КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра системного анализа и информационных технологий

Е.В. РАЗИНКОВ

ТЕОРИЯ ЧИСЕЛ И АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ

Конспект лекций

Казань – 2020

УДК 003.26.09
ББК В

Принято на заседании кафедры системного анализа
и информационных технологий
Протокол № __ от _____2020 года

Рецензенты:
кандидат физико-математических наук,
доцент кафедры теоретической кибернетики КФУ **В.С. Кугураков;**
кандидат физико-математических наук,
доцент кафедры анализа данных и исследования операций КФУ **В.В. Бандеров**

Разинков Е.В.
Теория чисел и асимметричная криптография / Е.В. Разинков. –
Казань: Казан. ун-т, 2020. – 53 с.

В современном информационном обществе особенно важную роль играет защита информации. Асимметричное шифрование применяется во многих важных криптографических протоколах, используемых миллиардами пользователей каждый день. Изучение теории чисел необходимо для понимания принципов построения асимметричных криптографических алгоритмов, оценок их стойкости к различным криптоаналитическим атакам.

Настоящее учебное пособие адресовано студентом таких направлений, как «Информационная безопасность» и «Фундаментальная информатика и информационные технологии».

Оглавление

МАТЕМАТИЧЕСКИЕ ОСНОВЫ

В данной главе приводятся сведения из теории чисел и линейной алгебры, необходимые для понимания принципа работы алгоритма RSA, возможных уязвимостей и атак.

1.1 Кольца, группы и поля

Определение 1. Кольцо – множество с определенными на нем операциями сложения и умножения, обладающее следующими свойствами:

- Замкнутость относительно сложения:

$$\forall a, b \in R : a + b \in R;$$

- Ассоциативность сложения:

$$\forall a, b, c \in R : (a + b) + c = a + (b + c);$$

- Обладает единицей по сложению:

$$\exists 0 \in R, \forall a \in R : 0 + a = a + 0 = a;$$

- Каждый элемент обладает обратным по сложению:

$$\forall a \in R, \exists (-a) : a + (-a) = (-a) + a = 0;$$

- Сложение коммутативно:

$$\forall a,b \in R : a+b = b+a;$$

- Замкнутость относительно умножения:

$$\forall a,b \in R : a \cdot b \in R;$$

- Ассоциативность умножения:

$$\forall a,b,c \in R : (a \cdot b) \cdot c = a \cdot (b \cdot c);$$

- Обладает единицей по умножению:

$$\exists 1 \in R, \forall a \in R : 1 \cdot a = a \cdot 1 = a;$$

- Умножение и сложение связаны законом дистрибутивности:

$$\forall a,b,c \in R : (a+b) \cdot c = a \cdot c + b \cdot c.$$

Если умножение в кольце обладает свойством коммутативности, то кольцо называется коммутативным.

Определение 2. Группа – множество с определенной на нем операцией, обладающее следующими свойствами:

- Замкнутость относительно операции:

$$\forall a,b \in G : a \cdot b \in G;$$

- Обладает единицей:

$$\exists 1 \in G, \forall a \in G : 1 \cdot a = a \cdot 1 = a;$$

- Ассоциативность операции:

$$\forall a,b,c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c);$$

- Каждый элемент обладает обратным:

$$\forall a \in G, \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Если групповая операция называется умножением, то группа называется мультипликативной, если сложением – аддитивной.

Если групповая операция обладает свойством коммутативности, то группа называется коммутативной (абелевой).

Определение 3. Полем называется множество $(F, \cdot, +)$ с двумя операциями, обладающее следующими свойствами:

- $(F, +)$ – коммутативная группа с единичным элементом 0.
- $(F \backslash \{0\}, \cdot)$ – коммутативная группа с единичным элементом 1.
- Операции сложения и умножения удовлетворяют закону дистрибутивности:

$$(a+b)c = ac + bc.$$

Примеры полей:

- Множество действительных чисел $\mathbb{R}$.
- Множество рациональных чисел $\mathbb{Q}$.
- Множество комплексных чисел $\mathbb{C}$.

1.2 Наибольший общий делитель

Определение 4. Наибольшим общим делителем целых чисел a и b называется такое натуральное число c, что a делится на c, b делится на c и не существует такого натурального $d > c$, что a делится на d, b делится на d.

Если НОД$(a,b) = 1$, числа a и b называются взаимно простыми.

1.2.1 Алгоритм Евклида

Теорема 1. Пусть a, b – целые числа, а $r \in \mathbb{Z}$ – остаток от деления a на b, $0 \leq r < |b|$:

$$a = q \cdot b + r.$$

Тогда НОД$(a,b) =$ НОД(b,r).

Алгоритм Евклида позволяет эффективно вычислить НОД(a,b). Положим $r_0 = a$, $r_1 = b$, получим:

$$r_0 = q_1 \cdot r_1 + r_2.$$

Так как НОД$(r_0,r_1) =$ НОД(r_1,r_2), повторим данную операцию для r_1 и r_2:

$$r_1 = q_1 \cdot r_2 + r_3.$$

Будем продолжать процесс для все пар $(r_2,r_3),(r_3,r_4),...,(r_{n-1},r_n)$, пока не будет выполнено равенство

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

Число r_n является наибольшим общим делителем чисел a и b.

1.2.2 Расширенный алгоритм Евклида

Расширенный алгоритм Евклида позволяет эффективно вычислить целые числа s и t такие, что

$$s \cdot a + t \cdot b = \text{НОД}(a,b).$$

1.3 Арифметика остатков

Определение 5. Пусть a, b – целые числа, а n – натуральное число. Будем говорить, что a сравнимо с b по модулю n:

$$a \equiv b \pmod{n},$$

если $(a-b)$ делится на n.

1.3.1 Кольцо вычетов $\mathbb{Z}_n$

Определение 6. Пусть n – натуральное число. Через $\mathbb{Z}_n$ обозначим множество возможные остатков от деления на n:

$$\mathbb{Z}_n = \{0, 1, ..., n-1\}.$$

Определим операции сложения и умножения на множестве $\mathbb{Z}_n$:

- Сложение:

$$a + b \pmod{n} = (a+b) \mod n;$$

- Умножение:

$$a \cdot b \pmod{n} = (a \cdot b) \mod n.$$

Множество $\mathbb{Z}_n$ с заданными на нем операциями сложения и умножения является кольцом.

Определение 7. Множество $\mathbb{Z}_n$ с заданными на нем операциями сложения и умножения называется кольцом вычетов по модулю n.

1.3.2 Мультипликативная группа $\mathbb{Z}_n^*$

Теорема 2. Пусть a – целое, а n – натуральное. Уравнение

$$ax = 1 \pmod{n}$$

имеет решение тогда и только тогда, когда НОД$(a,n) = 1$.

Определение 8. Через $\mathbb{Z}_n^*$ обозначим множество элементов $\mathbb{Z}_n$ взаимно простых с n:

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n | \text{НОД}(z,n) = 1\}.$$

Множество $\mathbb{Z}_n^*$ является мультипликативной группой.

1.3.3 Китайская теорема об остатках

Рассмотрим систему уравнений:

$$\begin{cases} x = a_1 \pmod{m_1} \\ x = a_2 \pmod{m_2} \\ \dots \\ x = a_n \pmod{m_n} \end{cases}$$

Эта система имеет единственное решение относительно x по модулю M, $M = \prod_{i=1}^{n} m_i$, тогда и только тогда, когда для любых $i \neq j$:

$$\text{НОД}(m_i, m_j) = 1.$$

Решение вычисляется по формуле:

$$x = \sum_{i=1}^{n} a_i M_i y_i \pmod{M},$$

где $M_i = M/m_i$, а $y_i = M_i^{-1} \pmod{m_i}$.

1.4 Функция Эйлера $\varphi(n)$

Определение 9. Пусть n – натуральное число, а $p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ – разложение n на простые множители:

$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

Функция $\varphi(n)$,

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$$

называется функций Эйлера, ее значение равно количеству меньших n и взаимно простых с n натуральных чисел.

Таким образом, $|\mathbb{Z}_n^*| = \varphi(n)$.

1.4.1 Теорема Эйлера

Теорема 3. Пусть $a \in \mathbb{Z}_n^*$. Тогда $a^{\varphi(n)} = 1 \pmod{n}$.

Доказательство. Пусть $x_1, x_2, ..., x_{\varphi(n)} \in \mathbb{Z}_n^*$ – все различные элементы $\mathbb{Z}_n^*$.
Рассмотрим произведения $x_i a$ для всех $i = 1, 2, ..., \varphi(n)$. Так как $x_i \in \mathbb{Z}_n^*$ и $a \in \mathbb{Z}_n^*$, $x_i a \in \mathbb{Z}_n^*$, то есть $x_i a = x_k \pmod{n}$ для некоторого k.
Все произведения $x_i a$ различны, так как в противном случае

$$x_i a = x_j a \pmod{n},$$

откуда, умножив обе части на $a^{-1} \pmod{n}$, получим противоречие:

$$x_i = x_j \pmod{n}.$$

Рассмотрим произведение всех $x_i a$, $i = 1, 2, ..., \varphi(n)$:

$$x_1 x_2 ... x_{\varphi(n)} a^{\varphi(n)} = x_1 x_2 ... x_{\varphi(n)} \pmod{n},$$

откуда следует утверждение теоремы.

□

1.5 Непрерывные дроби

Определение 10. Непрерывной дробью называется выражение вида

$$[a_0, a_1, a_2, a_3, ...] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + ...}}},$$

где $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$, $i = 1, 2, 3, ...$

Любое рациональное число представимо в виде конечной непрерывной дроби. Любое вещественное число представимо в виде непрерывной дроби.

Алгоритм представления числа $\alpha \in \mathbb{R}$ в виде непрерывной дроби:

$$a_0 = \lfloor \alpha \rfloor, r_0 = \alpha - a_0$$
$$a_i = \left\lfloor \frac{1}{r_{i-1}} \right\rfloor, r_i = \frac{1}{r_{i-1}} - a_i, i = 1, 2, ...$$
Если $r_m = 0, \alpha = [a_0, ..., a_m]$.

Определение 11. Непрерывная дробь $[a_0, a_1, a_2, ..., a_m]$ называется подходящей дробью к непрерывной дроби вида

$$[a_0, a_1, a_2, ..., a_m, ..., a_n]$$

или

$$[a_0, a_1, a_2, ..., a_m, ..., a_n, ...],$$

где $n > m$.

Числители и знаменатели подходящих дробей $\frac{s_i}{t_i}$ связаны следующим соотношением:

$$s_0 = a_0, \quad t_0 = 1,$$
$$s_1 = a_0 a_1 + 1, \quad t_1 = a_1,$$
$$s_i = a_i s_{i-1} + s_{i-2}, \quad t_i = a_i t_{i-1} + t_{i-2}, \quad i = 2, ..., m$$

Утверждение 1. Подходящая дробь $\frac{s}{t}$ к представлению вещественного числа x в виде непрерывной дроби является наилучшим приближением x седи всех дробей, знаменатель которых не превосходит t.

Утверждение 2. Пусть x – рациональное число, НОД$(s,t) = 1$ и выполняется равенство

$$\left| x - \frac{s}{t} \right| < \frac{1}{2t^2},$$

то $\frac{s}{t}$ – подходящая дробь к представлению числа x в виде непрерывной дроби.

1.6 Векторное пространство

Определение 12. Векторным (линейным) пространством V над полем F называется множество, на котором определены операция сложения элементов и операция умножения элемента множества V на элемент поля F, удовлетворяющие следующим условиям:

- Коммутативность: $a + b = b + a$;
- Ассоциативность: $(a + b) + c = a + (b + c)$;
- $\exists \mathbf{0} \in V : a + \mathbf{0} = a, \forall a \in V$.
- $\forall a \in V, \exists (-a) \in V : a + (-a) = \mathbf{0}$.

- $\forall \alpha \in F, \forall a, b \in V : \alpha(a+b) = \alpha a + \alpha b.$
- $\forall \alpha, \beta \in F, \forall a \in V : (\alpha+\beta)a = \alpha a + \beta a.$
- $\forall \alpha, \beta \in F, \forall a \in V : (\alpha\beta)a = \alpha(\beta a).$
- $\forall a \in V : 1 \cdot a = a.$

Определение 13. Скалярным произведением векторов x и y в векторном пространстве V над полем F называется операция

$$(x, y) \in F,$$

обладающая следующими свойствами:

- $(x, y) = (y, x), \quad x, y \in V$
- $(x+y, z) = (x, z) + (y, z), \quad x, y, z \in V$
- $(\alpha x, y) = \alpha(x, y), \quad x, y \in V, \alpha \in F.$

Определение 14. Подпространством пространства V называется множество $L \subset V$, являющееся пространством.

1.6.1 Линейная комбинация, линейная оболочка, линейная независимость

Рассмотрим m векторов $a_1, a_2, ..., a_m \in V$ и m элементов поля $\lambda_1, \lambda_2, ..., \lambda_m \in F$.

Определение 15. Вектор $\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_m a_m$ называется линейной комбинацией векторов $a_1, a_2, ..., a_m$.

Определение 16. Множество всех линейных комбинаций векторов $a_1, a_2, ..., a_m$ называется линейной оболочной векторов $a_1, a_2, ..., a_m$.

Определение 17. Если существует ненулевой набор чисел $\lambda_1, \lambda_2, ..., \lambda_m$ такой, что $\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_m a_m = 0$, система векторов $a_1, a_2, ..., a_m$ называется линейно зависимой, в противном случае – линейно независимой.

1.6.2 Базис пространства

Определение 18. Базисом пространства называется максимальная линейно независимая система векторов этого пространства.

Определение 19. Размерностью пространства называется количество векторов в базисе этого пространства.

1.6.3 Векторное пространство $\mathbb{R}^n$

Рассмотрим пространство $\mathbb{R}^n$ над полем действительных чисел. Элементами этого пространства будут упорядоченные системы из n действительных чисел:

$$x \in \mathbb{R}^n \Rightarrow x = (x_1, x_2, ..., x_n), \quad x_i \in \mathbb{R}^n, \quad i = 1, ..., n.$$

Сложение элементов $\mathbb{R}^n$ определено следующим образом:

$$x + y = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n).$$

Умножение элемента $\mathbb{R}^n$ на действительное число:

$$\lambda x = (\lambda x_1, \lambda x_2, ..., \lambda x_n).$$

В пространстве $\mathbb{R}^n$ операция скалярного произведения определена следующим образом:

$$(x, y) = \sum_{i=1}^{n} x_i y_i. \tag{1}$$

Определение 20. Векторное пространство с определенной в нем согласно (1) операцией скалярного произведения называется евклидовым пространством.

1.6.4 Ортогональность

Определение 21. Два вектора евклидова пространства называются ортогональными, если их скалярное произведение равно нулю.

Определение 22. Ортогональный базис – базис, все векторы которого попарно ортогональны.

1.6.4.1 Проекция вектора на подпространство

Определение 23. Пусть L – линейное подпространство пространства $\mathbb{R}^n$. Ортогональным дополнением к L называется множество

$$L^{\perp} = \{z \in \mathbb{R}^n | \, (z,y) = 0, \forall y \in L\}.$$

Любой вектор $x \in \mathbb{R}^n$ можно единственным образом представить в виде $x = y + z$, где $y \in L$, $z \in L^{\perp}$. Вектор y – ортогональная проекция x на подпространство L, вектор z – ортогональная проекция x на $L^{\perp}$, так как $(y,w) = 0, \forall w \in L^{\perp}$.

1.6.4.2 Метод ортогонализации Грама-Шмидта

Метод ортогонализации Грама-Шмидта позволяет по произвольному базису $\{b_1, ..., b_n\}$ построить ортогональный базис $\{b_1^*, ..., b_n^*\}$.

Метод состоит из следующих шагов:

- $b_1^* = b_1$
- Для всех i = 2, ..., n:

  $$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*,$$

  где $\mu_{ij} = (b_i, b_j^*)/(b_j^*, b_j^*)$.

1.7 Решетки в $\mathbb{R}^n$

Рассмотрим линейно независимую систему векторов $b_1, ..., b_n$ из $\mathbb{R}^n$.

Определение 24. Решеткой называется множество всех целочисленных комбинаций векторов $b_1, ..., b_n$:

$$\Lambda = \left\{ \sum_{i=1}^{n} s_i b_i \middle| s_i \in \mathbb{Z}, \quad i = 1, 2, ..., n \right\}$$

Определение 25. Система векторов $b_1, ..., b_n \in \mathbb{R}^n$ называется базисом решетки Λ.

Определение 26. Матрица

$$B = \begin{pmatrix} b_1^{(1)} & \cdots & b_n^{(1)} \\ \vdots & \ddots & \vdots \\ b_1^{(n)} & \cdots & b_n^{(n)} \end{pmatrix},$$

где $b_i^{(1)}, ..., b_i^{(n)}$ – координаты вектора b_i в ортонормированном базисе $\mathbb{R}^n$, $i = 1, ..., n$, называется матрицей базиса решетки Λ.

Для того, чтобы получить другую матрицу базиса решетки Λ, необходимо умножить матрицу базиса на унимодулярную матрицу:

$$B' = BU,$$

где U – квадратная целочисленная матрица, такая, что $|\det U| = 1$.

Модуль определителя матрицы базиса является инвариантом решетки и называется определителем решетки:

$$d(\Lambda) = |\det B|.$$

1.7.1 LLL-приведенный базис решетки

Определение 27. Базис $b_1, b_2, ..., b_n$ решетки $\Lambda \subset \mathbb{R}^n$ называется LLL-приведенным, если для векторов $b_1^*, b_2^*, ..., b_n^*$ и коэффициентов μ_{ij}, полученных с помощью метода ортогонализации Грама-Шмидта, выполнены следующие неравенства:

$$\begin{aligned} \left|\mu_{ij}\right| &\leq \frac{1}{2}, \quad 1 \leq j < i \leq n, \\ \left|b_i^* + \mu_{i,i-1} b_{i-1}^*\right|^2 &\geq \frac{3}{4} \left|b_{i-1}^*\right|^2. \end{aligned} \tag{2}$$

Через λ_i обозначим линейную оболочку векторов $b_1, b_2, ..., b_n$. В соответствии с методом ортогонализации Грама-Шмидта

$$b_k = b_k^* + \sum_{j=1}^{k-1} \mu_{kj} b_j^*,$$

тогда $\sum_{j=1}^{k-1} \mu_{kj} b_j^* \in \lambda_{k-1}$, $b_k^* \in \lambda_{k-1}^{\perp}$. Таким образом, b_k^* – проекция b_k на $\lambda_{k-1}^{\perp}$.

Заметим, что $b_k = b_k^* + \mu_{k,k-1} b_{k-1}^* + \sum_{j=1}^{k-2} \mu_{kj} b_j^*$, поэтому $b_k^* + \mu_{k,k-1} b_{k-1}^* \in \lambda_{k-2}^{\perp}$, то есть $b_k^* + \mu_{k,k-1} b_{k-1}^*$ – проекция вектора b_k на $\lambda_{k-2}^{\perp}$.

Теорема 4. Если Λ – решетка в $\mathbb{Z}^n$ с базисом $b_1, b_2, ..., b_n$, причем

$$|b_i| \leq B, \quad i = 1, 2, ..., n,$$

где $B \in \mathbb{R}$, $B \geq 2$, то алгоритм построения LLL-приведенного базиса выполняется за $O(n^4 \log B)$ арифметических операций. При этом двоичная запись целых чисел, встречающихся в ходе работы алгоритма, содержит не более $O(n \log B)$ битов.

1.7.2 Свойства LLL-приведенного базиса решетки

Теорема 5. Пусть $b_1, b_2, ..., b_n$ – LLL-приведенный базис решетки $\Lambda \subset \mathbb{R}^n$. Истинны следующие неравенства:

- $|b_j|^2 \leq 2^{i-1}|b_i^*|^2$, $1 \leq j < i \leq n$;
- $d(\Lambda) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n(n-1)/4} d(\Lambda)$;
- $|b_1| \leq 2^{(n-1)/4} d(\Lambda)^{1/n}$.

Доказательство. В силу ортогональности векторов b_i^*, выполняется равенство

$$|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 = |b_i^*|^2 + \mu_{i,i-1}^2 |b_{i-1}^*|^2.$$

По определению LLL-приведенного базиса, $\mu_{i,i-1}^2 \leq 1/4$, из неравенства (2) следует:

$$|b_i^*|^2 \geq \frac{1}{2}|b_{i-1}^*|^2.$$

Таким образом,

$$|b_j^*|^2 \leq 2^{i-j}|b_i^*|^2, \quad \forall j \leq i.$$

Так как векторы $b_1 *, b_2^*, ..., b_n^*$ ортогональны,

$$|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 \leq |b_i^*|^2 \left(1 + \sum_{j=1}^{i-1} \frac{1}{4} 2^{i-j}\right) =$$
$$= |b_i^*|^2 \left(1 + \frac{1}{2}(2^{i-1} - 1)\right) \leq 2^{i-1}|b_i^*|^2.$$

Поэтому $|b_j|^2 \leq 2^{j-1}|b_j^*|^2 \leq 2^{j-1} \cdot 2^{i-j}|b_i^*|^2$, откуда следует первое утверждение теоремы.

Первое неравенство второго утверждения теоремы представляет собой неравенство Адамара. Второе неравенство выполняется, так как

$$\prod_{i=1}^{n} |b_i| \leq 2^{\sum_{i=1}^{n} \frac{i-1}{2}} \prod_{i=1}^{n} |b_i^*| = 2^{\frac{n(n-1)}{2}} d(\Lambda),$$

что также следует из неравенства Адамара.

Из неравенства $|b_1|^2 \leq 2^{i-1}|b_i^*|^2$, $i = 1, ..., n$, следует, что

$$|b_1|^{2n} \leq 2^{n(n-1)/2} \prod_{i=1}^{n} |b_i^*|^2 = 2^{n(n-1)/2} d(\Lambda)^2,$$

что доказывает третье утверждение теоремы.

□

1.7.3 Теорема Копперсмита

Зафиксируем некоторое $n \in \mathbb{N}$. Полиномы, степени которых не превосходят n, образуют линейное пространство. Один из базисов данного пространства:

$$1, x, x^2, ..., x^n.$$

Координаты полинома $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ в этом базисе:

$$(a_0, a_1, ..., a_{n-1}, a_n).$$

Теорема 6 (Теорема Копперсмита). Пусть $p(x) \in \mathbb{Z}[x]$ – приведенный полином степени n над кольцом целых чисел, а N – натуральное число. Если у полинома p есть корень $x_0 \in \mathbb{Z}$ по модулю N $(p(x_0) = 0 \pmod N)$, удовлетворяющий неравенству

$$|x_0| \leq t = c(n, \varepsilon) N^{\frac{1}{n} - \varepsilon},$$

то этот корень может быть найден за полиномиальное от $(n, \frac{1}{\varepsilon}, \log N)$ время.

Доказательство. Докажем эту теорему для $t = c_0(n) N^{\frac{2}{n(n+1)}}$.

Рассмотрим множество полиномов

$$C = \left\{ x^i \middle| \, 0 \leq i < n \right\} \cup \left\{ p(x)/N \right\}.$$

Пусть $x_0 \in \mathbb{Z}$ такое, что

$$p(x_0) = 0 \pmod N.$$

Рассмотрим $q(x) \in C$. Очевидно, что $q(x_0) \in \mathbb{Z}$, так как $p(x_0) = kN$, $k \in \mathbb{Z}$. Это справедливо для любой целочисленной комбинации полиномов из C, то есть

$$\sum_{i=1}^{s} q_i(x_0) \in \mathbb{Z}, \quad \forall q_i \in C.$$

Рассмотрим базис пространства полиномов, степень которых не превосходит n:

$$1, \frac{x}{t}, \frac{x^2}{t^2}, ..., \frac{x^n}{t^n}.$$

Запишем координаты полиномов из C в этом базисе в виде матрицы:

$$B = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & p_0/N \\ 0 & t & 0 & \dots & 0 & p_1 t/N \\ 0 & 0 & t^2 & \dots & 0 & p_2 t^2/N \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & t^{n-1} & p_{n-1} t^{n-1}/N \\ 0 & 0 & 0 & \dots & 0 & t^n/N \end{bmatrix}$$

Эти векторы являются линейно независимыми, рассмотрим решетку Λ, порожденную этой системой векторов. Построим LLL-приведенный базис $b_1, b_2, ..., b_n, b_{n+1}$. По свойствам LLL-приведенного базиса

$$|b_1| \le c(n) d(\Lambda)^{\frac{1}{n+1}} = c(n) \left(t^{\frac{n(n+1)}{2}} / N \right)^{\frac{1}{n+1}} = c(n) N^{-\frac{1}{n+1}} t^{\frac{n}{2}}.$$

Вектор $b_1 = (v_0, v_1 t, ..., v_n t^n)$ будем интерпретировать как полином в базисе

$$1, \frac{x}{t}, \frac{x^2}{t^2}, ..., \frac{x^n}{t^n},$$

таким образом, $v(x) = \sum_{i=0}^{n} v_i x^i$.

Пусть $c(n) N^{-\frac{1}{n+1}} t^{\frac{n}{2}} < \frac{1}{n+1}$, то есть

$$t < \left(N^{\frac{1}{n+1}} \frac{1}{c(n)(n+1)} \right)^{\frac{2}{n}} = c_0(n) N^{\frac{2}{n(n+1)}}.$$

Тогда $|b| < \frac{1}{n+1}$, откуда получим $|v_i t^i| < \frac{1}{n+1}$.

Пусть x_0 – корень $p(x)$ по модулю N, $x_0 \le t$, $x_0 \in \mathbb{Z}$.

$$|v(x_0)| \le \sum_{i=0}^{n} |v_i x_0^i| \le \sum_{i=0}^{n} |v_i t^i| < \sum_{i=0}^{n} \frac{1}{n+1} = (n+1) \frac{1}{n+1} = 1.$$

Мы получили, что $|v(x_0)| < 1$, но так как $v(x)$ – целочисленная комбинация полиномов из C, $v(x_0) \in \mathbb{Z}$, откуда следует

$$v(x_0) = 0, \quad v(x) \in \mathbb{Q}[x].$$

□

1.8 Извлечение корней в $\mathbb{Z}_n^*$

1.8.1 Квадратичные вычеты

Определение 28. Порядком элемента $a \in \mathbb{Z}_n^*$ группы называется минимальное число $m \in \mathbb{N}$, для которого выполняется

$$a^m = 1 \pmod{n}.$$

Если такого m не существует, элемент a имеет бесконечный порядок.

Определение 29. Первообразным корнем по модулю n (образующим элементом группы $\mathbb{Z}_n^*$) называется такой элемент $a \in \mathbb{Z}_n^*$, порядок которого равен $\varphi(n)$.

Первообразный корень по модулю n существует тогда и только тогда, когда

$$n = 2, 4, p^\alpha, 2p^\alpha,$$

где p – простое число, $p > 2$, $\alpha \in \mathbb{N}$.

Определение 30. Группа, обладающая образующим элементом, называется циклической.

Если группа $\mathbb{Z}_n^*$ является циклической, она содержит $\varphi(\varphi(n))$ образующих элементов.

Определение 31. Число $a \in \mathbb{N}$ называется квадратичным вычетом по модулю n, если НОД$(a,n) = 1$ и существует такое $x \in \mathbb{N}$, что

$$x^2 = a \pmod{n}.$$

Определение 32. Пусть p – нечетное простое число. Символ Лежандра – функция, определенная на множестве натуральных чисел:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{если } a \text{ – квадратичный вычет по модулю } p \text{ и } a \neq 0 \pmod{p} \\ -1, \text{если } a \text{ не является квадратичным вычетом по модулю } p \\ 0, \text{если } a = 0 \pmod{p} \end{cases}$$

Теорема 7 (Критерий Эйлера). Пусть p – нечетное простое число. Для любого натурального a истинно равенство

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

Лемма 1. Пусть $m = p^s$, где p – нечетное простое число, а s – натуральное число. Рассмотрим циклическую группу $\mathbb{Z}_m^*$ с образующим элементов $g \in \mathbb{Z}_m^*$:

$$\mathbb{Z}_m^* = \left\{1, g, g^2, \ldots, g^{\varphi(m)-1}\right\}.$$

Элемент $a = g^j \pmod{m}$ группы $\mathbb{Z}_m^*$ является квадратичным вычетом по модулю m тогда и только тогда, когда j – четное.

Доказательство. Пусть $a = g^j \pmod{m}$ – квадратичный вычет по модулю m, тогда существует $b \in \mathbb{Z}_m^*$ такое, что:

$$b^2 = a \pmod{m}.$$

Так как $b \in \mathbb{Z}_m^*$, существует такое целое неотрицательное i, что $b = g^i$. Таким образом, $j = 2i$.

Пусть j – четно, тогда существует такое $b = g^{\frac{j}{2}} \in \mathbb{Z}_m^*$:

$$b^2 = a \pmod{m},$$

откуда следует, что a – квадратичный вычет по модулю m. □

Теорема 8. Пусть $m = p^s$, где p – нечетное простое число, а s – натуральное число. Элемент $a \in \mathbb{Z}_m^*$ является квадратичным вычетом по модулю m тогда и только тогда, когда

$$a^{\frac{\varphi(m)}{2}} = 1 \pmod{m}.$$

Элемент $a \in \mathbb{Z}_m^*$ не является квадратичным вычетом по модулю m тогда и только тогда, когда

$$a^{\frac{\varphi(m)}{2}} = -1 \pmod{m}.$$

Доказательство. Пусть $a \in \mathbb{Z}_m^*$ – квадратичный вычет по модулю m. Тогда $\exists b \in \mathbb{Z}_m^* : b^2 = a \pmod{m}$. Тогда, по теореме Эйлера:

$$a^{\frac{\varphi(m)}{2}} = b^{\varphi(m)} = 1 \pmod{m}.$$

Пусть a не является квадратичным вычетом. Тогда, по лемме 1, $a = g^{2i+1}$ для некоторого образующего элемента $g \in \mathbb{Z}_m^*$ и некоторого неотрицательного целого i. Тогда

$$a^{\frac{\varphi(m)}{2}} = g^{\frac{(2i+1)\varphi(m)}{2}} = g^{\frac{\varphi(m)}{2}+i\varphi(m)} = g^{\frac{\varphi(m)}{2}} = (g^{\varphi(m)})^{\frac{1}{2}} = 1^{\frac{1}{2}} \pmod{m}.$$

Так как $m = p^s$, где p – простое,

$$1^{\frac{1}{2}} = \pm 1 \pmod{m}.$$

Заметим, что g – образующий элемент группы $\mathbb{Z}_m^*$ и порядок g равен $\varphi(m)$, а потому

$$g^{\frac{\varphi(m)}{2}} \neq 1 \pmod{m}.$$

Таким образом,

$$a^{\frac{\varphi(m)}{2}} = -1 \pmod{m}.$$

□

Теорема 9. Пусть $m = p^s$, где p – нечетное простое число, а s – натуральное число, $a \in \mathbb{Z}_m^*$. Определим $b = a \mod p$, $b \in \mathbb{Z}_p^*$.
Если $a^{\frac{\varphi(m)}{2}} = 1 \pmod m$, то $b^{\frac{p-1}{2}} = 1 \pmod p$. Если $a^{\frac{\varphi(m)}{2}} = -1 \pmod m$, то $b^{\frac{p-1}{2}} = -1 \pmod p$.
Таким образом, если натуральное число n является квадратичным вычетом по модулю p, оно является квадратичным вычетом по модулю m.

1.8.2 Алгоритм извлечения квадратного корня в $\mathbb{Z}_p^*$

Теорема 10. Пусть $a \in \mathbb{Z}_n^*$ имеет порядок k. Тогда k делит некоторое $m \in \mathbb{Z}$ тогда и только тогда, когда $a^m = 1 \pmod n$.

Теорема 11. Пусть $a \in \mathbb{Z}_n^*$ имеет порядок k. Тогда для любого $s \in \mathbb{Z}$:

$$\operatorname{ord}_n a^s = \frac{k}{\text{НОД}(k,s)}.$$

Доказательство. Пусть $\operatorname{ord}_n a^s = t$. По теореме 10, st делится на k, откуда следует, что $\frac{s}{\text{НОД}(k,s)}t$ делится на $\frac{k}{\text{НОД}(k,s)}$, а потому:

$$t = \frac{k}{\text{НОД}(k,s)}.$$

□

Теорема 12. Пусть p – простое число, такое, что $p = 3 \pmod 4$, и a – квадратичный вычет по модулю p. Тогда решение уравнения $x^2 = a \pmod p$ имеет следующий вид:

$$x = a^{\frac{p+1}{4}} \pmod p.$$

Пусть p – нечетное простое число. Запишем $p - 1 = 2^r s$, где s – нечетно. Положим $y = a^{\frac{s+1}{2}} \pmod p$, тогда $y^2 = a^{s+1} = a^s \cdot a \pmod p$. В силу того, что y^2 и a – квадратичные вычеты по модулю p, a^s – также квадратичный вычет по

модулю p.

Пусть $b = a^s \pmod p$. Тогда задача сводится к нахождению z – квадратного корня b:

$$z^2 = b \pmod p,$$

так как $\left(yz^{-1}\right)^2 = a^{s+1} \cdot a^{-s} = a \pmod p$.

Порядок b по модулю p делит 2^{r-1}, в силу того, что

$$b^{2^{r-1}} = (a^s)^{2^{r-1}} = a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = 1 \pmod p.$$

Порядок z по модулю p делит 2^r, так как

$$\mathrm{ord}_p z = 2 \cdot \mathrm{ord}_p b,$$

а 2^{r-1} делится на $\mathrm{ord}_p b$.

Лемма 2. Множество S элементов $\mathbb{Z}_p^*$, порядок которых равен степени числа 2, является подгруппой $\mathbb{Z}_p^*$.

Лемма 3. Пусть $n \in \mathbb{Z}_p^*$ не является квадратичным вычетом по модулю p. Пусть $m = n^s \pmod p$. Тогда $S = \{m, m^2, m^3, \ldots, m^{2^r}\}$

Лемма 4. Если $\mathrm{ord}_p m = 2^r$ и $\mathrm{ord}_p b = 2^u$, где $u < r$, тогда $\mathrm{ord}_p(m^{2^{r-u}} b) = 2^v$, где $v < u$.

Алгоритм 1. Вход: нечетное просто число p, натуральное число a,
$1 \le a \le p$.
Выход: такое x, что $x^2 = a \pmod p$, если a – квадратичный вычет по модулю p.

1. Вычисляем символ Лежандра:

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

Если $\left(\frac{a}{p}\right) = -1$, алгоритм заканчивает свою работу, так как a не является квадратичным вычетом по модулю p.

2. Случайным образом выбираем $n \in \mathbb{Z}_p^*$ до тех пор, пока не получим
$$\left(\frac{n}{p}\right) = -1.$$
3. Вычисляем такие r и s, что $p-1 = 2^r s$.
4. Положим $m = n^s \pmod p$, $y = a^{(s+1)/2} \pmod p$, $z = 1 \pmod p$.
5. Для всех i от 1 до $r-1$:
   - Если $b^{2^{r-i-1}} = -1 \pmod p$, присвоим $b := bm^2 \pmod p$, $z := zm^{-1} \pmod p$.
   - Присвоим $m := m^2$.
6. Выход: $x = \pm yz^{-1} \pmod p$.

1.8.3 Извлечение квадратного корня в $\mathbb{Z}_{p^e}^*$

Теорема 13. Пусть $a, n \in \mathbb{Z}$, где $n > 0$. Для любого $b \in \mathbb{Z}$ уравнение
$$az = b \pmod n$$
имеет решение тогда и только тогда, когда b делится на НОД(a,n).

Доказательство. Выберем произвольное $b \in \mathbb{Z}$. Пусть
$$az = b \pmod n$$
для некоторого $z \in \mathbb{Z}$. Тогда
$$az = b + kn$$

для некоторого $k \in \mathbb{Z}$. Очевидно, что b делится на НОД(a,n). В другую сторону, пусть b делится на НОД(a,n). Тогда существуют такие числа $z,k \in \mathbb{Z}$, что

$$az + kn = b,$$

откуда получаем $az = b \pmod{n}$. □

Пусть p – нечетное простое число, число $a \in \mathbb{Z}$ такое, что НОД$(a,p) = 1$. Пусть $e \in \mathbb{Z}$, $e > 1$, и известно $z \in \mathbb{Z}$: $z^2 = a \pmod{p}$. Задача – найти такое $x \in \mathbb{Z}$, что $x^2 = a \pmod{p^e}$.

Пусть нам известно $b \in \mathbb{Z}$: $b^2 = a \pmod{p^f}$. Найдем $c \in \mathbb{Z}$ такое, что $c^2 = a \pmod{p^{f+1}}$. Заметим, что $c^2 = a \pmod{p^f}$, поэтому $c = \pm b \pmod{p^f}$. Положим $c = b + p^f h$, где $h \in \mathbb{Z}$, и решим для h. Получим:

$$c^2 = \left(b + p^f h\right)^2 = b^2 + 2bp^f h + p^{2f} h^2 = b^2 + 2bp^f h \pmod{p^{f+1}}.$$

Таким образом, необходимо найти h, для которого

$$2bp^f h = a - b^2 \pmod{p^{f+1}}.$$

Так как $2b$ не делится на p, НОД$(2bp^f, p^{f+1}) = p^f$. В силу того, что $b^2 = a \pmod{p^f}$, $(a - b^2)$ делится на p^f. Таким образом, по теореме 13 получаем, что это уравнение имеет единственное решение по модулю p.

АЛГОРИТМ RSA

В этой главе рассматривается криптографическая система RSA, алгоритмы генерирования модуля RSA, открытого и закрытого ключей, алгоритмы шифрования и расшифрования сообщений.

2.1 Алгоритм RSA

2.1.1 Генерация ключей RSA

Ключи шифрования и расшифрования RSA генерируются следующим образом:

- Генерация двух случайных больших простых чисел p и q.
- Вычисление модуля:

$$N = pq.$$

- Вычисление функции Эйлера:

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

- Выбор открытой (шифрующей) экспоненты e такой, что

$$\text{НОД}(e, \varphi(N)) = 1.$$

Обычно e выбирается из множества $\{3, 17, 65537\}$. Пара (N, e) представляет собой открытый ключ, используемый для шифрования.

- Вычисление секретной (расшифровывающей) экспоненты d:

$$d = e^{-1} \pmod{\varphi(N)}.$$

Пара (N,d) представляет собой закрытый ключ, используемый для расшифрования.

2.1.2 Шифрование RSA

Шифротекст c, являющийся результатом шифрования сообщения $m \in \mathbb{Z}_N^*$ с использованием открытого ключа (N,e), вычисляется по формуле

$$c = m^e \pmod{N}.$$

2.1.3 Расшифрование RSA

Сообщение m, являющееся результатом расшифрования шифротекста c с использованием закрытого ключа (N,d), вычисляется по формуле

$$m = c^d \pmod{N}.$$

Теорема 14. Пусть p и q – простые числа, $N = pq$, НОД$(e, \varphi(N)) = 1$, $d = e^{-1} \pmod{\varphi(N)}$ и $c = m^e \pmod{N}$, где $m \in \mathbb{Z}_N^*$;. Тогда

$$m = c^d \pmod{N}.$$

Доказательство. Заметим, что

$$c^d = (m^e)^d = m^{ed} = m^{1+k\varphi(N)},$$

где $k \in \mathbb{Z}$. Тогда, по теореме Эйлера:

$$c^d = mm^{k\varphi(N)} = m(m^{\varphi}(N))^k = m \cdot 1 = m \pmod{N}.$$

□

2.2 Практическая реализация RSA

2.2.1 Эффективный алгоритм возведения в степень

Пусть $k \in \mathbb{N}$, а $b_t b_{t-1} ... b_0$ – двоичное представление числа k, то есть

$$k = \sum_{i=0}^{t} 2^i b_i.$$

Тогда значение m^k может быть вычислено по формуле:

$$m^k = m^{\sum_{i=0}^{t} 2^i b_i} = \prod_{i=0}^{t} m^{2^i b_i}.$$

Заметим, что все значения $m, m^2, m^4, ..., m^{2^t}$ могут быть вычислены за t операций, а значение m^k, таким образом, не более, чем за $2t$ операций.

2.2.2 Эффективный алгоритм расшифрования RSA

Пусть $N = pq$ – модуль RSA, e – шифрующая экспонента, d – секретная экспонента, m – открытый текст, c – шифротекст:

$$c = m^e \pmod{N}.$$

Для того, чтобы расшифровать шифротекст, необходимо возвести c в степень d по модулю N:

$$m = c^d \pmod{N}.$$

Если получателю известна факторизация N, он может построить систему уравнений:

$$\begin{cases} m = c^d \pmod{p} \\ m = c^d \pmod{q} \end{cases}$$

По теореме Эйлера, $c^d = c^{d \mod \varphi(p)} = c^{d \mod (p-1)} \pmod{p}$, $c^d = c^{d \mod \varphi(q)} = c^{d \mod (q-1)} \pmod{q}$. Таким образом, система приобретает следующий вид:

$$\begin{cases} m = c^{d \mod (p-1)} \pmod{p} \\ m = c^{d \mod (q-1)} \pmod{q} \end{cases}$$

В силу взаимной простоты p и q система уравнений имеет единственное решение по модулю N:

$$m = c^d \pmod{N},$$

и это решение может быть найдено с помощью китайской теоремы об остатках.

2.2.3 PKCS1 v2.0: Optimal Asymmetric Encryption Padding

Пусть N – модуль RSA, а n – количество битов в двоичной записи числа N. k_1, $k_2 \in \mathbb{N}$. Пусть $msg \in \{0,1\}^{n-k_1-k_2}$ – открытый текст. Пусть H и G – криптографический хэш-функции:

$$H : \{0,1\}^{k_2} \to \{0,1\}^{n-k_2}, G : \{0,1\}^{n-k_2} \to \{0,1\}^{k_2}.$$

Алгоритм OAEP:

- Случайная последовательность *rand* длиной k_1 битов подается на вход хэш-функции H.
- Выполняется операция побитового исключающего ИЛИ строки $H(rand)$ и исходного сообщения, дополненного строкой 0100...0 длиной k_1 битов.
- Результат предыдущего шага составляет старшие $(n-k_2)$ битов итоговой последовательности, он также подается на вход хеш-функции G.
- Выполняется операция побитового исключающего ИЛИ выходного значения хеш-функции G и последовательности *rand*.

- Результат предыдущего шага составляет младшие k_2 битов итоговой последовательности.

Сообщение, подаваемое на вход алгоритму шифрования, имеет вид:

$$\left(\left(msg \parallel 01 \parallel 0^{k_1-2}\right) \oplus H\left(rand\right)\right) \parallel \left(G\left(\left(msg \parallel 01 \parallel 0^{k_1-2}\right) \oplus H\left(rand\right)\right) \oplus rand\right)$$

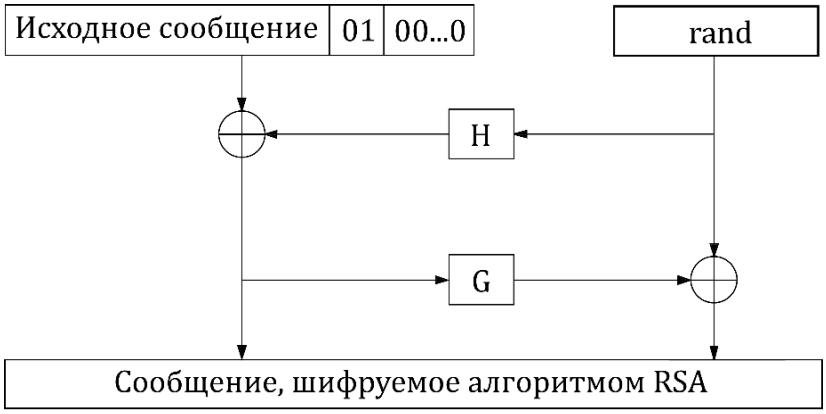

Рис. 2.1: PKCS1 v2.0: OAEP

После расшифровывания:

- Полученная последовательность разделяется на две последовательности: старшие $(n-k_2)$ битов и младшие k_2 битов.
- Первая последовательность подается на вход хеш-функции G.
- Выполняется операция побитового исключающего ИЛИ результата предыдущего шага и второй последовательности.
- Результат предыдущего шага – последовательность *rand* – подается на вход хеш-функции H.
- Выполняется операция побитового исключающего ИЛИ результата предыдущего шага и первой последовательности.
- Результат: Исходное сообщение $\parallel 01 \parallel 0^{k_1-2}$.

АТАКИ НА RSA

3.1 Элементарные атаки на криптосистему RSA

3.1.1 Разделенный модуль

Пусть два участника информационного обмена используют одинаковый модуль N алгоритма RSA, но разные шифрующие экспоненты e_1 и e_2, $e_1 \neq e_2$. Предположим, противник перехватил два шифротекста, c_1 и c_2, представляющие собое один и тот же открытый текст m, зашифрованный на разных открытых ключах с одинаковым модулем N:

$$c_1 = m^{e_1} \pmod{N}, c_2 = m^{e_2} \pmod{N}.$$

Противник может восстановить открытый текст m:

- $t_1 = e_1^{-1} \pmod{e_2}$.
- $t_2 = \frac{t_1 e_1 - 1}{e_2}$
- $c_1^{t_1} c_2^{-t_2} = m^{t_1 e_1} m^{-t_2 e_2} = m^{t_1 e_1} m^{1 - t_1 e_1} = m \pmod{N}$

3.1.2 Малая шифрующая экспонента

Пусть несколько пользователей используют малую шифрующую экспоненту $e = 3$. Противник перехватил три шифротекста, c_1, c_2 и c_3, являющиеся результатами шифрования одного и того же открытого текста m на открытых

ключах (N_1, e), (N_2, e) и (N_3, e) соответственно:

$$c_1 = m^e \pmod{N_1},$$
$$c_2 = m^e \pmod{N_2},$$
$$c_3 = m^e \pmod{N_3}.$$

В этом случае противник может восстановить открытый текст m с помощью китайской теоремы об остатках:

$$\begin{cases} m^e = c_1 \pmod{N_1} \\ m^e = c_2 \pmod{N_2} \\ m^e = c_3 \pmod{N_3} \end{cases}$$

Существует единственное решение этой системы по модулю $N_1N_2N_3$, так как N_1, N_2 и N_3 взаимно просты. Так как $m < N_1$, $m < N_2$, $m < N_3$,

$$m^e \mod N_1N_2N_3 = m^e.$$

3.2 Атака Винера

Атака 1. Пусть $N = pq$ – модуль RSA, e – шифрующая экспонента, d – расшифровывающая экспонента, и выполняются следующие условия:

- $q < p < 2q$;
- $e < \varphi(N)$;
- $d < \frac{1}{3}N^{\frac{1}{4}}$.

Нарушитель может восстановить расшифровывающую экспоненту d за $O(\log N)$ операций как знаменатель одной из подходящих дробей к представлению $\frac{e}{N}$ в виде непрерывной дроби.

Так как $ed = 1 \pmod{\varphi(N)}$, выполняется равенство

$$ed = 1 + k\varphi(N),$$

где $k \in \mathbb{Z}$. Получим:

$$\frac{e}{\varphi(N)} - \frac{k}{d} = \frac{1}{d\varphi(N)}.$$

Заметим, что $N - \varphi(N) = pq - (p-1)(q-1) = p + q - 1$. Так как $q < p$ и $p < 2q$, получаем неравенства:

$$q < \sqrt{N}, \quad p < 2\sqrt{N},$$

откуда следует:

$$|N - \varphi(N)| < 3\sqrt{N}.$$

Рассмотрим абсолютное значение разности:

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN}{Nd}\right| = \left|\frac{ed - k\varphi(N) + k\varphi(N) - kN}{Nd}\right| = \left|\frac{1 - k(N - \varphi(N))}{Nd}\right| =$$
$$= \left|\frac{k(N - \varphi(N)) - 1}{Nd}\right| < \frac{3k\sqrt{N}}{Nd} = \frac{3k}{d\sqrt{N}}.$$

Из равенства $ed - k\varphi(N) = 1$ и условия $e < \varphi N$ следует, что $k < d$ и НОД$(k, d) = 1$. Тогда

$$\frac{3k}{d\sqrt{N}} < \frac{3d}{d\sqrt{N}} = \frac{3}{\sqrt{N}}.$$

Но $d < \frac{1}{3}N^{\frac{1}{4}}$, поэтому

$$\frac{3}{\sqrt{N}} < \frac{3}{9d^2} = \frac{1}{3d^2} < \frac{1}{2d^2},$$

откуда получим истинность неравенства

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Таким образом, $\frac{k}{d}$ – подхоядщая дробь к представлению $\frac{e}{N}$ в виде непрерывной дроби.

3.2.1 Атака Винера: пример

Пусть $p = 107$, $q = 131$, $N = pq = 107 \cdot 131 = 14017$. Тогда

$$\varphi(N) = 106 \cdot 130 = 13780.$$

Выберем шифрующую экспоненту $e = 9187$, вычислим секретную экспоненту d:

$$d = e^{-1} \pmod{\varphi(N)} = 9187^{-1} \pmod{13780} = 3 \pmod{13780}.$$

Заметим, что

$$d = 3 < \frac{1}{3}N^{\frac{1}{4}} \approx 3,626957892395294.$$

Вычислим $\frac{e}{N}$ и построим подходящую дробь:

$$\alpha = \frac{e}{N} \approx 0.6554184204894057.$$

Воспользуемся алгоритмом построения непрерывных дробей:

- $a_0 = 0$, $r_0 \approx 0.6554184204894057$;
- $a_1 = 1$, $r_1 \approx 0.525742897572657$;
- $a_2 = 1$, $r_2 \approx 0.9020703933747412$;
- $a_3 = 1$, $r_3 \approx 0.1085609364241451$;
- $a_4 = 9$, $r_4 \approx 0.2114164904862541$;
- И т.д.

Таким образом, представление $\frac{e}{N}$ в виде непрерывной дроби имеет вид

$$[0,1,1,1,9,...].$$

Построим последовательность подходящих дробей:

- $\frac{s_0}{t_0} = \frac{0}{1}$;
- $\frac{s_1}{t_1} = \frac{0 \cdot 1 + 1}{1} = \frac{1}{1}$;
- $\frac{s_2}{t_2} = \frac{1 \cdot 1 + 0}{1 \cdot 1 + 1} = \frac{1}{2}$;
- $\frac{s_3}{t_3} = \frac{1 \cdot 1 + 1}{1 \cdot 2 + 1} = \frac{2}{3}$;

Знаменатель дроби $\frac{s_3}{t_3}$ равен значению секретной экспоненты d.

3.3 Частичное восстановление секретной экспоненты

При использовании малой шифрующей экспоненты возможно восстановление половины старших битов секретной экспоненты.

$$\begin{aligned} ed &= 1 \pmod{\varphi(N)}, \\ ed &= 1 + k\varphi(N), \\ ed - k(N - (p+q) + 1) &= 1, \\ d &= \frac{k(N - (p+q) + 1) + 1}{e}. \end{aligned}$$

Заметим, что $k < e$. Для всех $i = 1, 2, ..., e$ вычислим

$$d_i = \left\lfloor \frac{iN + 1}{e} \right\rfloor.$$

Для d_k получим (предполагается истинность неравенства $q < p < 2q$):

$$|d_k - d| \leq \frac{k(p+q)}{e} \leq \frac{3k\sqrt{N}}{e} < 3\sqrt{N}.$$

Примерно половина старших битов d_k и d совпадают.

3.4 Факторизация модуля RSA, когда известна половина младших битов p или q

Теорема 15. Пусть $p(x,y)$ – неприводимый полином двух переменных над $\mathbb{Z}$, степень которого по каждой из переменных не превосходит n, наибольший общий делитель всех коэффициентов которого равен единице. Через X и Y обозначим границы сверху для корней (x_0, y_0) соответственно. Определим полином $\bar{p}(x,y) = p(xX, yY)$. Через W обозначим абсолютное значение наибольшего коэффициента $\bar{p}$. Если

$$XY < W^{\frac{2}{3n} - \varepsilon} 2^{-\frac{14n}{3}},$$

то все пары (x_0, y_0), $|x_0| < X$, $|y_0| < Y$, $x_0, y_0 \in \mathbb{Z}$, для которых

$$p(x_0, y_0) = 0$$

могут быть найдены за полиномиальное от $\left(\log W, n, \frac{1}{\varepsilon}\right)$ время.

Атака 2. Пусть N – n-битовый модуль RSA, $N = pq$, $p \approx q$. Пусть дано некоторое $r \geq 2^{\frac{n}{4}}$. Тогда, если атакующему известно $p_0 = p \mod r$, он может эффективно разложить N на множители.

Доказательство. Покажем, в первую очередь, что в этом случае он может вычислить $q_0 = q \mod r$. Из равенства

$$N = p_0 q_0 \pmod{r},$$

и взаимной простоты p_0 и r следует, что атакующий может вычислить q_0 следующим образом:

$$q_0 = N {p_0}^{-1} \pmod{r}.$$

Построим полином

$$u(x,y) = (p_0 + rx)(q_0 + ry) - N = r^2 xy + r p_0 y + r q_0 x + p_0 q_0 - N.$$

Для того, чтобы разложить N на множители, необходимо найти корень (x_0, y_0), $x_0, y_0 \in \mathbb{Z}$ этого полинома, удовлетворяющий неравенствам $|x_0| < X = 2^{\frac{n}{2}+1}/r$, $|y_0| < Y = 2^{\frac{n}{2}+1}/r$. Заметим, что наибольший общий делитель коэффициентов полинома $u(x,y)$ равен r. Построим полином $\bar{u}(x,y) = u(xX, yY)/r$:

$$\bar{u}(x,y) = rXYxy + p_0Yy + q_0Xx + (p_0q_0 - N)/r.$$

Коэффициент полинома $\bar{u}(x,y)$ с наибольшим абсолютным значением не меньше $2^{n+2}/r$. Для выполнения условий теоремы 15 необходимо, чтобы:

$$XY = 2^{n+2}/r^2 < \left(2^{n+2}/r\right)^{2/3} 2^{-14/3},$$

что выполняется при $r > 2^{\frac{n}{4}+4}$. Перебрав все возможные значения пяти битов, получаем возможность факторизации N при $r \geq 2^{\frac{n}{4}}$. □

ПРОВЕРКА ЧИСЛА НА ПРОСТОТУ

Необходимое условие корректной работы алгоритма RSA – простота чисел p и q, на основе которых осуществляется вычисление числа N – модуля RSA. Таким образом, важную роль в применении криптографической системы RSA на практике играют вычислительно эффективные алгоритмы проверки чисел на простоту. Один из таких алгоритмов – тест на простоту Миллера-Рабина – описывается данной главе.

4.1 Тест Миллера-Рабина

Тест на простоту Миллера-Рабина – вероятностный тест на простоту, основанный на теореме [16], формулировка и доказательство которой приводятся ниже.

Определение 33. Порядком элемента $a \in \mathbb{Z}_n^*$ группы называется минимальное число $m \in \mathbb{N}$, для которого выполняется

$$a^m = 1 \pmod{n}.$$

Если такого m не существует, элемент a имеет бесконечный порядок.

Определение 34. Первообразным корнем по модулю n называется такое число a, порядок которого равен $\varphi(n)$.

Первообразный корень по модулю n существует тогда и только тогда, когда

$$n = 2, 4, p^\alpha, 2p^\alpha,$$

где p – простое число, $p > 2$, $\alpha \in \mathbb{N}$.

Определение 35. Число называется бесквадратным, если среди его делителей нет квадратов натуральных чисел, отличных от единицы.

Теорема 16 (Миллера-Рабина). Пусть n – нечетное составное число, не делящееся на 3. Пусть $n-1 = 2^r t$, где $r \geq 1$, t – нечетно. Пусть S – множество чисел a, $0 < a \leq n-1$, что либо $a^t = 1 \pmod{n}$, либо для некоторого j, $1 \leq j \leq r$, $a^{(n-1)/2^j} = n-1 \pmod{n}$. Тогда

$$|S| \leq n/4.$$

Проверка числа n на простоту с помощью теста Миллера-Рабина заключается в случайном выборе числа a, $0 < a \leq n-1$, и проверке числа a на принадлежность множеству S. Если $a \notin S$, число n является составным. Вероятность того, что $a \in S$ в случае, когда n составное, не превышает 25%.

Истинность теоремы [16] следует из истинности семи лемм, которые приводятся ниже с доказательствами.

Через A обозначим множество элементов $a \in \mathbb{Z}_n^*$, для которых выполнено одно из следующих двух условий:

1. $a^{n-1} \neq 1 \pmod{n}$
2. $a^k \neq n-1 \pmod{n}$ для любого $k \in \mathbb{Z}$, и порядок $a \pmod{p}$ равен $p-1$ для некоторого простого p, делящего n.

Пусть $a \in \mathbb{Z}_n^*$. Через S_a обозначим множество

$$S_a = \{as | s \in S\}.$$

Лемма 5. Пусть $a \in A$, $s \in S$. Тогда $as \notin S$.

Доказательство. Если $a^{n-1} = 1 \pmod{n}$, то поскольку $s^{n-1} = 1 \pmod{n}$, получим $(as)^{n-1} \neq 1 \pmod{n}$, то есть $as \notin S$.

Пусть a не удовлетворяет первому, но удовлетворяет второму условию в определении множества A, то есть $a^k \neq n-1 \pmod{n}$ для любого $k \in \mathbb{Z}$, и порядок $a \pmod{p}$ равен $p-1$ для некоторого простого p, делящего n.

Выберем такое i, что

$$a^{(n-1)/2^i} = 1 \pmod{n}.$$

Такое i существует, например, $i = 0$. В силу того, что n делится на p, выполнено равенство

$$a^{(n-1)/2^i} = 1 \pmod{p}.$$

Так как порядок $a \pmod{p}$ равен $p-1$, получаем, что $(n-1)/2^i$ делится на $p-1$. Заметим, что $p-1$ четно, поэтому $0 \leq i < r$. Из этого неравенства следует, что

$$a^{(n-1)/2^r} = a^t \neq 1 \pmod{n}.$$

Покажем, что при всех j таких, что $0 \leq j \; lei < r$, выполнено равенство

$$s^{(n-1)/2^j} = 1 \pmod{n}. \tag{3}$$

Если $s^{(n-1)/2^r} = 1 \pmod{n}$, то равенство (3) выполнено. Пусть для некоторого j_1, $0 \leq j_1 \leq r$,

$$s^{(n-1)/2^{j_1}} = n-1 \pmod{n}.$$

Покажем, что в этом случае $j_1 > i$. Пусть это не так, и $j_1 \leq i$. Поскольку

$$s^{(n-1)/2^{j_1}} = n-1 \pmod{n},$$

то

$$s^{(n-1)/2^{j_1}} = p-1 \pmod{p}.$$

Если $j_1 \leq i$, то $(n-1)/2^{j_1}$ делится на $p-1$, откуда, по малой теореме Ферма, следует, что

$$s^{(n-1)/2^{j_1}} = 1 \pmod{p}.$$

Получаем противоречие, так как $1 \neq p-1 \pmod{p}$.

Таким образом, $j_1 > i$, откуда следует, что при всех j, $0 \leq j \leq i$, выполнено равенство

$$s^{(n-1)/2^j} = 1 \pmod{n},$$

то есть формула (3) верна.

Из (3) следует, что

$$s^{(n-1)/2^{i+1}} = 1 \pmod{n}$$

или

$$s^{(n-1)/2^{i+1}} = n-1 \pmod{n}.$$

Выберем i максимальным. Так как $i < r$, имеем

$$\begin{aligned} a^{(n-1)/2^i} &= 1 \pmod{n}, \\ a^{(n-1)/2^{i+1}} &\neq 1 \pmod{n}, \\ a^{(n-1)/2^{i+1}} &\neq n-1 \pmod{n}. \end{aligned}$$

Тогда при всех j, $0 \leq j \leq i$, выполнено равенство

$$(as)^{(n-1)/2^j} = 1 \pmod{n},$$

но

$$(as)^{(n-1)/2^{i+1}} = a^{(n-1)/2^{i+1}} \pmod{n}$$

или

$$(as)^{(n-1)/2^{i+1}} = (n-1)a^{(n-1)/2^{i+1}} \pmod{n},$$

а потому

$$(as)^{(n-1)/2^{i+1}} \neq 1 \pmod{n},$$
$$(as)^{(n-1)/2^{i+1}} \neq n-1 \pmod{n}.$$

Отсюда следует, что $as \notin S$. □

Лемма 6. Пусть $a, b \in \mathbb{Z}_n^*$, $a \neq b$. Множества S_a и S_b не пересекаются тогда и только тогда, когда не пересекаются множества $S_{ab^{-1}}$ и S.

Следствие 1. Пусть G – подгруппа $\mathbb{Z}_n^*$. Множества S_{g_1} и S_{g_2} не пересекаются при всех $g_1, g_2 \in S$, $g_1 \neq g_2$, тогда и только тогда, когда не пересекаются множества S и S_g для всех $g \in G$, $g \neq 1$.

Лемма 7. Если существует такое простое p, что n делится на p^2, то множество

$$G = \left\{ 1 + k\frac{n}{p} \pmod{n} \middle| k = 0, ..., p-1 \right\}$$

является подгруппой $\mathbb{Z}_n^*$.

Лемма 8. Пусть n - составное число, делящееся на p^2, где p – простое. Тогда

$$|S| \leq \frac{1}{4} |\mathbb{Z}_n^*|.$$

Доказательство. Пусть G – подгруппа $\mathbb{Z}_n^*$ из леммы 7. Поскольку n делится на p, то $n-1$ не делится на p, и тогда для любого $g \in G$, $g \neq 1$, выполняется $g^{n-1} \neq 1 \pmod{n}$. Поэтому $g \in A$ и по лемме 5 множества S и S_g не пересекаются. Отсюда и по следствию леммы 6 множества S_g, $g \in G$, попарно не пересекаются. Поэтому $\left|\bigcup_{g \in G} S_g\right| = |G| \cdot |S| = p|S|$, и $p|S| \leq |\mathbb{Z}_n^*| = \varphi(n)$, откуда

$$|S| \leq \frac{\varphi(n)}{p} \leq \frac{1}{4} |\mathbb{Z}_n^*|,$$

так как $p \geq 5$ по условию теоремы 16. □

Лемма 9. Пусть $n = p_1 p_2$, где p_1 и p_2 – различные простые числа. Тогда $n-1$ не делится на $p_1 - 1$ или на $p_2 - 1$.

Лемма 10. Пусть $n = p_1 p_2$, где $p_1 \neq p_2$. Тогда $|S| \leq \varphi(n)/4$.

Доказательство. Так как p_1, p_2 – простые числа, существуют первообразные корни по модулю p_1 и по модулю p_2. Пусть b_1, $1 < b_1 < p_1$ – первообразный корень по модулю p_1, а b_2, $1 < b_2 < p_2$ – первообразный корень по модулю p_2. В силу взаимной простоты чисел p_1, p_2, по китайской теореме об остатках, существует такое a_1, $1 < a_1 < n$, что

$$\begin{cases} a_1 = b_1 \pmod{p_1} \\ a_1 = 1 \pmod{p_2}, \end{cases}$$

и такое a_2, $1 < a_2 < n$, что

$$\begin{cases} a_2 = b_2 \pmod{p_2} \\ a_2 = 1 \pmod{p_1}. \end{cases}$$

Заметим, что $a_1^k \neq p_2 - 1 \pmod{p_2}$ для любого $k \in \mathbb{Z}$, а потому $a_1^k \neq n-1 \pmod{n}$, кроме того, порядок a_1 по модулю p_1 равен $p_1 - 1$. Это значит, что $a_1 \in A$. Заметим также, что $a_1^{-k} \neq n-1 \pmod{n}$, и порядок a_1^{-1} по модулю p_1 равен $p_1 - 1$, откуда получаем $a_1^{-1} \in A$.

Аналогичные рассуждения справедливы и для a_2, $a_2 \in A$, $a_2^{-1} \in A$.

Для элемента $a = a_1 a_2 \pmod{n}$, равенство $a^k = 1 \pmod{n}$ выполнено только в том случае, когда $a_1^k = 1 \pmod{p_1}$ и $a_2^k = 1 \pmod{p_2}$, откуда следует, что k должно делиться и на $p_1 - 1$, и на $p_2 - 1$. По лемме 9 получаем, что $k \neq n-1$, то есть $a^{n-1} \neq 1 \pmod{n}$. Таким образом, $a \in A$.

Аналогично, $a_1 a_2^{-1} \in A$.

Рассмотрим множества S, S_{a_1}, S_{a_2}, S_a. По леммам 5 и 6, эти множества не пере-

секаются. Кроме того, эти множества равномощны и содержатся в $\mathbb{Z}_n^*$. Поэтому

$$|S| \leq \frac{1}{4}\varphi(n).$$

□

Лемма 11. Пусть n бесквадратно и делится на три различных простых числа p_1, p_2, p_3. Тогда $|S| \leq \varphi(n)/4$.

Доказательство. Так как p_1, p_2 – простые числа, существуют первообразные корни по модулю p_1 и по модулю p_2. Пусть b_1, $1 < b_1 < p_1$ – первообразный корень по модулю p_1, а b_2, $1 < b_2 < p_2$ – первообразный корень по модулю p_2. В силу бесквадратности n, взаимно просты n/p_1 и p_1, а также n/p_2 и p_2. По китайской теореме об остатках, существует такое a_1, $1 < a_1 < n$, что

$$\begin{cases} a_1 = b_1 \pmod{p_1} \\ a_1 = 1 \pmod{\frac{n}{p_1}}, \end{cases}$$

и такое a_2, $1 < a_2 < n$, что

$$\begin{cases} a_2 = b_2 \pmod{p_2} \\ a_2 = 1 \pmod{\frac{n}{p_2}}. \end{cases}$$

Тогда $a_1 = 1 \pmod{p_3}$, $a_2 = 1 \pmod{p_3}$, $a_1 a_2 = a = 1 \pmod{p_3}$, $a_1 a_2^{-1} = b = 1 \pmod{p_3}$. Отсюда следует, что $a_1^k \neq n-1 \pmod{n}$, $a_2^k \neq n-1 \pmod{n}$, $a^k \neq n-1 \pmod{n}$, $b^k \neq n-1 \pmod{n}$ для любого $k \in \mathbb{Z}$. Значит, $a_1, a_2, a, b \in A$. Рассмотрим множества S, S_{a_1}, S_{a_2}, S_a. По леммам 5 и 6, эти множества не пересекаются. Кроме того, эти множества равномощны и содержатся в $\mathbb{Z}_n^*$. Поэтому

$$|S| \leq \frac{1}{4}\varphi(n).$$

□

МЕТОДЫ ФАКТОРИЗАЦИИ

Атака методом грубой силы на криптографическую систему RSA – разложение на множители модуля N. Таким образом, знание существующих методов факторизации необходимо для построения криптоаналитических атак на уязвимые реализации RSA.

5.1 Метод факторизации Ферма

Лемма 12. Пусть $N = pq$, $\Delta = |p - q|$. Тогда

$$0 < p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}}.$$

Доказательство. Заметим, что

$$\Delta^2 = p^2 - 2pq + q^2 = p^2 + 2pq + q^2 - 4N = (p+q)^2 - 4N = (p + q + 2\sqrt{N})(p + q - 2\sqrt{N}).$$

Таким образом,

$$p + q - 2\sqrt{N} > 0.$$

В силу истинности равенства

$$p + q - 2\sqrt{N} = \frac{\Delta^2}{p + q + 2\sqrt{N}}$$

и неравенства

$$p + q > 2\sqrt{N},$$

получим:

$$p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}}$$

□

Пусть $N = pq$, $p > q$, $\Delta = |p-q| < cN^{1/4}$. Требуется найти натуральные x и y ($x \neq n+1$, $y \neq n-1$) такие, что

$$4N = x^2 - y^2.$$

Перебираем значения $x = \lceil 2\sqrt{N} \rceil, \lceil 2\sqrt{N} \rceil + 1, \lceil 2\sqrt{N} \rceil + 2$, ... до тех пор, пока $x^2 - 4N$ не будет квадратом целого числа. Положим

$$p = \frac{1}{2}(x+y), q = \frac{1}{2}(x-y).$$

Вычислим количество значений, которое необходимо перебрать для факторизации N. По доказанной выше лемме:

$$x + 1 - \lceil 2\sqrt{N} \rceil \approx x - 2\sqrt{N} = p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}} < \frac{c^2}{4}$$

5.2 $(p-1)$-метод Полларда

Определение 36. Пусть m – натуральное число и разложение m на простые множители имеет вид:

$$m = \prod_{1 \leq i \leq k} q_i^{\alpha_i}.$$

Число m называется B-степенно-гладким, если для всех i, $1 \leq i \leq k$,

$$q_i^{\alpha_i} \leq B.$$

Пусть n – составное натуральное число, p – простой делитель n, такой, что число $p-1$ является B-степенно-гладким для некоторого B. Рассмотрим разложение $p-1$ на простые множители:

$$p - 1 = \prod_{1 \leq i \leq k} p_i^{\alpha_i}.$$

По определению, $p_i^{\alpha_i} \leq B$. Таким образом, $L = \text{НОК}(1,2,...,B)$ делится на $p-1$. По малой теорема Ферма, для любого натурального a, не делящегося на p:

$$a^L = 1 \pmod{p}.$$

Тогда НОД$(a^L - 1, n)$ делится на p.

Для всех простых чисел, не превосходящих B, $q_1 < q_2 < ... < q_k \leq B$ вычислим

$$\beta_i = \lfloor \log_{q_i} B \rfloor.$$

Выберем некоторое $a \in \mathbb{N}$, не делящееся на n, Убедимся, что НОД$(a,n) = 1$. В противном случае, нетривиальный делитель n найден.
Выберем некоторое натуральное k, вычислим:

$$P_k = a^{q_1^{\beta_1} q_2^{\beta_2} ... q_k^{\beta_k}}.$$

Если НОД$(P_k - 1, n) = 1$, вычисляем

$$P_{2k} = a^{q_1^{\beta_1} q_2^{\beta_2} ... q_{2k}^{\beta_{2k}}} = P_k a^{q_{k+1}^{\beta_{k+1}} q_{k+2}^{\beta_{k+2}} ... q_{2k}^{\beta_{2k}}}.$$

Значения $P_k, P_{2k}, P_{3k}, \ldots, P_{tk}$ вычисляются, пока для полученного на очередном шаге значения P_{tk} не будет выполнено неравенство:

$$\text{НОД}(P_{tk} - 1, n) > 1.$$

Последовательно вычисляем наибольшие общие делители

$$\text{НОД}(P_{(t-1)k}^{q_{(t-1)k+1}} - 1, n), \text{НОД}(P_{(t-1)k}^{q_{(t-1)k+1}^2} - 1, n), \ldots, \text{НОД}(P_{(t-1)k}^{q_{(t-1)k+1}^{\beta_{(t-1)k+1}}} - 1, n),$$
$$\text{НОД}(P_{(t-1)k}^{q_{(t-1)k+1}^{\beta_{(t-1)k+1}} q_{(t-1)k+2}} - 1, n), \ldots, \text{НОД}(P_{(t-1)k}^{q_{(t-1)k+1}^{\beta_{(t-1)k+1}} ... q_{tk}^{\beta_{tk}}} - 1, n),$$

пока не получим отличное от единицы значение.

Рассмотрим случай, когда $p-1$ не является B-степенно-гладким числом, но

$p-1=fr$, где f – B-степенно-гладкое число, а r – простое число, $B<r\leq B_1$.
Вычислим

$$b=a^{\text{НОК}(1,2,\ldots,B)} \pmod{n}.$$

В силу того, что $\text{НОК}(1,2,\ldots,B)$ делится на f,

$$b^r=1 \pmod{p},$$

а $\text{НОД}(b^r-1,n)$ будет делиться на p.
Находим все простые числа $r_1,r_2,\ldots,r_s$, $B<r_1<r_2<\cdots<r_s\leq B_1$, и вычисляем:

$$x_1=b^{r_1} \pmod{n},$$
$$x_i=b^{r_i} \pmod{n}=x_{i-1}b^{r_i-r_{i-1}} \pmod{n},$$

пока не получим $\text{НОД}(x_i-1,n)>1$.

5.3 ρ-метод Полларда

Пусть n – составное натуральное число, а p – некоторый неизвестный делитель n.

Рассмотрим некоторую функцию $f:\mathbb{Z}_n\to\mathbb{Z}_n$. Выберем произвольное $x_0\in\mathbb{Z}_n$. Рассмотрим последовательность

$$x_0,x_1=f(x_0),x_2=f(x_1),\ldots,x_i=f(x_{i-1}),\ldots$$

Заметим, что в силу конечности множества $\mathbb{Z}_n$

$$\exists i\geq 0,\exists t>0: x_i=x_{i+t}.$$

Тогда $x_{i+1}=f(x_i)=f(x_{i+t})=x_{i+t+1}$, откуда следует, что последовательность x_i является периодической, то есть

$$\exists m\geq 0,\exists t>0: x_j=x_{j+t} \text{ для } \forall j,j\geq m. \tag{4}$$

Наименьшее целое m из (4) будем называть предпериодом последовательности x_i, а наименьшее натуральное t – периодом этой последовательности.

Рассмотрим следующую последовательность элементов множества $\mathbb{Z}_p$

$$y_0 = x_0 \bmod p,$$
$$y_1 = x_1 \bmod p,$$
$$\dots$$
$$y_i = x_i \bmod p,$$
$$\dots$$

Последовательность y_i также периодична, через m_y обозначим предпериод этой последовательности, через t_y – ее период, $m_y \leq m$, $t_y \leq t$ и t делится на t_y.

Если $y_i = y_j$, существует такое $k \in \mathbb{Z}$, что

$$x_i - x_j = kp,$$

то есть НОД$(|x_i - x_j|, n)$ делится на p.

Построим последовательность z_i элементов из $\mathbb{Z}_n$:

$$z_0 = x_0, z_1 = f(f(z_0)), z_2 = f(f(z_1)), \dots, z_i = f(f(z_{i-1})), \dots$$

Очевидно, что $z_i = x_{2i}, \forall i$. Заметим, что для любых m_y и t_y существует $k \geq m_y$, делящееся на t_y. Таким образом,

$$\forall m_y, \forall t_y, \exists k \geq m_y : y_k = x_k \bmod p = z_k \bmod p = y_{2k}.$$

Алгоритм факторизации n состоит из следующих шагов:

1. Выберем функцию $f : \mathbb{Z}_n \to \mathbb{Z}_n$

2. Выберем $x_0 \in \mathbb{Z}_n$

3. $z_0 = x_0$

4. $i := 1$

5. $x_i = f(x_{i-1}), z_i = f(f(z_{i-1}))$

6. Если НОД$(|z_i - x_i|, n) = 1$, увеличиваем значение i на единицу и переходим к шагу 5.

7. Если $r =$ НОД$(|z_i - x_i|, n) < n$, r – выходное значение алгоритма, в противном случае делитель n найти не удалось.

Заключение

В данном учебном пособии представлено описание асимметричного криптографического алгоритма RSA, некоторых элементарных атак на этот алгоритм и методов факторизации. Пособие содержит необходимые для понимания этого материала сведения из теории чисел и линейной алгебры.

Литература

[1] Василенко О. Н. В19. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. — 328 с.

[2] Н. Смарт. Криптография. Москва: Техносфера, 2005. 528 с.

[3] Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. - М.: МЦНМО, 2006. - 91 с.

[4] Касселс, Дж В. С. Введение в геометрию чисел. Ed. А. В. Малышев. Мир, 1965.

[5] Курош, Александр Геннадиевич. "Курс высшей алгебры."(1968).

[6] Дж, Конвей. Упаковки шаров, решетки и группы. Мир, 1990.

[7] Дэвенпорт, Г. Высшая арифметика: Введение в теорию чисел. Ed. Ю. В. Линник. Наука. Гл. ред. физ.-мат. лит., 1965.

[8] Coppersmith, Don. "Finding a small root of a bivariate integer equation; factoring with high bits known."Advances in cryptology—EUROCRYPT'96. Springer Berlin Heidelberg, 1996.

[9] Coppersmith, Don. "Finding small solutions to small degree polynomials."Cryptography and lattices. Springer Berlin Heidelberg, 2001. 20-31.

[10] Coppersmith, Don. "Small solutions to polynomial equations, and low exponent RSA vulnerabilities."Journal of Cryptology 10.4 (1997): 233-260.

[11] Howgrave-Graham, Nicholas. "Finding small roots of univariate modular equations revisited."Crytography and Coding. Springer Berlin Heidelberg, 1997. 131-142.

[12] De Weger, Benne. "Cryptanalysis of RSA with small prime difference."Applicable Algebra in Engineering, Communication and Computing 13.1 (2002): 17-28.

[13] Boneh, Dan, and Glenn Durfee. "Cryptanalysis of RSA with private key d less than $N^{0.292}$."Information Theory, IEEE Transactions on 46.4 (2000): 1339-1349.

[14] Boneh, Dan. "Twenty years of attacks on the RSA cryptosystem."Notices of the AMS 46.2 (1999): 203-213.

[15] Wiener, Michael J. "Cryptanalysis of short RSA secret exponents."Information Theory, IEEE Transactions on 36.3 (1990): 553-558.

[16] Boneh, Dan, Glenn Durfee, and Yair Frankel. "Exposing an RSA private key given a small fraction of its bits."Full version of the work from Asiacrypt 98 (1998).

[17] Lenstra, Arjen, et al. "Factoring estimates for a 1024-bit RSA modulus."Advances in Cryptology-ASIACRYPT 2003. Springer Berlin Heidelberg, 2003. 55-74.

[18] Nguyen, Phong Q., and Jacques Stern. "The two faces of lattices in cryptology."Cryptography and lattices. Springer Berlin Heidelberg, 2001. 146-180.

[19] Hardy, Godfrey Harold, et al. An introduction to the theory of numbers. Vol. 4. Oxford: Clarendon press, 1979.

[20] Bellare, Mihir, and Phillip Rogaway. "Optimal asymmetric encryption."Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1995.

[21] Kaliski, Burt, and Jessica Staddon. PKCS# 1: RSA cryptography specifications version 2.0. RFC 2437, October, 1998.

Учебное издание

Разинков Евгений Викторович

ТЕОРИЯ ЧИСЕЛ И АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ

Подписано в печать
Бумага офсетная. Печать цифровая.
Формат 60x84 1/16. Гарнитура «Times New Roman». Усл. печ. л. .
Тираж экз. Заказ

Отпечатано с готового оригинал-макета
в типографии Издательства Казанского университета

420008, г. Казань, ул. Профессора Нужина, 1/37
тел. (843) 233-73-59, 233-73-28