучанди нуқтаи $2P$ –ин нуқтаи баръакс ба нуқтаи бурриши ин расанда ба ХКЭ мебошад.

Акнун координатаҳои нуқтаи $R(x_3, y_3)$–ро тавассути координатаҳои нуқтаҳои $P(x_1, y_1)$ ва $Q(x_2, y_2)$ ифода карда, ҳосил мекунем(меёбем). Дар ин вақт нуқтаи $P(x_1, y_1)$ ва $Q(x_2, y_2)$ метавонанд гуногун ё якхела бошанд. Вобаста ба ин ду ҳолат ҷой дорад.

1) Ҳангоми $P \neq \pm Q$ будан. Дар ин ҳолат, ибтидо муодилаи ХР-и аз ду нуқтаи $P(x_1, y_1)$ ва $Q(x_2, y_2)$ гузарандаро менависем, ки шакли зеринро дорад:

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}.$$

Аз ин ҷо коэффитсиенти кунҷи ХР ба

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p) \qquad (6)$$

баробар мешавад. Муодилаи ХР-и PQ бошад, шакли зеринро мегирад:

$$y = y_1 + \lambda(x - x_1) \qquad (7)$$

Акнун координатаҳои нуқтаи сеюми расандаи ХК ва ХР-и PQ–ро ҷустуҷӯ мекунем.

$$\begin{cases} y^2 = x^3 + ax + b, \\ y = y_1 + \lambda(x - x_1). \end{cases} \Rightarrow (y_1 + \lambda(x - x_1))^2 = x^3 + ax + b.$$

Тарафи чапи баробарии охиронро ба квадрат бардошта, пас аз гурӯҳбандии аъзоҳои монанд муодилаи кубии зеринро ба даст меорем.

$$x^3 - \lambda^2 x^2 + \cdots = 0$$

Мувофиқи теоремаи Виет барои муодили кубӣ: суммаи решаҳои муодилаи кубӣ ба коэффитсиенти назди x^2 ба аломати баръакс баробар мебошад, яъне

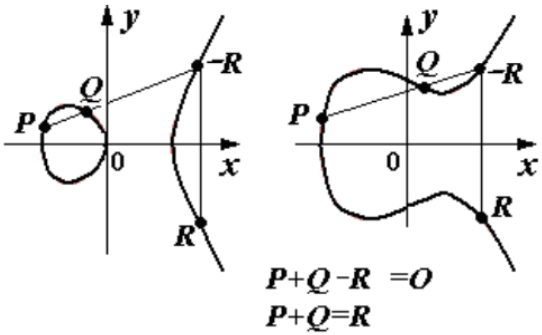
$$\begin{cases} x_1 + x_2 + x_3 = \lambda^2, \\ x_3 = \lambda^2 - x_1 - x_2. \end{cases}$$

Қимати x_3–ро ёфта ба муодилаи ХР –и PQ гузошта, ординатаи нуқтаи $-R$ –ро меёбем.

$$y'_3 = y_1 - \lambda(x_3 - x_1).$$

Нуқтаи R ба нуқтаи $-R$ нисбат ба тири Ox симметрӣ мебошад, аз ин рӯ координатаҳои нуқтаи матлуб шакли зеринро мегиранд:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 (mod\ p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p). \end{cases} \quad (8)$$



2) Ҳангоми $P = Q$ будан, барои ёфтани $R = 2P$ ҳарду тарафи муодилаи (4)-ро дифференсиронида, ҳосил мекунем.

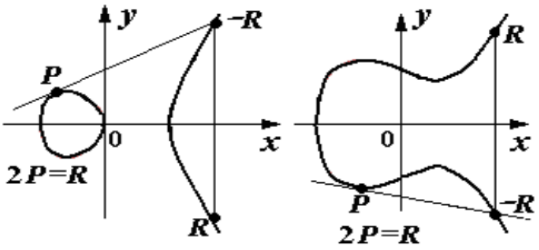
$$2ydy = (3x^2 + a)dx.$$

Тавре ки аз курси таҳлили математика медонем, дар нуқтаи P ҳосила ба коэффитсиенти расандаи ХК баробар мешавад.

$$\lambda = \frac{dy(x_1, y_1)}{dx}\Big| = \frac{3x_1^2 + a}{2y_1} \qquad (9)$$

Акнун айнан монанди ҳолати қаблӣ, координатаҳои нуқтаи $R -$ ро меёбем ки дар ҳамон ХР мехобанд.

$$\begin{cases} x_3 = \lambda^2 - 2x_1 (mod\ p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p). \end{cases} \qquad (10)$$



Бевосита аз ифодаҳои (8) ва (9) аён аст, ки нуқтаи O ҳангоми дучанди нуқтаи P бо координатаҳои сифрии y ё ҳангоми ҷамъи ду нуқтаҳои гуногун бо координатаҳои якхелаи x ҳосил мешавад.

Барои нуқтаи O чунин қоидаи амали ҷамъ муайян карда шудааст.:

$$(x, y) + O = O + (x, y) = (x, y),$$
$$O + O = O$$
$$(x, y) + (x, -y) = O$$

Мисоли 1. ХКЭ-и $E_7(2,6)$ –ро дида мебароем, ки муодилаи умуми он шакли зеринро дорад:

$$E_7(2,6): y^2 = x^3 + 2x + 6.$$

Ибтидо иҷроиши шарти (9)-ро месанҷем

$$4a^3 + 27b^2 = 42^3 + 276^2 = 4 \cdot 1 + 6 \cdot 1 = 3 \neq 0(mod\ 7).$$

Тавре ки аён аст, ХК-и додашуда ғайрисингулярӣ мебошад. Ягон нуқтаи ихтиёриро дар $E_7(2,6)$ меёбем. Бигузор $x = 5$ бошад, он гоҳ аз муодилаи ХК ҳосил мекунем.

$$y^2 = 5^3 + 2 \cdot 5 + 6 = 6 + 3 + 6 = 1(mod\ 7)$$

Аз ин ҷо $y = 1(mod\ 7)$ ё $y = -1 = 6(mod\ 7)$ мешавад. Ҳамин тариқ, мо ду нуқтаи (5,1) ва (5,6) -ро ҳосил кардем. Акнун ҷуфти нуқтаҳои дигарро бо истифода аз амали дучанди нуқтаҳо меёбем. Барои ҳисобкунии $[2](5,1)$ аз формулаҳои (9) ва (10) истифода бурда мешавад.

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 5^2 + 2}{2 \cdot 1} = \frac{0}{2} = 0(mod\ 7).$$

$$\begin{cases} x_3 = 0^2 - 2 \cdot 5 = 4(mod\ 7), \\ y_3 = 0(5-4) - 1 = 6((mod\ 7). \end{cases}$$

Ҳамин тариқ, мо нуқтаи $[2](5,1)$ –ро ҳосил кардем. Барои санҷиши онки нуқтаҳои ҳосилшуда дар ХК мехобанд, координатаҳои онро ба муодилаи мисоли додашуда гузошта месанҷем. Бо ҳамин тарз метавон нуқтаҳои дигарро низ ҳосил кард.

Мисоли 2. Бигузор $P(-3,9)$ ва $Q(-2,8)$ нуқтаҳои ХКЭ $E_7(1,-36)$ бошанд. Қимати $R = P + Q$ –ро ҳисоб мекунем.

Дар ин ҷо, $x_1 = -3, y_1 = 9, x_2 = -2,\ y_2 = 8$ мебошад. Аз формулаҳои (11) ва (13) истифода карда ҳосил мекунем.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-9}{-2-(-3)} = \frac{-1}{1} = -1 = 6(mod\ 7)$$

$$\begin{cases} x_3 = 6^2 - (-3) - (-2) = 41 = 6(mod\ 7), \\ y_3 = 6(-3-6) - 9 = -45 = 4(mod\ 7). \end{cases}$$

Ҷавоб. $R = P + Q = (6, 4)$.

Барои ҳисобкунии сумма ва дучанди нуқтаи додашуда, метавон аз класси зерин, ки дар забони C++ навишта шудааст, истифода кард:

```
int mod(int a, int b){
        if (a<0)
                return (b + (a%b));
        else
                return a%b;
}
int modInverse(int n, int p) {
        n = mod(n, p);
        for (int x = 1; x < p; x++) {
                if (mod(n*x, p) == 1) return x;
        }
        return 0;
}
class ECPoint{
public:
        int a, b, p, x, y;
        ECPoint(){
                a = b = p = x = y = 0;
```

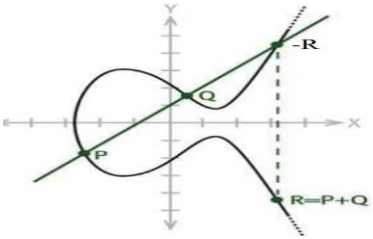
```
        }
};
 ECPoint DoubleP(ECPoint p1){
   int l1, l2, l;
        ECPoint Z;
        Z.p = p1.p;
        Z.a = p1.a;
        Z.b = p1.b;
        l1 = mod((3 * p1.x * p1.x + p1.a), p1.p);
        l2 = mod((2 * p1.y), p1.p);
        l = (l1*modInverse(l2, p1.p)) % p1.p;
        Z.x = mod((l*l - 2 * p1.x), p1.p);
Z.y = mod((l*(p1.x - Z.x) - p1.y), p1.p);
        return Z;
}
  ECPoint operator+(ECPoint p1, ECPoint p2){
        ECPoint Z;
        int l1, l2, l;
        p2.p = p1.p;
        p2.a = p1.a;
        p2.b = p1.b;
        l1 = mod((p2.y - p1.y), p1.p);
        l2 = mod((p2.x - p1.x), p1.p);
        l = (l1*modInverse(l2, p1.p)) % p1.p;
        Z.x = mod((l*l - p1.x - p2.x), p1.p);
        Z.y = mod((l*(p1.x - Z.x) - p1.y), p1.p);
        return Z;
}
```

Масъалаи ҳисобкунии миқдори умумии нуқтаҳои ХК –яке аз масъалаҳои муҳим дар истифодаи криптографии онҳо ба ҳисоб меравад. Баъдтар ин масъаларо мавриди баҳс қарор медиҳем.

Барои таҳия намудани гурӯҳи нуқтаҳои ХКЭ, ба сифати элементи нейтралии гурӯҳ нуқтаи $O(x,\infty)$ –ро интихоб мекунем. Барои нуқтаи мазкур баробарии зерин ҷой дорад:

$$R + (-R) = O, \quad \forall R \in E_p(a,b).$$

ХР – и аз нуқтаҳои R ва $-R$ гузаранда, нисбат ба тири абтсисса Ox перпендикуляр мебошад, аз ин ҷо метавон хулоса баровард, ки нуқтаи сеюми расанда перпендикуяр буда, ХК қад-қади (ба самти) тири ординат $0y$ ба беохир майл мекунад. Аз ин ҷост, ки нуқта O–ро нуқтаи беохир дури ХК меноманд.



Мувофиқи теоремаи Анри Пуанкаре [1] маҷмӯи нуқтаҳои ХКЭ якҷоя ба нуқтаи O нисбат ба амали ҷамъ гурӯҳи комутативиро ташкил медиҳанд. Бе душворӣ дидан мумкин аст, ки дар ин ҷо ҳамаи аксиёмаҳои

[1] https://en.wikipedia.org/wiki/Henri_Poincar%C3%A9

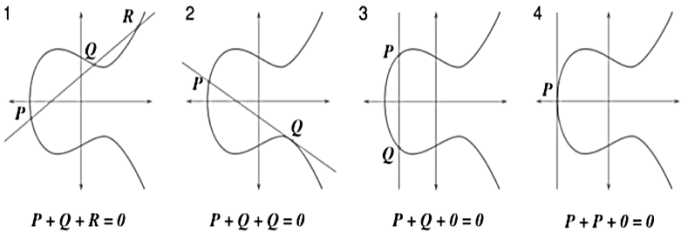
гурӯҳи мултипликативӣ иҷро мешаванд: маҳдудӣ, комутативӣ, ассостсиативӣ, мавҷудияти элементи баръакс ва элементӣ нейтралӣ.

Таъриф. Гурӯҳи нуқтаҳои ХКЭ дар майдони охирноки $GF(p)$ гуфта, маҷмӯи нуқтаҳои (x, y) – ро мемонанд, ки координатаҳои он ба майдони мазкур таалуқ дошта, муодилаи (8)-ро қаноат мекунонанд, агар характеристикаи майдон $p \neq 2, 3$ буда, $a, b \in GF(p)$ ва шарти (9) ҷой дошта бошад. Ба гурӯҳи нуқтаҳои ХКЭ нуқтаи $O(x, \infty)$ низ дохил мешавад.

Барои осон шудани истифодабарӣ формулаҳои ҷамъ ва дучанди нуқтаҳо ХКЭ-и (8)-ро ба шакли ҷадвал меорем.

Амал	Майдони характеристикааш аз 2 ва 3 фарқкунанда.
Ҷамъи нуқтаҳо: $P \neq \pm Q$, $R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2)$.	$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$ $\begin{cases} x_3 = \lambda^2 - x_1 - x_2 (mod\ p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p). \end{cases}$
Дучанди нуқтаҳо: $P = Q$, $R(x_3, y_3) = 2P(x_1, y_1)$.	$\lambda = \frac{3x_1^2 + a}{2y_1};$ $\begin{cases} x_3 = \lambda^2 - 2x_1 (mod\ p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (mod\ p). \end{cases}$
$P(x, y) + O = O + P(x, y) = P(x, y).$ $O + O = O.$ $P(x, y) + P(x, -y) = O.$	

Қайд кардан ба маврид аст, ки барои нуқтаи O хосиятҳои зерин, ки ба шакли графикӣ оварда шудаанд, низ ҷой доранд.



5. Тартиби нуқтаҳои ХКЭ

Таъриф. Тартиби нуқтаи P гуфта, чунин ададӣ хурдтарини k –ро меноманд, ки барои он баробарии $[k]P = 0$ иҷро шавад.

Масалан, дар гурӯҳи $E_{11}(6,3)$ тартиби нуқтаи $(9,4)$ ба 5 баробар мебошад. Дар ҳақиқат

$$2(9,4) = (7,6);\ \ 3(9,4) = (7,5);\ \ 4(9,4) = (9,7);$$
$$5(9,4) = 0\,.$$

Мувофиқи теоремаи Лагранҷ тартиби нуқта тартиби ХКЭ-ро тақсим мекунад. Аз ин рӯ ҳангоми муайянкунии тартиби ХК метавон онро ба ХК мувофиқи изоморфизм иваз кард, чунки тартиби хатҳои качӣ изоморфӣ якхела мебошад. Ҳангоми интихоби параметрҳои a, b, p тартиби ХК метавонад ададӣ сода бошад. Дар ин ҳолат, дилхоҳ нуқта ба ғайр аз O (сифр) метавонад генератори ҳамаи маҷмӯъ ба ҳисоб равад, яъне чунин нуқтаи G ёфт мешавад, ки қатори: $G, [2]G,\ [3]G, \dots,$ $[n]G$ (дар ин ҷо $n = \#E_p(a,b)$ аст) ҳамаи нуқтаи маҷмӯи $E_p(a,b)$ –ро дарбар мегирад, зимнан $[n]G = 0$ аст.

Чунин ХК аз нуқтаи назари криптографӣ истифодаи хеле васеъ дорад. Агар бо баъзе сабабҳо ёфтани чунин ХК имкон надошта бошад, вале $\#E_p(a,b) = hq$ шавад (дар ин ҷо p–ададии сода ва h – ададии хурд аст), он гоҳ дар $E_p(a,b)$ зермаҷмӯи иборат аз q –нуқта мавҷуд аст, ки генератори он метавонад, дилхоҳ нуқтаи $G \neq 0$ ба ҳисоб равад, ки барои он $[q]G = 0$ мебошад.

Қайд кардан ба маврид аст, ки дар сурати таритиби n доштани нуқтаи P маҷмӯи $\{O, P, 2P, \dots, (n-1)P\}$ – зергурӯҳи давриро дар $E_p(a,b)$ташкил медиҳад.

Барои ёфтани тартиби нуқтаи додашудаи P-и ХКЭ-и (8) дар майдони $GF(p)$ бояд муодилаи $[n]P = 0$ ҳал карда шавад. Ин амалро метавон тавассути алгоритми зерин иҷро кард.

1) Қимати $m = \left[\sqrt{N_1}\right]$ – (бо барзиёди яклухт карда мешавад), ки дар ин ҷо $N_1 = p + 1 + 2\sqrt{p}$ (баҳои максималии тартиби гурӯҳи нуқтаҳои ХКЭ дар теоремаи Хассе аст, ҳисоб карда мешавад.
2) Ҷадвали ҷуфти (j, jP) -ҳо барои $j = 1,2, \dots, m$ сохта мешавад.
3) Қимати $\alpha = -mP$ ҳисоб карда мешавад.
4) $\gamma = 0$ карда мешавад (бахшида мешавад).
5) Барои $i = 1,2, \dots, m-1$ амалҳои зерин иҷро карда мешаванд.
    5.1. Санҷида мешавад, ки нуқтаи γ дар ҷадвал мавҷуд аст ё не.
    5.2. Агар $\gamma = jP$ бошад, он гоҳ ҳисоб карда мешавад: $m = mi + j$.

5.3. Қимати γ α воҳид зиёд карда мешавад, яъне $\gamma = \gamma + \alpha$.

Мисол. Тартиби нуқтаи $P(0,1)$–и ХКЭ $y^2 = x^3 + x + 1$ дар майдони $GF(5)$ ҳисоб карда шавад.

Ҳал. $N_1 = p + 1 + 2\sqrt{p} = 5 + 1 + 2\sqrt{5} \approx 10 \Longrightarrow m = \left[\sqrt{N_1}\right] = \left[\sqrt{10}\right] = 4$.

Ҷадвали зеринро тартиб дода пур мекунем.

j	1	2	3	4
jP	(0, 1)	(4, 2)	(2, 1)	(3, 4)

Қимати

$\alpha = -mP = -4(0,1) = -(3,4) = (3,-4)(mod\ 5) = (3\ 1) -$ ро меёбем.

$\gamma = 0$ мегузорем. Ин нуқта дар ҷадвал вуҷуд надорад. Қадами оянда ҳисоб мекунем.

$i = 1 \Longrightarrow \gamma = \gamma + \alpha = O + (3,1) = (3,1) -$ дар ҷадвал вуҷуд надорад.

$i = 2 \Longrightarrow \gamma = \gamma + \alpha = (3,1) + (3,1) = (0,1) -$ дар ҷадвал ҳангоми $j = 1$ будан мавҷуд аст.

Ҳамин тариқ, тартиби нуқтаи $P(0,1)$ ба $m = m \cdot i + j = 4 \cdot 2 + 1 = 9$ баробар мешавад.

6. Миқдори нуқтаҳои ХКЭ

Маҷмӯи $E_p(a,b)$ аз ҳамаи нуқтаҳои (x,y), $0 \le x,y \le p$, ки муодилаи (1) ва нуқтаи О-ро қаноат мекунонанд, таркиб ёфтааст. Маълум аст, ки ин маҷмӯи нуқтаҳо охирнок мебошад, чунки дар он танҳо нуқтаҳо бо

координатаҳои бутун дохил мешаванд. Миқдори нуқтаҳо дар $E_p(a,b)$ бо $\#E_p(a,b)$ ишорат карда мешавад.

Миқдори умумии нуқтаҳо $\#E_p(a,b)$–ро дар ХК низ тартиби n–уми ХКЭ меноманд.

Барои адади на онқадар калони p ҳисобкунии гурӯҳи нуқтаҳои ХКЭ ва тартиби онҳо имконпазир аст.

Барои сохтани руйхати нуқтаҳо, кифоя аст, ки элементҳои $0 \le x \le p-1-$ ро интихоб намуда, барои ёфтани y муодилаи

$$y^2 = f(x)(mod\ p) \qquad (1)$$

-ро ҳал карда, яъне амали аз решаи квадратӣ баровардан иҷро карда мешавад. Усули баровардан аз решаи квадратӣ дар майдони охирнокро дар боби 5 мавриди баҳс қарор дода будем. Дар ин ҳолат ёфтани як решаи кифоя аст, решаи дигарро бошад тавассути формулаи $-mod\ p = p - y$ ёфтан мумкин аст.

Барои ҳисобкунии решаҳои муодилаи (1) метавон аз назарияи тафриқҳои квадратӣ ва рамзи Лежандр истифода карда, дар ин ҳолат ҳангоми $p > 2$ будан, ба содагӣ метавон формула барои ҳисоби миқдори нуқтаҳои ХКЭ $y^2 = f(x)$ ҳосил карда. Муқоисаи (1) нисбат ба y барои x–ҳои қайдкардашуда ва $p > 2$ дорои $1 + \frac{f(x)}{p}$ ҳал мебошад, аз ҷумла 0 низ ҳал ба ҳисоб меравад. Бо назардошти нуқтаи 0 формулаи умумии ҳисобкунии тартиби n–уми ХК шакли зеринро мегирад.

$$n = p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) \qquad (2)$$

Хосиятҳои нишонаи Лежандр ва Якобӣ қаблан дар бобҳи 3 мавриди баҳс қарор гирифта шуда буданд.

Мисол. Миқдори нуқтаҳо дар ХКЭ-и зерин ҳисоб карда шавад.

$$E_7(2,6): y^2 = x^3 + 2x + 6(mod\ 7).$$

Алгоритми азназаргузаронии (перебор) ҳамаи нуқтаҳоро истифода мекунем, ки барои ин вақти иҷроиши алгоритм ба таври экспоненсиалӣ зиёд мешавад. Барои x қиматҳои аз 0 то 6-ро дода? маҷмӯи нуқтаҳои $E_7(2,6)$ −ро бо координатаҳои бутун меёбем

x	y^2		y_1	y_2
$x=0$	$y^2=6$		$y_{1,2}$ − мавҷуд нест	
$x=1$	$y^2=1+2+6=9=2$		$y_1=3$	$y_2=-3=4$
$x=2$	$y^2=8+4+5=4$		$y_1=2$	$y_2=-2=5$
$x=3$	$y^2=27+6+6=4$		$y_1=2$	$y_2=-2=5$
$x=4$	$y^2=64+8+6=1$		$y_1=1$	$y_2=-1=6$
$x=5$	$y^2=125+10+6=1$		$y_1=1$	$y_2=-1=6$
$x=6$	$y^2=216+12+6=3$		$y_{1,2}$ − мавҷуд нест	

Миқдори нуқтаҳои ёфташударо ҳисоб карда, пас аз иловакунии нуқтаи О миқдори нуқтаҳоро ба сурати зерин ҳосил мекунем.

$$\#E_p(a,b) = 10 + 1 = 11.$$

Роҳи дуюми ҳисобкунии миқдори нуқтаҳои ХКЭ ин истифода аз нишонаи Лежандр $\left(\frac{f(x)}{p}\right)$ мебошад. Ҳосил мекунем:

$$x = 0,\ \left(\frac{0^3 + 2\cdot 0 + 6}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = |7 \equiv 3(mod\ 4)| = -1.$$

$$x=1,\ \left(\frac{1^3+2\cdot 1+6}{7}\right)=\left(\frac{9}{7}\right)=\left(\frac{1\cdot 3^2}{7}\right)=\left(\frac{1}{7}\right)=1.$$

$$x=2,\ \left(\frac{2^3+2\cdot 2+6}{7}\right)=\left(\frac{18}{7}\right)=\left(\frac{2\cdot 3^2}{7}\right)=\left(\frac{2}{7}\right)\cdot\left(\frac{1\cdot 3^2}{7}\right)$$
$$=\left(\frac{2}{7}\right)=(-1)^{\frac{7^2-1}{8}}=1.$$

$$x=3,\ \left(\frac{3^3+2\cdot 3+6}{7}\right)=\left(\frac{39}{7}\right)=\left(\frac{4+5\cdot 7}{7}\right)=\left(\frac{4}{7}\right)=\left(\frac{2}{7}\right)\cdot\left(\frac{2}{7}\right)$$
$$=1.$$

$$x=4,\ \left(\frac{4^3+2\cdot 4+6}{7}\right)=\left(\frac{78}{7}\right)=\left(\frac{1+11\cdot 7}{7}\right)=\left(\frac{1}{7}\right)=1.$$

$$x=5,\ \left(\frac{5^3+2\cdot 5+6}{7}\right)=\left(\frac{141}{7}\right)=\left(\frac{1+20\cdot 7}{7}\right)=\left(\frac{1}{7}\right)=1.$$

$$x=6,\ \left(\frac{6^3+2\cdot 6+6}{7}\right)=\left(\frac{234}{7}\right)=\left(\frac{3+33\cdot 7}{7}\right)=\left(\frac{3}{7}\right)$$
$$=(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{3}\right)=-\left(\frac{1+2\cdot 3}{3}\right)=-1.$$

Формулаи (2)-ро татбиқ карда ҳосил мекунем:

$$\#E_p(2,6)=7+1+3=11.$$

Акнун таърифи тартиби гурӯҳро бо суханҳои дигар баён мекунем.

Таъриф. Миқдори элементҳои гурӯҳи нуқтаҳои ХКЭ $E_p(a,b)$ тартиби ин гурӯҳ номида мешавад.

Барои муайянкунии сарҳадҳои болоӣ ва поёнии тартиби нуқтаҳо метавон аз теоремаи Хассе истифода кард.

Теорема (Хассе). Барои тартиби N_E-гурӯҳи нуқтаҳои ХКЭ дар майдони $GF(q)$ (дар ин ҷо q–миқдори элементҳои майдон мебошад) нобаробарии зерин ҷой дорад:

$$q + 1 - 2\sqrt{q} \leq N_E \leq q + 1 + 2\sqrt{q}.$$

Дар ҳолати умумӣ дақиқ муайянкунии миқдори нуқтаҳои ХКЭ масъалаи бениҳоят душвор мебошад. Нахустин алгоритми ҳисобкунии миқдори нуқтаҳои ХКЭ дар майдони охирнок бо печидагии полиномиалӣ Рене Шуф пешниҳод кард. Дар ибтидо алгоритми Шуф дар амалия камтар татбиқ пайдо кард. Баъдтар Элкис ва Аткин якчанд тағйирот ба он ҳамроҳ кардаанд, ки ҳоло бо номи SEA (ҳарфҳои аввалаи насаби муаллифон) машҳур мебошад.

7. Композитсияи нуқтаҳои ХКЭ

Аз амали ҷамъ ва дучанди нуқтаҳо, амали зарби нуқтаи ХКЭ бо адади додашуда (скаляр) бармеояд. Нуқтаи $[m]P$ ба m–маротиба ҷамъи нуқтаи P бо худаш дар гурӯҳи аддитивии ХКЭ баробар буда, зарби скалярии нуқтаи P ба адади m номида мешавад. Худи нуқтаи $[m]P$ бошад, каратии скалярии нуқта ба ҳисоб меравад. Амали зарби скаляриро бо нуқта композитсия низ меноманд. Амали композитсияи нуқтаро бо ягон адади m ҷамъбаст карда ҳосил мекунем.

1) $[m]P = \underbrace{P + P + \cdots + P}_{m-\text{мартиба}}$.
2) $[0]P = O$;
3) $-[m]P = -(\underbrace{P + P + \cdots + P}_{m-\text{мартиба}})$.
4) $-mP(x, y) = mP(x, -y)$.

Қайд кардан ба маврид аст, ки амали композитсия хело зуд иҷро гардида на зиёда аз $2logm$ амалро талаб мекунад.

Дар арифметикаи ХКЭ барои ҳисоб намудани $[m]P(x,y)$ алгоритми муайян вуҷуд надорад. Ин амал тавассути амали ҷамъ, тарҳ ва дучанди нуқта иҷро карда мешавад. Яке аз роҳҳои сода ҳисобкунии амали композитсияи чунин мубошад: ибтидо адади m ба намуди дӯӣ (системаи дӯӣ) $m = (b_t b_{t-1} \dots b_1)_2, (b_i \in \{0,1\})$ баргардонида шуда, сипас, ҳамаи нуқтаҳои $[2]P, [4]P, \dots, [2^t]P$ ҳисоб карда мешавад. Баъд аз ин суммаи ҳамаи он нуқтаҳои $2^i P$, ки барои онҳо $b_i = 1$ аст, ҳисоб карда мешаванд. Алгоритми ин амал чунин шакл дорад:

Вурудӣ: нуқтаи $P(x,y)$, адади $m = (b_t b_{t-1} \dots b_1)_2$.

Хурӯҷӣ: $Q = [m]P(x,y)$.

1) $Q \leftarrow 0$.

2) Барои $i = t, t-1, \dots, 1$ иҷро карда шавад.

2.1. $Q \leftarrow [2]Q$.

2.2. Агар $b_i = 1$ бошад, он гоҳ $Q \leftarrow Q + P$.

3) Натиҷа Q.

Ин алгоритм на зиёда аз t –амали ҷамъ ва t –дучанди нуқтаро талаб мекунад.

Мисол. Ҳисоб карда шавад: $[21]P$.

Ҳал. Маълум аст, ки $21 = (10101)_2$ ва $t = 5$ аст. Акнун нишон медиҳем, ки дар ҳар як қадами алгоритм чӣ ба амал меояд.

$[i = 5, \quad m_5 = 1]: Q \leftarrow 0; \ Q \leftarrow Q + P = P;$

$[i = 4, \quad m_4 = 0]: Q \leftarrow [2]Q = [2]P;$

$[i = 3, \quad m_3 = 1]: Q \leftarrow [2]Q = [4]P;$
$Q \leftarrow Q + P = [5]P;$
$[i = 2, \quad m_2 = 0]: Q \leftarrow [2]Q = [10]P;$
$[i = 1, \quad m_1 = 1]: Q \leftarrow [2]Q = [20]P;$
$Q \leftarrow Q + P = [21]P;$

Ба ёд меорем, ки $P_3 = P_1 + P_2 \ \ (P_1 \neq \pm P_2)$ (сатри чоруми алгоритм) тавасссути формулаи (12), (8) ва амали дучанди нуқта $P_3 = [2]P_1$ (сатри сеюми алгоритм) тавассути формулаи (9) ва (10) ҳисоб карда мешаванд. Нуқтаи O дорои чунин инъикос намебошад ва барои сарфи назар кардани амали дучанд то ҷамъи нахустин ҳамчун як байрақча(флажок) истифода мешавад.

Амали композитсияи нуқтаҳоро метавон ба шакли дигар низ навишт. Ҳоло ин навиштро бо мисоле дида мебароем.

Мисоли 2. Барои ёфтани $100P$ онро ба шакли зерин менависем.

$$100P = 2\Big(2\Big(P + 2\Big(2\big(2(P + 2P)\big)\Big)\Big)\Big).$$

Амали зарби нуқта бо адад монанди амали дараҷабардорӣ дар ҳолати RSA буда, миқдори на онқадар зиёди ҷамъро талаб мекунанд. Масалан, барои зарби нуқта ба адади дарозиаш ба 200 бит баробар тақрибан 100 амали дучанди ва 56 амали ҷамъи нуқтаҳо талаб карда мешавад. Барои муқоиса: ҳангоми ба дараҷаи адади дарозиаш ба 200 бит баробар бардоштани адади додашуда, тақрибан 300 амали зарб зарур мебошад.

8. Логарифмиронии дискретӣ дар ХКЭ

Амали зарби скалярӣ айнан ба амали бадарафтабардорӣ дар майдонҳои охирнок мебошад. Аз ин рӯ, дар ХКЭ дар нақши масъалаи роста зарби скалярии нуқтаи ХК амал (баромад) мекунад, яъне ҳисобкунии $Q = [m]P$ ҳангоми маълум будани m ва P. Масъалаи баръакс аз рӯйи анъана логарифмиронии дискретӣ дар ХКЭ номида шуда, чунин тасвият (формулировка) карда мешавад: ҳангоми маълум будани P ва Q чунин нуқтаи m ёфта шавад, ки барои он $[m]P$ ба Q баробар гардад.

Устувории рамзгузориро дар ХКЭ печидагии ҳалли масъалаи логарифмиронии дискретӣ ($ЛД$) дар гурӯҳи нуқтаҳои ХК муайян мекунад, яъне душвории ҳалли муодилаи $[m]P = Q$ нисбат ба m (дар ин ҷо P ва Q дар як зергурӯҳӣ даврӣ таалуқ доранд). Фарз карда мешавад, ки масъалаи $ЛД$ дар ХКЭ аз масъалаи ба он монанд дар майдонҳои охирнок душвортар мебошад. Қайд кардан ба маврид аст, ки барои ҳалли масъалаи $ЛД$ дар майдонҳои охирнок танҳо алгоритмҳои экспоненсиалӣ мавҷуд мебошанд, ки аз ҳама тезтарини онҳо – алгоритми Шенксӣ ва ρ −методи Полларда (ҳар кадомашон дорои печидагии $O(\sqrt{n})$ мебошанд), ба ҳисоб мераванд. Дар ХКЭ таҳияи чунин алгоритмҳо ғайриимкон аст, зеро дар ХКЭ аналоги ададҳои сода ва бисёраъзогиҳои оварданашаванда (неприводимих) мавҷуд намебошад.

Теорема. *Бисёраъзогии* $F(x) = x^3 + ax + b -$ *аз рӯӣ модули сода* (p) *ба зарбкунандаҳо ҷудошаванда, фақат ва фақат ҳамон вақт мешавад, агар* $КТУ(F(x), x^p - 1) = 1$ *шавад.*

Барои баъзе ХКЭ-и суперсингулярӣ масъалаи $ЛД$ эффиктивнӣ ҳал карда мешавад. Барои ХК сингулярӣ соли 1993 Менезес, Окатто ва Винстоун дар асоси табдилдиҳиҳи Вейля-Тейта алгоритми (MOV-атака) –ро коркард карданд, ки масъалаи $ЛД$-и ХКЭ-ро дар майдони $GF(q)$ ба масъалаи ба он мувофиқ дар ягон майдони аввалаи васеъкардаи $GF(q^k)$ (дар ин ҷо амали логарифмиронӣ метавонад эффективнитар бошад) меоварад. Аммо ин маълумотнома танҳо дар ҳолати хурд будани k муфид мебошад. Ин шарт асосан барои ХКЭ суперсингулярӣ иҷро мегардад. Дар ҳолатҳои боқимонда чунин маълумотнома амалан ҳеҷ вақт ба алгоритмҳои субэкспонентсиалӣ оварда намешавад.

Аз ин ҷост, ки ХК-и суперсингулярӣ дар рамзгузорӣ ва ИЭР татбиқ карда мешавад. Соли 2000 А. Ҷоукс татбиқи шоёни диққатӣ (замечателний) табдилдиҳии Вейля-Тайтама-ро дар криптография пайдо карда, протоколи сетарафаи як раундаро дар ассоси системаи Диффи-Ҳеллман коркард кард. Аз ин ҷо таҳиякунии калиди кушоди истифодабаранда, дар асосӣ итилоотҳои ошкор (ном, суроға ва ғайра) имконпазир гардид. Дар айниҳол ин масъала яке аз масъалаҳои маъмултарин ба ҳисоб меравад.

Агар тартиби N_E – гурӯҳи нуқтаҳои ХК ҳосили зарби ададҳои содаи хурд бошад, он гоҳ $ЛД$-ро метавон дар асоси алгоритми Полига-Ҳеллман коркард кард (провести).

9. Аналоги системаи Диффи-Ҳеллман дар ХКЭ

Криптоалгоримҳо дар ХКЭ айнан монанди алгортмҳо дар майдонҳои охирнок ба таври сода сохта мешаванд. Амали бадарачабарорӣ аз рӯйи модули калон, устувории рамзро муайян карда, дар ХКЭ ба зарби скалярии нуқта иваз карда мешавад. Дар ҷадвали зерин системаи криптоалгоритмҳои муқаррарӣ ва криптоалгоритмҳои ХКЭ ба намуди муҳовара оварда шудаанд.

Истилоҳҳо ва мафҳумҳо	Криптосистема дар майдонҳои охирноки сода	Криптосистемаҳои ХКЭ дар майдонҳои охирнок
Гурӯҳ	Z_p^*	$E\big(GF(p)\big)$
Элементҳои гурӯҳ	Ададҳои бутун $(1, 2, \dots, p-1)$	Нуқтаи $P(x, y)$ дар ХК ва нуқтаи O.
Амалҳои гурӯҳ	Зарб аз рӯйи модули p	Ҷамъи нуқтаҳо
Ишораҳо	Элементҳои g ва h.	Нуқтаҳои P ва Q.
	Элементи баръакс g^{-1}	Нуқтаи баръакс $-P$.
	Амали тақсим $g \cdot g^{-1}$	Фарқи нуқтаҳо $P - Q$.
	Бадарачабардорӣ g^a	Зарби скалярии $[m]P$.
Масъалаи ЛД	$g \in Z_p^*$; Аз рӯи $h \equiv g^a \ (mod\ p)$ ёфтани a	$P \in E\big(GF(p)\big)$; Аз рӯи $Q = [m]P$ ёфтани m

Моҳияти гузариш ба ХКЭ дар он аст, ки амали нисбатан сусти бадарачабардорӣ аз рӯйи модули калон ба амали нисбатан тезӣ зарби скалярӣ дар ХКЭ иваз карда мешавад. Дар ин ҳангом, амалҳо бо ададҳои бутун аз рӯйи модули на онқадар калон нигоҳ дошта мешаванд.

Ба сифати намуна аналоги эллиптикии схемаи Диффи-Ҳеллман (ECDH)-ро дида мебароем.

Ду истифодабаранда бо номҳои Алӣ ва Валӣ параметрҳои умумиро интихоб мекунанд, ки иборатанд аз:

- ✓ ХКЭ дар майдонҳои охирнок.
- ✓ Нуқтаи P дар ин ХК, ки тартиби калони $n-$ро доро мебошад. Элементи тавлидкунандаи гурӯҳи нуқтаҳои ХКЭ будани он шарт набуда, зергурӯҳи аз он тавлидшуда бояд калон бошад. Беҳтар мешавад, ки тартиби он ба тартиби гурӯҳ баробар бошад. Нуқтаи интихобкардашудаи P-ро нуқтаи базавӣ меноманд.

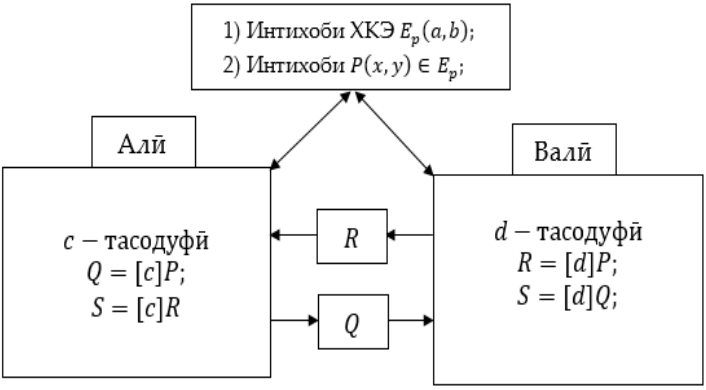
Параметрҳои умумӣ тавассути канали алоқаи кушод равон карда мешаванд. Пас аз ин, муштариён чунин амал мекунанд:

1) Алӣ ва Валӣ новобаста аз ҳамдигар ба сифати калиди махфии худ мувофиқан ададҳои тасодуфии c ва d (ададҳои наздик ба тартиби миқдори умумии нуқтаҳои ХКЭ)-ро интихоб карда, мувофиқан нуқтаҳои ошкори худ $Q = [c]P$ ва $R = [d]P -$ ро ҳисоб мекунанд(меёбанд).
2) Тавассути канали алоқаи кушод қиматҳои Q ва $R-$ро бо ҳамдигар мубодила мекунанд.

3) Алӣ ва Валӣ баъди ба дастоварии қиматҳои Q ва R мувофиқан қимати нуқтаи $S = [c]R$ ва $S = [d]Q$ –ро ҳисоб мекунанд.

Азбаски $[c]R = [c]([d]P) = [d]([c]P) = [d]Q$ аст, пас $S -$ ҳамчун калиди умумии истифодабарандагон ба ҳисоб меравад.

Шакли схематикии ин алгоритм чунин аст:



Мисол. Калиди умумӣ аз рӯйи схемаи Диффи-Ҳеллман сохта шавад, агар ХКЭ $E_{211}(0,-4)$ ва нуқтаи базавӣ (2, 2) интихоб карда шуда бошад.

Ҳал. ХК-и мавриди назар шакли $y^2 = x^3 - 4(mod\ 211)$ –ро дошта, тартиби нуқтаи P ба 241 баробар мебошад, чунки $[241]P = 0$ аст. Бигузор калиди махфии Алӣ $c = 121$ ва калиди махфии Валӣ $d = 203$ бошад. Онҳо мувофиқан қиматҳои $[121]P = [121](2,2) = (115,48)$ ва $[203]P = [203](2,2) = (130,203) -$ ро ҳисоб карда, ба ҳамдигар мубодила мекунанд, яъне Алӣ қимати $(115,48) -$ро ба Валӣ ва Валӣ бошад қимати

$(130, 203)$ – ро ба Алӣ равон мекунад. Баъди иҷрои ин амал чунин ҳисобкунӣ ба амал меояд.

$$\text{Алӣ: } [121](130, 203) = (161, 169);$$

$$\text{Валӣ: } [203](115, 48) = (161, 169);$$

Тавре ки аз ҳисобкуниҳои охирон дида мешавад, калиди махфии умумии Алӣ ва Валӣ ҷуфти ададҳои (нуқтаи) (161, 169) мебошад. Агар хоҳем, ки онро дар рамзгузории симметрӣ истифода барем, он гоҳ барои иҷрои ин мақсад метавон абтсиссаи нуқтаи x ё ягон функсияи аз x вобастаро истифода кард.

Барои шикастани ин схема, душман бояд аз муносибатҳои $Q = [c]P$ ва $R = [d]P$ қимати ададҳои c ва d –ро ҳисоб кунад, яъне амали $Л Д$-ро бояд иҷро кунад, лекин барои он логарифмӣ эффективӣ дар ХКЭ мавҷуд намебошад. Протоколӣ Диффи-Ҳеллман ҳимоякардашуда намебошад, зеро душман метавонад, бо истифода аз параметрҳои ошкори муштарён P ва Q аз номӣ як муштарӣ ба муштарии дигар паём ирсол кунад.

10.Криптографияи Месси-Омур дар ХКЭ

Пеш аз оғози рамзгузорӣ истифодабарандагон бояд тавассути канали алоқаи кушод параметрҳои зерини криптосистемаро бо ҳамдигар мубодила кунанд.

- ✓ майдони охирноки $GF(q)$ (q-ададӣ калон).
- ✓ муодилаи ХКЭ дар майдони $GF(q)$.
- ✓ тартиби ХК N_E (миқдори умумии нуқтаҳои ХК).

Бигузор Алӣ мехоҳад пайғоми M −ро ба Валӣ равон кунад. Фарз мекунем, ки ин пайғом ба нуқтаи P мувофиқ меояд. он гоҳ :

1) Алӣ ва Валӣ новобаста аз ҳамдигар, махфиёна аз интервалӣ $(1, N_E)$ адади тасодуфии e -ро (барои он КТУ$(e, N_E) = 1$ аст) интихоб карда, элементи ба он баръакс $d = e^{-1}(mod\ N_E)$ −ро ҳисоб мекунанд. Дар оянда зернависӣ A ва B мувофиқан ба Алӣ ва Валӣ тааллуқ доштани параметрро ифода мекунанд. Ин ададҳоро онҳо махфӣ нигоҳ медоранд. Пас аз ин:

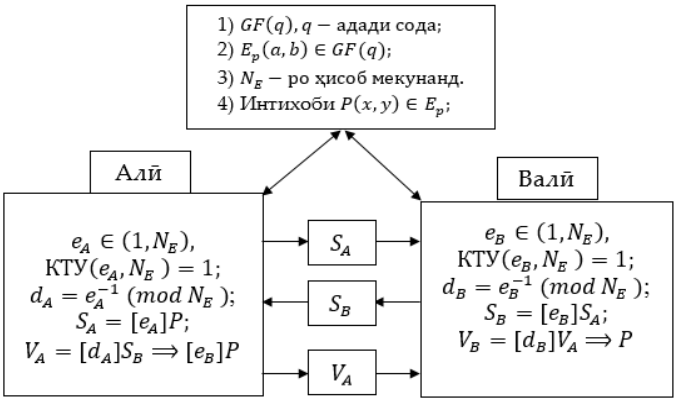
2) Алӣ қимати $S_A = [e_A]P$ –ро ҳисоб кард ба Валӣ равон мекунад.

3) Валӣ бошад, қимати $S_B = [e_B]S_A$ − ро ҳисоб карда, натиҷаашро ба Алӣ равон мекунад.

4) Алӣ қимати $V_A = [d_A]S_B$ −ро ҳисоб мекунад. Азбаски $d_A e_A \equiv 1(mod\ N_E)$ аст, пас $V_A = [e_B]P$ мешавад. Ин нуқтаро Алӣ ба Валӣ равон мекунад.

5) Валӣ бояд қимати $V_B = [d_B]V_A$ − ро ҳисоб кунад. Азбаски $d_B \cdot e_B = P$ аст, пас $V_B = P$ мешавад. Ҳамин тариқ Валӣ пайғоми аслро ба даст меорад.

Шакли схематикии ин алгоритм чунин аст.



11.Рамзӣ Ал-Ҷамол дар ХКЭ

Дилхоҳ системаи дар асоси ЛД сохташударо метавон содагӣ ба ХКЭ гузаронд. Принсипи асосии сохтани чунин криптосистема дар он аст, ки амали $y = g^x (mod\ p)$ ба $Y = [x]G$ иваз карда мешавад. Фарқият дар он аст, ки y–адад буда, Y-нуқтаи ХКЭ мебошад. Ҳамин тариқ гузариш аз нуқта ба адад талаб карда мешавад. Аз ҳама усули содаи ин гузаришҳо истифодаи абтсиссаи нуқта ба ҳисоб меравад.

Барои таҳияи криптосистема агар ХК ба таври тасодуфӣ интихоб карда шавад, он гоҳ аз нуқтаи назарӣ бехатарӣ устувортар мебошад.

Бигузор барои истифодабарандагони ягон шабака ХКЭ-и $E_p(a,b)$ ва нуқтаи G дар он интихоб карда шуда бошад, ки нуқтаҳои $G, [2]G, \dots, [n]G$ гуно-гун буда, барои ягон адади содаи q қимати $[q]G = O$ шавад.

Ҳар як истифодабарандаи U адади $c_U (0 < c_U < q)$–ро (калиди махфӣ) интихоб карда, қимати $D_U = [c_U]G$ –ро (калиди кушода) ҳисоб мекунад. Параметрҳои ХКЭ ва руйхати калидҳои кушода ба ҳамаи истифодабарандагон равон карда мешаванд.

Бигузор истифодабарандаи шабакаи мазкур Алӣ мехоҳад, ки ягон пайғомро ба истифодабаранадаи дигари шабака Валӣ равон кунад. Фарз мекунем, ки пайғом ба намуди адади $m < p$ тасвир карда шудааст.

1) Ибтидо Валӣ адади тасодуфии $c_B\ (0 < c_B < q) -$ ро интихоб карда, қимати $D_B = [c_B]G -$ ро ба Алӣ равон мекунад.

Алӣ амалҳои зеринро иҷро мекунад:

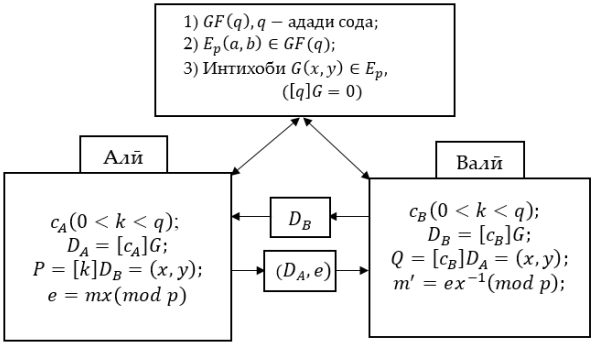
1) Адади тасодуфии $c_A\ (0 < c_A < q) -$ ро интихоб мекунад.
2) Қимати $D_A = [c_A]G, P = [c_A]D_B = (x, y)$ –ро ҳисоб мекунад.
3) Бо истифода аз $e = mx\ (mod\ p)$ –пайғомро рамзгузорӣ мекунад.
4) Пайғоми рамзгузошташуда, (D_A, e)-ро ба Валӣ равон мекунад

Валӣ пас аз оне ки қимати (D_A, e)-ро ба даст меорад, чунин амал мекунад:

2) Қимати $Q = [c_B]D_A = (x, y)$–ро ҳисоб мекунад.
3) Пайғоми ба дастовардаашро тавассути формулаи $m' = ex^{-1}\ (mod\ p)$ рамзкушоӣ мекунад.

Азбаски $Q = [c_B]D_A = [c_B]([c_A]G) = [c_A]([c_B]G) = [c_A]D_B = P$ аст, бинобар ин $m' = m$ мешавад.

Ба таври схематики ин алгоритм шакли зеринро дорад:



Барои душман координтаи x –и нуқтаи Q махфӣ мебошад, аз ин рӯ барои шикастани рамз он бояд қимати c_A –ро донад. Душман метавонад кушиши аз рӯйи D_A ҳисобкунии қимати c_A –ро кунад, аммо барои ин зарур аст, ки масъалаи $ЛД$-ро дар ХК ҳисоб кунад, лекин ин ғайриимкон аст.

Мисол. Амали рамзгузорӣ барои алгоритми Ал-Ҷамол дар ХКЭ-и зерин иҷро карда шавад.

$$E_p(a,b): y^2 = x^3 + x + 1\ (mod\ 11).$$

Дар ин ҷо $a = b = a, p = 11$ аст.

Ибтидо тартиби гурӯҳи нуқтаҳои ХКЭ-ро ҳисоб мекунем. Натиҷаи ин ҳисобкуниҳои фосилавӣ дар ҷадвали зерин гирд оварда шудаанд.

$\left(\frac{f(x)}{p}\right)$	x	x^2	$y^2 = x^3 + x + 1\ (mod\ 11)$		
1	0	0	1	$y_1 = 1$	$y_2 = -1 = 10$
1	1	1	3	$y_1 = 5$	$y_2 = -5 = 6$
0	2	4	0	$y_1 = 0$	$y_2 = 0$

1	3	9	9	$y_1 = 3$	$y_2 = -3 = 8$
1	4	5	3	$y_1 = 5$	$y_2 = -5 = 6$
-1	5	3	10	Мавҷуд нест	
1	6	3	3	$y_1 = 5$	$y_2 = -5 = 6$
-1	7	5	10	Мавҷуд нест	
1	8	9	4	$y_1 = 2$	$y_2 = -2 = 9$
-1	9	4	2	Мавҷуд нест	
-1	10	1	10	Мавҷуд нест	

Аз ҷадвал аён аст, ки миқдори нуқтаҳо ба $\#E_p(a,b) = 14$ баробар буда, тартиби нуқта адади сода намебошад, вале аз муносибати $n = \#E_p(a,b) = hq$ тартиби содаи зермаҷмӯи нуқтаҳо $q = 7$-ро ҳосил мекунем.

Акнун генератори ин маҷмӯъро ҳисоб мекунем. Азбаски $q < n$ аст, пас, нуқтаи тасодуфии G' –ро тавре интихоб мекунем, ки барои он $G = \left[\frac{n}{q}\right] G' \neq O$ шавад. Нуқтаи матлуб $G(0,1)$ мебошад. Қадами оянда муштариён чунин амал мекунанд:

Қабулкунанда (Валӣ):

Қадами 1. Калиди махфии $c_B = 5$ ($0 < c_B < q$) –ро интихоб мекунад.

Қадами 2. Калиди кушодаи $d_B = [c_B]G = [5](0,1)$ –ро ҳисоб мекунад.

$$c_B = 5 = 101_2 \rightarrow t = 3.$$
$$m_3 = 1, \quad Q = G = (0,1).$$

$$m_2 = 0,\ Q = [2](0,1) = \begin{vmatrix} \varphi(11) = 10 \\ \lambda = \frac{3\cdot 0^2+1}{2\cdot 1} = \frac{1}{2} = 1\cdot 2^{-1} = 6 \\ x = 6^2 - 2\cdot 0 = 3 \\ y = 6\cdot(0-3) - 1 = 6\cdot 8 - 1 = 3 \end{vmatrix} =$$

(3,3),

$$m_1 = 1, \qquad Q = [2](3,3) + (0,1)$$

$$= \begin{vmatrix} \lambda = \dfrac{3\cdot 3^2+1}{2\cdot 3} = \dfrac{28}{6} = \dfrac{6}{6} = 1 \\ x = 1^2 - 2\cdot 3 = -5 = 6 \\ y = 6\cdot(3-6) - 3 = 8 - 3 = 5 \end{vmatrix} =$$

$$= (6,5) + (0,1) = \begin{vmatrix} \lambda = \dfrac{1-5}{-6} = \dfrac{7}{5} = 7\cdot 5^{-1} = 8 \\ x = 8^2 - 6 - 0 = 3 \\ y = 8\cdot(6-3) - 5 = 8 \end{vmatrix} = (3,8).$$

Аз ин ҷо калиди кушода $d_B = [c_B]G = (3,8)$ мешавад.

Равонкунанда (Алӣ):

Қадами 1. Пайғоми додашударо ба шакли $m < p$ тасвир мекунад. Бигузор $m = 10$ бошад.

Қадами 2. Адади тасодуфии $c_A = 6$ $(0 < c_A < q)$ −ро интихоб мекунад.

Қадами 3. Қимати нуқтаи ХК $d_A = [c_A]G = [6](0,1)$ −ро ҳисоб мекунад.

$$c_A = 6 = 110_2 \to t = 3.$$
$$m_3 = 1, \quad Q = G = (0,1).$$

$m_2 = 1, \qquad Q = [2](0,1) + (0,1)$

$$= \begin{vmatrix} \varphi(11) = 10 \\ \lambda = \dfrac{3 \cdot 0^2 + 1}{2 \cdot 1} = \dfrac{1}{2} = 1 \cdot 2^{-1} = 6 \\ x = 6^2 - 2 \cdot 0 = 3 \\ y = 6 \cdot (0 - 3) - 1 = 6 \cdot 8 - 1 = 3 \end{vmatrix} =$$

$$=(3,3) + (0,1) = \begin{vmatrix} \lambda = \frac{1-3}{-3} = \frac{9}{8} = 9 \cdot 8^{-1} = 8 \\ x = 8^2 - 3 = 6 \\ y = 8 \cdot (3 - 6) - 3 = 64 - 3 = 6 \end{vmatrix} = (6,6).$$

$$m_1 = 0, \qquad Q = [2](6,6) = \begin{vmatrix} \lambda = \dfrac{3 \cdot 6^2 + 1}{2 \cdot 6} = \dfrac{109}{12} = \dfrac{10}{1} = 10 \\ x = 10^2 - 2 \cdot 6 = 0 \\ y = 10 \cdot (6 - 0) - 6 = 10 \end{vmatrix}$$

$$= (0,10).$$

Нуқтаи ХК $d_A = [c_A] = [6](0,1) = (0,10)$ мешавад.

Қадами 4. Қимати нуқтаи $P = [c_A]D_B = [6](3, \ 8)$ −ҳисоб мекунад.

$$m_3 = 1, \quad Q = D_B = (3,8).$$

$m_2 = 1, \qquad Q = [2](3,8) + (3,8)$

$$= \begin{vmatrix} \lambda = \dfrac{3 \cdot 3^2 + 1}{2 \cdot 8} = \dfrac{6}{5} = 6 \cdot 5^{-1} = 10 \\ x = 10^2 - 2 \cdot 3 = 6 \\ y = 10 \cdot (3 - 6) - 8 = 80 - 8 = 6 \end{vmatrix} =$$

$$= \quad (6,6) + (3,8) = \begin{vmatrix} \lambda = \frac{8-6}{3-6} = \frac{2}{8} = 2 \cdot 8^{-1} = 2 \cdot 8^9 = 2 \cdot 7 = 3 \\ x = 3^2 - 6 - 3 = 0 \\ y = 3 \cdot (6 - 0) - 6 = 1 \end{vmatrix} =$$

(0,1).

$$m_1 = 0, \qquad Q = [2](0,1) = \left| \begin{array}{c} \lambda = \dfrac{3 \cdot 0^2 + 1}{2 \cdot 1} = \dfrac{1}{2} = 1 \cdot 2^9 = 6 \\ x = 6^2 - 2 \cdot 0 = 3 \\ y = 6 \cdot (0 - 3) - 1 = 3 \end{array} \right| = (3,3).$$

Нуқтаи ХК $P = [c_A]d_B = (3,3)$ мешавад.

Қадами 5. Барои рамзгузорӣ абтсисаи нуқтаи P–ро истифода мебарад: $e = mx(mod\ p) = 10 \cdot 3(mod\ 11) = 8$.

Қадами 6. Матни рамзгузошташуда $(d_A, e) = ((0,10),8)$-ро ба Валӣ равон мекунад.

Қабулкунанда (Валӣ) баъди ба дастоварии пайғом:

Қадами 3. Қимати нуқтаи $Q = [c_B]d_A = (x,y) = [5](0,10)$ –ро ҳисоб мекунад.

$$m_3 = 1, \quad Q = G = (0,10).$$

$$m_2 = 0, \qquad Q = [2](0,10) = \left| \begin{array}{c} \varphi(11) = 10 \\ \lambda = \dfrac{3 \cdot 0^2 + 1}{2 \cdot 10} = \dfrac{1}{20} = 1 \cdot 20^{-1} = 5 \\ x = 5^2 - 2 \cdot 0 = 3 \\ y = 5 \cdot (0 - 3) - 10 = 8 \end{array} \right| = (3,8).$$

$$m_1 = 1, Q = [2](3,8) + (0,10) = \left| \begin{array}{c} \lambda = \dfrac{3 \cdot 3^2 + 1}{2 \cdot 8} = \dfrac{28}{5} = \dfrac{6}{5} = 6 \cdot 5^9 = 10 \\ x = 10^2 - 2 \cdot 3 = 6 \\ y = 10 \cdot (3 - 6) - 8 = 6 \end{array} \right| =$$

$$(6,6) + (0,10) = \left| \begin{array}{c} \lambda = \dfrac{10 - 6}{0 - 6} = \dfrac{4}{5} = 4 \cdot 5^9 = 4 \cdot 9 = 3 \\ x = 3^2 - 6 - 0 = 3 \\ y = 3 \cdot (6 - 3) - 6 = 3 \end{array} \right| = (3,3).$$

Нуқтаи ХК $Q = [c_B]d_A = (3,3)$ мешавад.

Қадами 4. Пайғомро рамзкушоӣ мекунад.

$$m' = ex^{-1}(mod\ p) = 8 \cdot 3^{-1}(mod 11) = 8 \cdot 4 = 10.$$

Азбаски $m' = m = 10$ аст, пас пайғом дуруст рамзкушоӣ карда шудааст.

Роҳи дигари татбиқи методи Ал-Ҷамол дар ХКЭ дар он аст, ки на аз абтсиссаи нуқта, балки аз худи нуқта истифода бурда мешавад. Дар ин усул параметрҳои кушода инҳо мебошанд:

1) Майдони охирноки F_q.
2) Муайянкунии ХК E дар он.
3) Нуқтаи асосӣ (ташкилкунанда) B дар он (донистани миқдори нуқтаҳо N дар E шарт намебошад).

Ҳар як истифодабаранда, ягон адади тасодуфии c –ро интихоб карда ҳамчун калиди махфӣ нигоҳ медорад. Сипас, дар асоси ин калиди махфӣ калиди ошкори $[c]B$– ро ҳисоб мекунад.

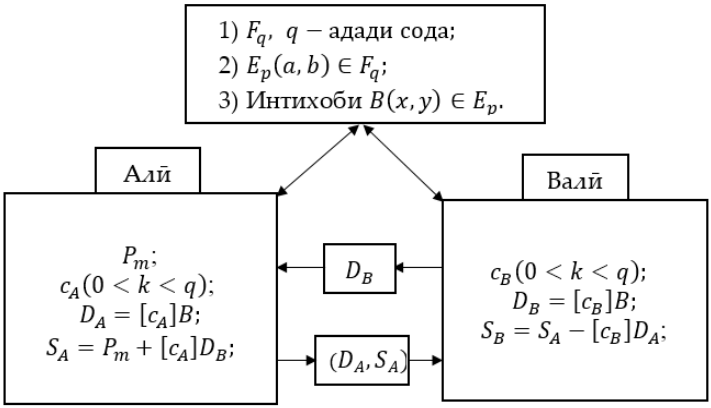
Масалан, барои ба Валӣ фиристонидан пайғоми P_m Алӣ адади тасодуфии c_A –ро интихоб карда, ҷуфти нуқтаҳои $\{[c_A]B,\ P_m + [c_A] \cdot [c_B]B\}$ –ро ба Валӣ равон мекунад. Дар ин ҷо $[c_B]B -$ калиди кушодаии Валӣ мебошад. Барои хондани ин мактуб Валӣ нуқтаи аввалаи ба даст овардаашро ба калиди махфии худ c_B зарб карда, аз нуқтаи дуюм қимати онро тарҳ мекунад.

$$P_m + [c_A] \cdot [c_B]B - [c_B] \cdot ([c_A]B) = \ P_m.$$

Ҳамин тариқ Валӣ пайғоми равонкардашударо мехонад.

Мисол. Ҳолати $p = 751, E_p(a,b), G = (0,376)$–ро дида мебароем, ки ба ХКЭ-и $y^2 = x^3 - x + 188$ мувофиқ меояд. Бигузор Алӣ мехоҳад пайғомеро, ки ба нуқтаи $P_m = (562,201)$ мувофиқ аст ба Валӣ равон кунад. Алӣ ҳосил мекунад $[386](0,376) = (676,558)$ ва $(562,\ 201) + [386](201,5) = (385,328)$. Дар ин ҷо $[c_B]B = (201,5)$ калиди махфии Валӣ мебошад. Ҳамин тариқ, Алӣ бояд пайғоми $\{(676,\ 558),(385,328)\}$–ро ба Валӣ равон кунад.

Шакли схематикии ин алгоритм чунин мебошад:



12.ИЭР дар ХКЭ (стандарти ГОСТ Р34.10-2001)

Ба сифати стандарти байналмилали алгоритми амрикоии имзоҳои рақами дар ХКЭ (ECDSA) қабул карда шудааст. Дар стандарти мазкур ХКЭ дар майдони характеристикааш ба ду баробар истифода бурда мешавад. Лекин устувории криптографӣ дар чунин ХКЭ суст мебошад, бинобар ин, дар ин ҷо ИЭР-ро дар ХКЭ-и,

ки дар майдонҳои характеристикаашон калонтар дода шудаанд дида мебароем.

Дар Федратсияи Россия бошад, расман стандарти ИЭР дар майдонҳои характеристикаашон калон ГОСТ Р34.10-94 қабул карда шудааст. Алгоритми ГОСТ Р34.10-2001 стандарти пешинаи ГОСТ Р34.10-94-ро иваз кард, ки дар асоси ЛД сохта шуда буд. Дар стандарти нав ба сифати ЛД аз амали композитсияи нуқтаҳо истифода бурда шудааст. Барои мубодилаи итилоот истифодабарандагон ХКЭ-и умумӣ $E_p(a,b)$ ва нуқтаи G дар онро интихоб мекунанд, ки нуқтаҳои $G, [2]G, \dots, [n]G$ гуногун буда, барои ягон адади содаи q қимати $[q]G = O$ мешавад.

Барои интихоби ХК ва нуқтаи G (дар он) бояд якчанд масъалаҳои ёрирасон ҳал карда шаванд. Пеш аз ҳама бояд миқдори нуқтаҳо дар ХКЭ ҳисоб карда шавад. Агар N миқдори нуқтаҳо дар ХКЭ-и $E(F_p)$ бошад, он гоҳ бояд барои он шартҳои зерин иҷро гарданд:

$$\begin{cases} p + 1 - 2\sqrt{p} \le N \le p + 1 + 2\sqrt{p} & (1) \\ G \in E(F_p) \Longrightarrow N \cdot G = O. & (2) \end{cases}$$

Ҳамин тариқ, барои ҷудо намудани ададҳои зиёдатии байни интервали $(p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p})$ метавон иҷроиши шарти 2-ро барои нуқтаҳои гуногуни G истифода кард. Ададии ягонаи боқимонда тартиби матлуби хати каҷ ба шумор меравад.

Барои ба даст овардани устувории рамзгузории системаи имзои электронӣ рақамӣ бояд чунин шартҳо иҷро шаванд:

1) Тартиби нуқтаи G, ки дар системаи ИЭР истифода мешавад, бояд адади содаи $n\,(n > max\{2160\ ,4\sqrt{p}\})$ бошад.

2) Бояд $N \neq p$ ва $N \neq p + 1$ шавад, дар ин ҷо N –тартиби хати каҷ ба ҳисоб меравад.

3) Шарти $p^k \neq 1(mod\ n)$ барои ҳамаи $k = 1,\ldots,C$ (дар ин ҷо С бояд чунон калон бошад, ки ҳисобкунии логарифми дискретӣ (дар $F_p c$) дар вақти гузошташуда номумкин гардад) бояд санҷида шавад.

Қайд. *Айни замон қимати С = 20 кифоя ба ҳисоб меравад.*

Пас аз оне ки тартиби N-и хати каҷ муайян шуд, бояд тақсимкунандаи содаи калони тартиби n –и хати каҷ ёфта шавад. Чунин тақсимкунанда мумкин аст, ки пайдо нашавад. Дар ин ҳолат бояд амали интихоби хати каҷ то он лаҳзае, ки ҳама шартҳо иҷро нашаванд такрор меёбад. Ҷустуҷӯи адади n метавонад ба зарбкунандаҳо ҷудо кардани адади *N ва ё* исботи сода будани адади *n-ро* талаб кунад.

Нуқтаи G-ро метавон бо чунин тарз интихоб кард: Нуқтаи тасодуфии $G' \in E(F_p)$ -ро интихоб карда, қимати ифодаи $G = \frac{N}{n} \cdot G'$ –ро ҳисоб мекунем: Агар $G \neq O$ шавад, пас нуқтаи матлуб ёфт шудааст, вагарна (агар $G = O$ бошад) дигар нуқтаи G'-ро интихоб мекунем.

Пас аз интихоби параметрҳои лозимӣ ҳар як истифодабарандаи U адади $c_U (0 < c_U < q)$ –ро (калиди махфӣ) интихоб карда, қимати $D_U = [c_U]G$–ро (калиди

кушода) ҳисоб мекунад. Параметрҳои ХКЭ ва руйхати калидҳои кушода ба ҳамаи истифодабарандагон равон карда мешаванд.

Барои ҳосилкунии ИЭР-и пайғоми $\tilde{m}$ Алӣ амалҳои зеринро иҷро мекунад:

1) Ҳисобкунии қимати ҳэш-функсия $h = H(\tilde{m}) -$ и пайғом.
2) Интихоби ададй тасодуфии $c_A (0 < c_A < q)$.
3) Ҳисобкунии қимати нуқтаи ХКЭ $Y_A = [c_A]G = (x_p, y)$.
4) Ҳисобкунии қимати $r = x_p \ mod \ q$. Агар $r = 0$ шавад, ба қадами 2 бармегардад.
5) Ҳисобкунии қимати $s = (c_A h + r \cdot x_U) \ mod \ q$. Агар $s = 0$ шавад, ба қадами 2 бармегардад.
6) Ба дастоварии ИЭР ба намуди $\xi = r||s$ ҳам-чун якҷоякунии ду вектори 256 битаи r ва s.

Барои тафтиши пайғоми имзогузоштаи $(\tilde{m}, \xi)$ дилхоҳ истифодабарандае, ки калиди Y_A–ро медонад чунин амал мекунад:

1) Қимати $h = H(\tilde{m})$–ро ҳисоб мекунад.
2) Дурустии шарти $0 < r, s < q -$ ро месанҷад, агар он иҷро гардад ба қадами навбати мегузарад, вагарна имзо ғайриҳақиқӣ дониста мешавад.
3) Қиматҳои $u_1 = s \cdot h^{-1} \ mod \ q$ ва $u_2 = -r \cdot h^{-1} \ mod \ q$ –ро ҳисоб мекунад.
4) Қимати $P = [u_1]G + [u_2]Y_A = (x_p, y)$–ро ҳисоб мекунад, агар $P = O$ шавад, имзо ғайриҳақиқӣ дониста мешавад.
5) Агар $x_p \ mod \ q = r$ шавад, имзо қабул карда мешавад, дар акси ҳол, имзо ғайриҳақиқӣ дониста мешавад.

Мувофиқи стандарт бояд ҳэш-функсияи дар ГОСТ Р34.11.94 муайяншударо истифода бурда шавад, ки дарозии он аз 256 бит зиёд намебошад. ХК тавасути коэфитсиентҳои a ва b ё тавасути инвариант $j(E)$ дода мешавад, p-модули ХКЭ буда, бояд шарти $p > 2^{255}$ –ро қаноат кунонад. Миқдори нуқтаҳои ХКЭ (адади q), бояд теоремаи Хассе $q \neq p$ ва $2^{254} < q < 2^{256} -$ ро қаноат кунонад.

Мисол. ИЭР-ро аз рӯйи стандарти ГОСТ Р34.10-2001 ва ҳэш-функсияе, ки қаблан дар боби 8 (мавзӯъи 1, мисоли 2.) мавриди баҳс қарор гирифта буд, ҳисоб мекунем.

Бигузор ХКЭ чунин шаклро дошта бошад:

$$E_p(a,b):\ y^2 = x^3 + x + 1\ (mod\ 11).$$

Дар ин ҷо $a = b = 1, p = 11$ мебошад. Тартиби зергурӯҳи нуқтаҳои ХК $q = 7$ буда, нуқтаи $G = (0,1)$ генератори гурӯҳ ба ҳисоб меравад. Пайғоми мавриди назар бошад $\tilde{m}$ = “маша” мебошад.

Равонкунанда чунин амал мекунад:

Қадами 1. Интихоби адади махфии x_A $(0 < x_A < q)$: масалан $x_A = 4$.

Қадами 2. Ҳисобкунии калиди кушод: $Y_A = [x_A]G = (6,5)$.

Қадами 3. Ҳисобкунии қимати ҳэш-функсия: $h = H(\tilde{m}) = 4$.

Қадами 4. Интихоби адади тасодуфии c_A $(0 < c_A < q)$: масалан, $c_A = 5$.

Қадами 5. Ҳисобкунии қимати нуқтаи ХКЭ: $P = [c_A]G = (3,8)$.

Қадами 6. Ҳисобкунии қимати ифодаҳои:

$r = x \; mod \; q = 3 \; mod \; 7 \neq 0$

$s = (c_A h + r \cdot x_A) mod \; q = (25 + 12) mod \; 7 = 2 \neq 0.$

Қадами 7. Ба шакли $(r, s) = (3, 2)$ имзо гузоштани пайғоми $\tilde{m}$.

Қабулкунандаи ИЭР бошад, баъди ба даст оварии имзо барои тафтиши он чунин амал мекунад:

Қадами 1. Ҳисобкунии қимати ҳэш-функсия: $h = H(\tilde{m}) = 5$.

Қадами 2. Санҷиши дурустии шартҳои:

$$0 < (r = 3) < 7, \quad 0 < (s = 2) < 7.$$

Қадами 3. Ҳисобкунии қимати ифодаҳои зерин:

$$u_1 = s \cdot h^{-1} \; mod \; q = 2 \cdot 5^{-1} \; mod \; 7 = 2 \cdot 3 \; (mod \; 7) = 6,$$

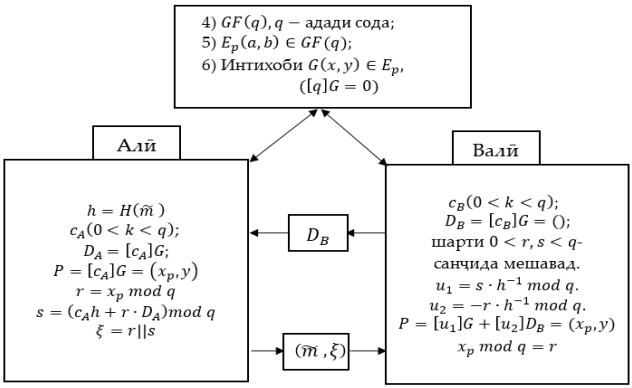
$$u_2 = -r \cdot h^{-1} \; mod \; q = -3 \cdot 5^{-1} \; mod \; 7 = 4 \cdot 3 \; mod \; 7 = 5.$$

Қадами 4. Ҳисобкунии қимати нуқтаи ҲК:

$$P = [6](0,1) + [5](6,5) = (3,8).$$

Қадами 5. Санҷиши дурустии имзо. Азбаски $x \; mod \; q = 3 = r$ аст, пас имзо қабул карда мешавад.

Ба таври схематики ин алгоритм шакли зеринро дорад:



Саволҳо барои мустаҳкамкунӣ

1. ХКЭ чист?
2. ХК сингулярӣ гуфта чӣ гуна ХК-ро меноманд?
3. Коэффитсиентҳои ХКЭ аз рӯйи инвариант чӣ тавр муайян карда мешаванд?
4. Чӣ тавр ду нуқтаи ХКЭ-ро ҷамъ кардан мумкин аст?
5. Чӣ тавр тартиби нуқтаҳои ХКЭ муайян карда мешавад?
6. Барои таҳия кардан гурӯҳи нуқтаҳои ХКЭ аз кадом қоидаҳо истифода бурда мешавад?
7. Амали композитсияи нуқтаҳо чӣ гуна амал аст?
8. Логарифми дискретӣ дар гурӯҳи нуқтаҳои ХК чӣ тавр муайян карда мешавад?
9. Чӣ тавр методҳои рамзгузории бо калидҳои кушодаро метавон дар ХКЭ татбиқ кард?
10. ИЭР –ро дар ХКЭ чӣ тавр ҳисоб мекунанд?

Манбаъҳои истифодашуда

[1] Аграновский А.В. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади.- М.: Солон-Пресс, 2009, 256 с.

[2] Айерленд К. Классическое введение в современную теорию чисел. / К. Айерленд, М. Роузен. - М.: Мир, 1987, 428 с.

[3] Акритас А. Основы компьютерной алгебры и приложениями. /

[4] А. Акритас. - М.: Мир, 1994, 544 с.

[5] Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие // М.: Гелиос АРВ, 2005. 480 с.

[6] Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — 176 с. — ISBN 978-5-9912-0182-7

[7] Богопольский О.В. Алгоритмическая теория чисел и элементы криптографии. / О.В. Богопольский.- Спецкурс для студентов НГУ, Новосибирск, 2005, 35 с./http://math.nsc.ru/ bogopolski/Articles/SpezkNumber.pdf

[8] Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия. Телеком, 2001. – 120с.

[9] Березюк Н.Т., Андрущенко А.Г., Мощицкий С.С. и др. Кодирование информации (двоичные коды). / Под ред. Н.Т. Березюка. – Харьков: Вища школа, 1978. – 252 с.

[10] Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986.
[11] Боревич З.И. Теория чисел. / З.И. Боревич, И.Р. Шафаревич. - 3-е издание, М.: Наука, 1985, 504 с.
[12] Борисов В.А., Калмыков В.В., Ковальчук Я.М. и др. Радиотехнические системы передачи информации. / Под ред. В.В. Калмыкова. – М.: Радио и связи, 1990. – 304с.
[13] Брейсуэлл Р. Преобразование Хартли. / Пер. с английского А.И. Папкова. – М.: Мир, 1990. – 175с.
[14] Бураченко Д.Л., Клюев Н.Н., Коржик В.И., Финк Л.М. и др. Общая теория связи. / Под ред. Л.М.Финка. – Л.: ВАС, 1970. – 412с.
[15] Ван дер Варден Б.Л. *Алгебра.*/ Б.Л.ван дер Варден. - изд.2, М.: Наука, 1979, 623 с.
[16] Вальд А. Статистически решающие функции. Позиционные игры.. – М.: Наука, 1967. – 522с.
[17] Варакин Л. Е. Теория систем сигналов. – М.: Сов. радио, 1978. – 304с.
[18] Васильев К. К., Новосельцев Л. Я., Смирнов В. Н. Основы теории помехоустойчивых кодов: Учеб. пособие. – Ульяновск: УлГТУ, 2000. – 91с.
[19] Васильев К.К. Методы обработки сигналов: Учебное пособие. – Ульяновск: УлГТУ, 2001. – 80с.
[20] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии/ О.Н. Василенко. - МЦНМО, 2003, 326 с.

[21] Вельщенбах М. Криптография на C и C++ в действии: учебное пособие / М. Вельщенбах. - М.: Триумф, 2008, 464 с.
[22] Винер Н.Я. Математика. – М.: Наука, 1967. – 300с.
[23] Галлагер Р. Теория информации и надежная связь / Пер. с англ. под ред. М.С. Пинскера и Б.С. Цыбакова. – М.: Сов. радио, 1974. – 720с.
[24] Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 – х кн. – М.: Энергоатомиздат, 1994 г. – 576 с.
[25] Глушков В.А., Нестеренко А.Г. Теория электрической связи. Часть 1. Дискретные сигналы. Учебное пособие. Ульяновск: УФВУС, 2003. – 96с.
[26] Глушков В.А., Нестеренко А.Г., Попов Н.А. Телекоммуникационные системы. Учебное пособие. Часть 1. Аналоговые и цифровые сигналы. – Ульяновск: УВВИУС, 2007. – 131с.
[27] Глушков В.А., Нестеренко А.Г., Попов Н.А. Теория электрической связи. Учебное пособие. Часть 2. Помехоустойчивость. – Ульяновск: УВВИУС, 2007. – 78с.
[28] Глушков В.А., Нестеренко А.Г., Чикалев С.Б. Телекоммуникационные системы. Учебное пособие. Часть 2. Принципы построения систем связи. – Ульяновск: УВВИУС, 2007. – 118с.
[29] Гоноровский И.С., Демин М.П. Радиотехнические цепи и сигналы. – М.: Радио и связь, 1994. – 480с.

[30] Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций // М.: Гелиос АРВ, 2008. 288 с. ISBN 978-5-85438-177-2.

[31] ГОСТ 28147 – 89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преоб-разования. М. Госстандарт СССР.

[32] Девянин П. Н. Модели безопасности компьютерных систем // М.: Издательский центр «Академия», 2005. 144 с. ISBN 5-7695-2053-1.

[33] Диффи У. Хеллман М. Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. 1979. Т. 67. № 3. С 109.

[34] Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 336с.

[35] Захаров В.М. Вычисления в конечных полях: уч.-метод. пособие / В.М. Захаров, Б.Ф. Эминов. - Казань: КГТУ им. А.Н.Туполева, 2010, 132 с.

[36] Земор Ж. Курс криптографии // М.-Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. 256 с. ISBN 5-93972-510-4.

[37] Ишмухаметов Ш.Т. Методы факторизации натуральных чисел/ Ш.Т.Ишмухаметов. - Казань, 2012, 189 с.

[38] Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. - М.: ТВП, 2001, 260 с.

[39] Корешков Н.А. Теория чисел./Н.А. Корешков. - Уч.-мет. пособие, Казань, КФУ, 2010, 35 с.
[40] Кормен Т. Алгоритмы: построение и анализ /Т. Кормен, Ч. Лейзерсон, Р. Ривест. - М.: МЦНМО, 1999.
[41] Лазарева С.В. Математические основы криптологии: тесты простоты и факторизация / С.В. Лазарева, А.А. Овчинников. Учебное пособие, Санкт-Петербург, СПбГУАП, 2006, 65 с.
[42] Лидл Р. Конечные поля /Р. Лидл,Г. Нидеррайтер.- Т. 1, 2. М.: Мир, 1988, 428 с.
[43] Молдовян А. А., Молдовян Н. А. Молдовян П. А. Псевдовероятностные скоростные блочные шифры для программной реализации // Кибернетика и системный анализ. Киев, 1997. № 4. С. 133 – 141
[44] Молдовян А.А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: Издательство "Лань" , 2001. – 224 с, ил.
[45] Молдовян Н.А. Криптография. От примитивов к синтезу алгоритмов / Н.А.Молдовян, А.А. Молдовян,М.А. Еремеев. - БХВ-Петербург, 2004, 446 с.
[46] Нестеренко Ю.В. Теория чисел/ Ю.В. Нестеренко. - Москва, Изд.Центр Академия, 2008, 273 с.
[47] Оков И.Н. Криптографические системы защиты информации. – СПб.: ВУС, 2001. – 236с.
[48] Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, Профессионал, Санкт-Петербург, 2005, 479 с.

[49] Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации // Учебное пособие для вузов. — М.: Горячая линия-Телеком, 2005. — 229 с.
[50] Сизый С.В. Лекции по теории чисел: учебное пособие для математических специальностей / С.В. Сизый.- Екатеринбург, УрГУ, 1999, 136 с.
[51] Саломаа А. Криптография с открытым ключем. – М.: Мир, 1996 – 318 с.
[52] Чандрасекхаран К. Введение в аналитическую теорию чисел/ К. Чандрасекхаран.-М.- Мир, 1974, 187 с.
[53] Черемушкин А.В. Лекции по арифметическим функциям в криптографии / А.В. Черемушкин.- М.: МЦНМО, 2002, 103 с.
[54] Шаньгин Ф.Ф. Защита компьютерной информации: эффективные методы и средства /Ф.Ф. Шаньгин.- М.:ДМК, 2008, 542 с.
[55] Шеннон К. Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 333 – 402
[56] Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си // М.: Триумф. 2002. 816 с. ISBN 5-89392-055-4.
[57] Agrawal M. PRIMES is in P / M.Agrawal, N.Kayal, N.Saxena.- Annals of Mathematics.- 2004, v.160, p. 781-793.
[58] Atkin A. Prime sieves using binary quadratic forms/ A. Atkin, D. Bernstein.- http://cr.yp.to/papers/ primesieves-19990826.pdf

[59] Berstein D. ECM using Edwards curves/ D. Berstein, P. Birkner, T.Lange, C. Peters.-2008, p.1-40 http://eecm.cr.yp.to/eecm-20100616.pdf
[60] Berstein D. Faster addition and doubling on elliptic curves./ D. Berstein, T.Lange. in AsiaCrypt' 2007, p.29-50
[61] Berstein D. Explicit-formulas Database./ D. Berstein, T.Lange. 2007 http:// hyperelliptic.org/EFD
[62] Berstein D. Starfish on Strike/ D. Berstein, P. Birkner, T.Lange, C. Peters.- LATINCRYPT 2010, edited by Michel Abdalla and Paulo S. L. M. Barreto. Lecture Notes in Computer Science 6212. Springer, 2010, p.61-80
[63] Boldyreva A. Efficient Thresholf Signature, Multisignature and Blind Signature Schemes based on Diffie-Hellman-Group Signature Scheme. Cryp- to'2003, Lect.Not.Comp.Sci., p.31-46
[64] Boneh D., Franklin M. Identity based encrryption from the Weil pairing. In J.Killan, editor, Proceeding of Crypto'2001, volume 2139, Lect.Notes in Comp.Sci., 2001, p.213-229
[65] Brent R.P. Some integer factorization algorithms using elliptic curves/ R.P. Brent.- Austral.Comput.Sci.Comm, 1986, v.8, p. 149-163.
[66] Buhler J.P. Factoring integers with the number field sieve / J. P. Buhler, H. W. Lenstra, C. Pomerance.- in The Developement of the Number Field Sieve, Springer-Verlag, Berlin, Germany, 1993, p. 50-94.

[67] Chaum D. Zero-knowledge undeniable signatures. In I.Damgard, editor, Advances in Cryptology-Crypto'90, Lect.Not.Comp.Sci., v.740, 1992, p.89-105
[68] Cocks C. An identity based encryption scheme based on quadratic residues. Cryptography and Coding, 2001.
[69] Cohen H. *A* course in computational algebraic number theory / H. Cohen.- Springer-Verlag, Berlin, 1993, 545 p.
[70] Crandall R. The prime numbers: a computational perspertive / R. Crandall, C. Pomerance.- sec.ed. Springer-Verlag, Berlin, 2005, 604 p.
[71] Dunham W. Euler *:* The Master of Us All. Mathematical Association of America, 1999, 185 p.
[72] Edwards H.M. A normal form for elliptic curves./ H.M. Edwards.-Bull. Amer. Math. Soc. 44 (2007), p. 393-422
[73] Elkenbracht-Huising M. An implementation of the Number Field Sieve / M. Elkenbracht-Huising.- Experimental Mathematics, 1996, v.5, p. 231—253.
[74] Gardner M. A new kind of cipher that would take millions years to break / M. Gardner.- Sci. Amer. 1977, p. 120-124.
[75] Granville A. Smooth numbers: Computational number theory and beyond/ A. Granville.- Proc. of MSRI workshop, 2004, 268-363
[76] Hackmann P. Elementary Number Theory / P. Hackmann.- HHH Publ, 2007, 411 p.
[77] Ishmukhametov S.T.On a number of products of two primes./ S.T. Ish- mukhametov, R. Rubtsova.-Abstracts of

International Conference dedicated to 100-anniversary of V. V. Morozov, Kazan, 2011

[78] Joux A. A one round protocol for tripartite Diffie-Hellman. / A. Joux.- Algorithmic Number Theory: 4-th International Symposium, ANT-IV, Lecture Notes in Computer Science, v.1838(2000), Springer-Verlag, p. 385-393.

[79] Lenstra H.W. Factoring integers with elliptic curves / H.W. Lenstra.- Ann.Math. v.126 (1987), p. 649-674.

[80] Lenstra A. The Development of the Number Field Sieve / A. Lenstra and H. Lenstra (eds.).- Lect.Not.in Math.1554, Springer-Verlag, Berlin, 1993, 139 p.

[81] Longa P. ECC Point Arithmetic Formulae (EPAF): Jacobian coordinates/ P. Longa, C. Gebotus. In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010), 2010.

[82] Menezes A. Reducing Elliptic Curve Logarithms to a Finite Field / A. Menezes, T. Okamoto, S. Vanstone.- IEEE Trans. Info. Theory, v.39, 1993, p. 1639-1646.

[83] Menezes A. Elliptic Curve Public Key Cryptosystems / A. Menezes.- 1993, 144 p.

[84] Montgomery P.L. Speeding the Pollard and Elliptic Curve Methods of Fac- torization./P.L. Montgomery.- Mathematics of Computation, v.48, iss.177, 1987, p.234-264.

[85] Pollard J.M. Theorems on factorization and primality testing / J.M. Pollard.

[86] Proc.Cambridge Phil.Society. 1974, v.76, p. 521-578.

[87] Pomerance C. Smooth Numbers and the Quadratic Sieve / C. Pomerance. - MSRI publications, v.44 - 2008, p. 69-82.
[88] Shoup V. A Computational Introduction to Number Theory and Algebra / V. Shoup. - Cambridge University Press, Sec.Edition, 2005, 600 p. http://shoup.net/ntb/
[89] Venturi D. Lecture Notes on Algorithmic Number Theory./ D. Venturi. - Springer-Verlag, New-York, Berlin, 2009, 217 p.
[90] Washington L. Elliptic Curves Number Theory and Cryptography /L. Washington. - Series Discrete Mathematics and Its Applications, Chapman & Hall/CRC, second ed. 2008, 524 p.

Манбаъҳои интернетӣ

1. http :// skyscraper.fortunecity.com/disk/786
2. http : //www.security.ru/
3. http://www.fssr.ru
4. http://www.confident.ru/
5. http://www.quardralay.com/www/Crypt/
6. http : //www.rsa.com/
7. http : //www.xaker.ru
8. http://citforum.ru/security/
9. www.cryptography.ru
10. http://astu.secna.ru
11. http://www.cryptography.strongdisk.ru/
12. www.security.ukrnet.net

Ба чопхона 04.10.2017 . супорида шуд. Ба чопаш 07.10.2017 .

имзо шуд. Андозаи 60х84 1/16. Ҷузъи чопӣ 25,1.

Адади нашр 500. Китоб дар чопхонаи

«РТСУ» нашр шудааст. 734025,

ш. Душанбе