Набережночелнинский институт
ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

Симметричные криптографичекие системы

Учебно - методическое пособие по дисциплине
«Информационная безопасность»

Набережные Челны
2018 г.

УДК 004.056.55 (075.8)
ББК 32.811.4я73
С37

Печатается по решению кафедры «Математические методы в экономике».

Рецензент: канд. экон. наук, доцент Карамышев А.Н.

Симметричные криптографичекие системы: учебно-методическое пособие по дисциплине «Информационная безопасность»/ Д.Р. Григорьева, Г.А. Гареева, Р.Р. Басыров - Набережные Челны: Изд-во НЧИ КФУ, 2018. - 30 с.

Учебно-методическое пособие содержит общее описание криптографических систем. Приведены методические указания к выполнению процедуры шифрования с использованием симметричных криптографичеких систем: шифры перестановки, шифры простой замены, методы шифрования. Предназначается для студентов очной формы обучения экономических специальностей (направлений подготовки)

© Д.Р. Григорьева, Г.А. Гареева, Р.Р. Басыров
©Набережночелнинский институт (филиал) ФГАОУ ВО НЧИ КФУ, 2018.

Оглавление

Введение

Криптография, или криптология, наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать без специального секретного ключа. В отечественном словоупотреблении термин «криптология» объединяет в себе «криптографию», т.е. шифрование сообщений, и «криптоанализ», т.е. несанкционированное расшифровывание сообщений. Исходное сообщение называется в криптографии открытым текстом, или клером. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или криптограммой. Процедура шифрования обычно включает в себя использование определенного алгоритма и ключа. Алгоритм – это определенный способ засекречивания сообщения, например компьютерная программа или, скажем, список инструкций. Ключ же конкретизирует процедуру засекречивания.

Человечество использует шифрование с того момента, как появилась первая секретная информация - такая, доступ к которой не должен быть публичным.

Суть шифрования заключается в предотвращении просмотра исходного содержания сообщения теми, у кого нет средств его дешифровки.

Основные понятия и определения

Алфавит - законченное множество используемых для кодирования информации символов.

Текст - упорядоченный последовательность из символов алфавита.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

- алфавит Z_{33} - 32 буквы русского алфавита и пробел;
- алфавит Z_{256} - символы, входящие в стандартные кодировки ASCII и КОИ-8;
- бинарный алфавит - $Z_2 = \{0,1\}$;
- восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование - процесс преобразования исходного текста (который носит также название открытого текста) в зашифрованный.

Дешифрование - обратный шифрованию процесс. На основе ключа зашифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T преобразований открытого текста. Составные этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей K - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптографичекие системы делят на:

- *симметричные*
- *ассиметричные (шифрование с открытым ключом).*

*Симметри́чные криптосисте́мы (*также *симметричное шифрование, симметричные шифры)* — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

В настоящее время симметричные шифры — это:

- блочные шифры. Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.
- поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

Виды симметричных шифров (блочные шифры)

- AES (англ. AdvancedEncryptionStandard) - американский стандарт шифрования
- ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ

- DES (англ. DataEncryptionStandard) - стандарт шифрования данных в США
- 3DES (Triple-DES, тройной DES)
- RC2 (ШифрРивеста (Rivest Cipher или Ron’s Cipher))
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (InternationalDataEncryptionAlgorithm, международный алгоритм шифрования данных)
- CAST (по инициалам разработчиков CarlisleAdams и StaffordTavares)
- CRAB
- 3-WAY
- Khufu и Khafre
- Kuznechik

потоковыешифры

- RC4 (алгоритм шифрования с ключом переменной длины)
- SEAL (SoftwareEfficientAlgorithm, программно-эффективный алгоритм)
- WAKE (WorldAutoKeyEncryptionalgorithm, всемирный алгоритм шифрования на автоматическом ключе)

В *ассиметричных* системах используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Содержание шифруется при помощи открытого ключа,

который находится в свободном доступе, а расшифровывается при помощи закрытого ключа, известного только адресату сообщения.

Цифровой подписью является присоединенное к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления штампа времени (timestamp) на документах: сторона, которой мы доверяем, подписывает документ со штампом времени с помощью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения (сертификации - tocertify) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ

и информация о том, кому он принадлежит подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом, возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим a-priori, что ему можно доверять). В централизованной инфраструктуре ключей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агенства; их также называют сертификационными агенствами - certificationauthorities). В распределенной инфраструктуре нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название сети доверия (weboftrust) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый дайджест (messagedigest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что

открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA.

Криптостойкостью является характеристика шифра, определяющая его стойкость к дешифрованию без наличия ключа.

Шифры перестановки

В шифрах перестановки все буквы открытого текста остаются в зашифрованном сообщении, но меняют свои позиции.

Шифрующие таблицы

Правила перестановки букв в сообщении задают шифрующие таблицы. В качестве ключа в шифрующих таблицах используются:

- Размер таблицы
- Слово или фраза, задающие перестановку
- Особенности структуры таблицы

Одним из самых примитивных табличных шифров перестановки является *простая перестановка*, для которой ключом служит размер таблицы.

Задача 1.1. Зашифровать методами простой перестановки сообщение:

НА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЗУЧАЕМ ШИФРЫ

Решение

Сообщение записывается в таблицу поочередно по столбцам. Считывание производится по строкам.

Н	О	И	Й	П	С	У	Ш
А	Р	О	Б	А	Т	Ч	И
И	М	Н	Е	С	И	А	Ф
Н	А	Н	З	Н	И	Е	Р
Ф	Ц	О	О	О	З	М	Ы

Шифр текста записывается группами по пять букв:

НОИЙП СУШАР ОБАТЧ ИИМНЕ СИАФН АНЗНИ ЕРФЦО ООЗМЫ

Отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Объединение букв шифртекста в 5-буквенные группы не входит в шифр текста и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Задача 1.2. – Зашифровать сообщение «Прежде чем сдаваться, вспомни ради чего ты все начинал» методом одиночной перестановки по ключу. В качестве ключа использовать слово СОТРУДНИК.

Таблица 1

С	О	Т	Р	У	Д	Н	И	К
7	5	8	6	9	1	4	2	3
П	Е	Д	Ь	П	Р	Е	В	Ч
Р	Ч	А	С	О	А	Г	С	И
Е	Е	В	Я	М	Д	О	Ё	Н
Ж	М	А	В	Н	И	Т	Н	А
Д	С	Т	С	И	Ч	Ы	А	Л

Таблица 2

Р	В	Ч	Е	Е	Ь	П	Д	П
А	С	И	Г	Ч	С	Р	А	О
Д	Ё	Н	О	Е	Я	Е	В	М
И	Н	А	Т	М	В	Ж	А	Н
Ч	А	Л	Ы	С	С	Д	Т	И

В верхней строке таблицы 1 записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были пронумерованы слева направо. В таблице 2 столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого нижней таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

РВЧЕЕ ЬПДПА СИГЧС РАОДЁ НОЕЯЕ ВМИНА ТМВЖА
НЧАЛЫ ССДТИ.

Задача 1.3. Зашифровать методом *двойной перестановки* сообщение:

ПРИЛЕТАЮ ВОСЬМОГО

Для шифрования использовать ключи:

По столбцам – 4132, по строкам – 3142

Решение:

Текст исходного сообщения записывается в таблицу 4*4, т.к. сообщение содержит 16 символов. Затем поочередно переставляются столбцы, а затем строки.

Исходная таблица				
	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Перестановка столбцов				
	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка строк				
	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Если считать шифротекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТЮАЕ ООГМ РЛИП ОЬСВ

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблиц:

- Для таблицы 3х3 – 36вариантов
- Для таблицы 4х4 – 576 вариантов
- Для таблицы 5х5 – 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто «взламывается» при любом разреме таблицы шифрования.

Задания для самостоятельного выполнения

1. Зашифровать методом двойной перестановки сообщение:

ЧУДЕСНАЯ ПОГОДА, ДА?

2. Зашифровать методом двойной перестановки сообщение: ЛЮБЛЮ УЧИТЬСЯ
3. Зашифровать методом двойной перестановки сообщение: КОНГРЕССЫ УЧЕНЫХ
4. Сообщение «ТНПВЕ ГЛЕАР АДОНР ТИЕЪВ ОМОБТ МПЧИР ЫСООЬ» зашифровано методом одиночной перестановки по ключу. Таблица имеет размерность 7Х5. Расшифровать сообщение.
5. Сообщение «РВЧЕЕ ЬПДПА СИГЧС РАОДЁ НОЕЯЕ ВМИНА ТМВЖА НЧАЛЫ ССДТИ» зашифровано методом одиночной перестановки по ключу. В качестве ключа использовано слово СОТРУДНИК. Расшифровать сообщение.
6. Сообщение «ИЕОСУ АКХДЬ ЧЙОНР УИТМЕ АВТЕУ ПЖСЕН» зашифровано методом одиночной перестановки по ключу. В качестве ключа использовано слово СОЛНЦЕ. Расшифровать сообщение.
7. Сообщение «ЯЛОО ИЕЛЮ ШЛЛН ЮООА ЬЬБЧ КДНС» зашифровано методом одиночной перестановки по ключу. В качестве ключа использовано слово ВКУСНО. Расшифровать сообщение.
8. Сообщение «КУРЖДИЧ ЬИЬХШОЗ УКЕННЧН ВАИИИСВ ВТГЯЕЕЛ» зашифровано методом одиночной перестановки по ключу. В качестве ключа использовано слово ТРУБА. Расшифровать сообщение.
9. Сообщение «ДГМ НЕС ЕЛИ АНТ ТАР ЯНЬ ИВЕ ЦОВ» зашифровано методом одиночной перестановки по ключу. В

качестве ключа использовано слово ЖЕЛТЫЙ. Расшифровать сообщение.

Шифрование магическими квадратами

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифротекст, сформированный благодаря перестановке букв исходного сообщения. Считалось, что созданные с помощью магических квадратов шифротексты охраняет не только ключ, но и магическая сила.

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3. Количество магических квадратов 4x4 – 880, а 5x5 – 250000.

Задача 1.4. Зашифровать сообщение:

«ПРИЛЕТАЮ ВОСЬМОГО» с помощью магического квадрата. Считать шифротекст построчно блоками по четыре буквы.

Решение:

Используем магический квадрат 4x4 и заполним его заданным сообщением. В начале пронумеруем буквы:

ПРИЛЕТАЮ ВОСЬМОГО
1234567891011121314 1516

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Таблица 1.3. – Магический квадрат 4x4 и его заполнение сообщением

Шифротекст, получаемый при считывании содержимого таблицы по строкам,имеет вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Задания для самостоятельной работы

1. Сообщение «ИДАО СНОЫ ЕТНВ ОТСР» зашифровано методом магический квадрат 4х4.
2. Сообщение «ЕНС ГЙБ ЫЛЕ» зашифровано методом магический квадрат 3х3.
3. Сообщение «ЕЛПА ВКОН ААЮР ЫЛБУ» зашифровано методом магический квадрат 4х4.
4. Сообщение «ИМЙ ЧЫЧ ТСЯ» зашифровано методом магический квадрат 3х3.
5. Сообщение «ОНБ КЕВ ШЛИ» зашифровано методом магический квадрат 3х3.
6. Сообщение «АТЕЧ ДИАО ГОЛУ АТЕМ» зашифровано методом магический квадрат 4х4.

Шифры простой замены

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита по заранее установленным правилам замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки. Одним из важных подклассов методов замены являются одноалфавитные (или моноалфавитные) подстановки, в которых устанавливается однозначное соответствие между каждым знаком ai исходного алфавита сообщений A и соответствующим знаком ei зашифрованного текста E. Одноалфавитная подстановка иногда называется также простой заменой, так как является самым простым шифром замены.

Шифрование на основе квадрата Полибия (полибианского квадрата)

Полибианский квадрат выглядит следующим образом:

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	κ
χ	ν		φ	ι

Таблица 3 – Полибианский квадрат

Для шифрования в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже нее в том же столбце. Если буква текста оказывалась в нижней строчке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца.

Задача 1.5. Зашифровать сообщение ταυροδ с помощью полибианского квадрата.

Решение:

Шифртекст имеет вид κφδμτβ

Система шифрования Цезаря

Один из самых известных методов шифрования является метод Цезаря, которым активно пользовался римский император. Не имея доверия к своим посыльным, он шифровал письма элементарной заменой A на D, B на E и так далее по латинскому алфавиту. К примеру, при таком кодировании последовательность ABC была бы записана как DEF.

Спустя пол века шифрование стало использоваться уже повсеместно при составлении текстов религиозного содержания, молитв и важных государственных документов.

Шифр цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на k букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении k=3. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртектса.

Таблица4

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

Таблица4. – Таблица подстановок Цезаря

Задача 1.6. – Зашифровать послание Цезаря: VENIVIDIVICI

Решение:

Используя таблицу подстановок (Таблица4) получаем шифртекст:

YHQLYLGLYLFL

Система Цезаря с ключевым словом

Система шифрования Цезаря с ключевым словом является одноалфавитной системой подстановок. Особенностью этой системы является использование ключевого слова для смещения и изменения порядка символов в алфавитной подстановке.

Задача 1.7. Зашифровать сообщение «SENDMOREMONEY» по системе Цезаря с ключевым словом DIPLOMAT.

Решение:

Выберем некоторое число k, $0 \le k \le 25$ Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код который совпадает с выбранным числом k:

012345 10 15 20 25

ABCDEFGIJKLMNOPQRSTUVWXYZ

DIPLOMAT

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

ABCDEFGIJKLMNOPQRSTUVWXYZ

VWXYZDIPLOMATBCEFGHJKNQRSU

Теперь мы имеем подстановку для каждой буквы произвольного сообщения.

Исходное сообщение SENDMOREMONEY

Шифруется как HZBYTCGZTCBZS

Разновидностью рассмотренной системы, является система, в которой требование о различии всех букв ключевого слова не является обязательным. В этом случае ключевое слово (или фраза) записывается без повторения одинаковых букв.

Задача 1.8. Сформировать таблицу подстановок в системе с ключевой фразой

КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН

Полагая k=3 и исключая повторяющиеся буквы в ключевой фразе, получим следующую систему подстановок:

0 3

АБВГДЕЖЗИЙКЛМОПРСТУФХЦЧШЩЬЫЪЭЮЯ

ЪЭЮКАДЫМОТЕЧСВНЛИПРЯГЖЗЙУФХЦШЩЬ

Достоинством системы Цезаря с ключевым словом является то, что количество возможных ключевых слов практически неисчерпаемо. Недостатком этой системы является возможность взлома шифртекста на основе анализа частот появления букв.

Шифрующие таблицы Трисемуса

В 1508г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющееся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Задача 1.9. Зашифровать таблицей Трисемуса сообщение:

ВЫЛЕТАЮ ПЯТОГО

Решение:

Для русского алфавита шифрующая таблица может иметь размер 4х8. Шифрующая таблица выглядит так:

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

Таблица5. – Шифрующая таблица Трисемуса с ключевым словом БАНДЕРОЛЬ

Используя эту таблицу в соответствии с вышеизложенной методикой, получаем шифртекст

ПДКЗЫВЗЧШЛЫЙСЙ

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются *биграммными*.

Биграммный шифр Плейфейра

Шифр Плейфейра, изобретенный в 1854г. является наиболее известным биграммным шифром замены. Он применялся Великобританией во времена первой мировой войны. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщение.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущей задачи.

Процедура шифрования включает следующие шаги.

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

а) Если обе буквы биграммы открытого текста не попадают на одну строку или столбец, тогда находят буквы в углах прямоугольника, определяемого данной парой букв

б) Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними. Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца.

в) Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них.

Задача 1.10. Зашифровать биграммным шифром Плейфейра текст

ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ

Решение:

Разобьем этот текст на биграммы:

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в следующую последовательность биграмм шифртекста

ГП ДУ ОВ ДЛ НУ ПД ДР ЦЫ ГА ЧТ

При расшифровании применяется обратный порядок действий.

Шифрование биграммами резко повышает стойкость шифров к вскрытию. Хотя книга И.Трисемуса «Полиграфия» была относительно доступной, описанные в ней идеи получили признание лишь спустя три столетия. По всей вероятности, это было обусловлено плохой осведомленностью криптографов о работе богослова и библиофила Трисемуса в области криптографии.

Задания для самостоятельной работы

1. Зашифровать сообщение οδατρυ с помощью полибианского квадрата.
2. Зашифровать сообщение ζτμαυροδβ с помощью полибианского квадрата.
3. Зашифровать ροβζτμαυδ с помощью полибианского квадрата.
4. Зашифровать сообщение с помощью таблицы подстановок Цезаря: VISHAYAMATEMATIKA
5. Зашифровать сообщение с помощью таблицы подстановок Цезаря: SLOGNYIALGORITM
6. Зашифровать сообщение WANTTOBEHAPPY по системе Цезаря с ключевым словом DIPLOMAT.

Методы шифрования

Метод перестановок на основе маршрутов Гамильтона

Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходный текст разбивается на блоки. Если длина шифруемого текста не кратна длине блока, то на свободные места последнего блока помещаются служебные символы-заполнители(например,*)

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбирают либо последовательно, либо их очередность задается ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки

Фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходный текст на шаге 1.

Расшифрование производится в обратном порядке.

Задача 2.1. Требуется зашифровать текст $T_o =$<Экономическая теория>. Ключ и длины зашифрованных блоков равны: $K =< 2,1,1 >$, $L = 4$. Для шифрования использовать таблицу и два маршрута, представленные на рис.2.1.

Решение:

Воспользуемся вышеизложенной методикой построения шифра по шагам.

Шаг 1. Исходный текст разбивается на 3 блока:

Блок $Б_1$=<Экономич>

Блок $Б_2$=<Ская*тео>

Блок $Б_3$=<рия*****>

Шаг 2. Заполняется 3 матрицы с маршрутами 1(рис.2.2).

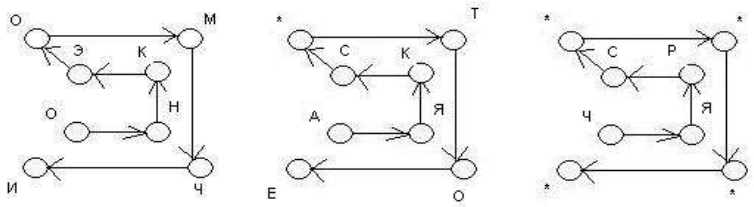

Рис.2.2. – Шифрование с помощью маршрутов Гамильтона

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

$T_1 =$<ОНКЭОМИЧАЯКС*ТОЕИЯРС***** >

Шаг 4. Разбиение на блоки шифртекста

$T_1 =$<ОНКЭ ОМИЧ АЯКС *ТОЕ ИЯРС **** >

Возможно применение и других маршрутов.

Аналитические методы шифрования

Среди аналитических методов наибольшее распространение получили методы, основанные на использовании матриц. Зашифрование k-го блока исходной информации, представленного в виде вектора $B_K = \|в_\varphi\|$ осуществляется путем перемножения матрицы ключа $A = \|a_\varphi\|$ вектора B_K. В результате перемножения получается блок шифртекста в виде вектора $C_K = \|c_\varphi\|$, где элементы вектора C_K определяется по формуле:

$$C_i = \sum_{j=1} a_{ij} b_j \quad (2.1.)$$

Расшифрование информации осуществляется путем последовательного перемножения вектора C_K и обратной матрицы A^{-1}.

Среди аналитических методов наибольшее распространение получили методы, основанные на использовании матриц. Зашифрование К-го блока исходной информации, представленного в виде вектора $B_K = \|в_\varphi\|$ осуществляется путем перемножения матрицы ключа $A = \|a_\varphi\|$ вектора B_K.

В результате перемножения получается блок шифртекста в виде вектора $C_K = \|c_\varphi\|$, где элементы вектора C_K определяется по формуле:

$$C_i = \sum_{j=1} a_{ij} b_j \quad (2.1.)$$

Расшифрование информации осуществляется путем последовательного перемножения вектора C_K и обратной матрицы A^{-1}

Задача 2.2. Требуется зашифровать слово T_o =<БИЗНЕС> с помощью матрицы ключа A.

$$A = \begin{bmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{bmatrix}$$

Решение:

1. Определим числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слова T_o:

   $\grave{O}_{\acute{y}} = <3,9,8,13,6,17>$

2. Разобьем $T_э$ на два вектора $B_1 = [8,1,2]$ и $B_2 = [1,3,1]$.
3. Умножим матрицу A на векторы B_1 и B_2:

$$\tilde{N}_1 = \begin{bmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{bmatrix} * \begin{bmatrix} 2 \\ 9 \\ 8 \end{bmatrix} = \begin{bmatrix} 102 \\ 85 \\ 133 \end{bmatrix}$$

$$\tilde{N}_2 = \begin{bmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{bmatrix} * \begin{bmatrix} 13 \\ 6 \\ 17 \end{bmatrix} = \begin{bmatrix} 172 \\ 115 \\ 217 \end{bmatrix}$$

4. Зашифрованное слово запишем в виде последовательности чисел $\grave{O}_1 = <102,85,133,172,115,217>$

Задача 2.3. Расшифровать текст, полученный в задаче 2.2.

Решение:

1. Вычислить определитель $|A| = -115$
2. Определяется присоединенная матрица A^*, каждый элемент которой является алгебраическим дополнением элемента a_{ij} матрицы A**:**

$$A^* = \begin{bmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{bmatrix}$$

3. Получается транспонированная матрица A^T

$$A^{T*} = \begin{bmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{bmatrix}$$

4. Вычисляется обратная матрица A^{-1} по формуле:

$$A^{-1} = \frac{A^T}{|A|}$$

В результате вычислений обратная матрица имеет вид:

$$A^{-1} = \begin{bmatrix} 17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{bmatrix}$$

5. Определяются векторы B_1 и B_2:

$$B_1 = A^{-1} * C_1 ; B_2 = A^{-1} * C_2$$

$$B_1 = \begin{bmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{bmatrix} \begin{bmatrix} 2 \\ 9 \\ 8 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \\ 8 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{bmatrix} \begin{bmatrix} 13 \\ 6 \\ 17 \end{bmatrix} = \begin{bmatrix} 13 \\ 6 \\ 17 \end{bmatrix}$$

6. Получаем числовой эквивалент расшифрованного слова:

$T_{,} =< 2,9,8,13,6,17 >$, который заменяется символами, в результате получается исходное слово$T_o =<$ Бизнес $>$

Список использованных источников

1. А.В. Крыжановский, Н.В. Киреева, В.В. Пугин. Методические разработки к лабораторным работам по дисциплине "Средства обеспечения информационной безопасности в сетях передачи данных". Самара: ИНУЛ ПГУТИ, 2008. 60с.
2. http://www.intuit.ru/studies/courses/108/108/lecture/3141
3. В.И.Ярочкин. Информационная безопасность: учебник для студентов вузов. — М.: Академический Проект; Гаудеамус. - 2-е изд.— 2004. — 544 с. (Gaudeamus).
4. В.Л. Цирлов. Основы информационной безопасности // Феникс. - 2008.
5. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков Теоретические основы компьютерной безопасности. – М.: Радио и связь, – 2000.

Подписано в печать 26.03.2018г.
Формат 60х84/16 Бумага офсетная Печать ризографическая
Усл.-печ. л.2 Тираж 50 экз
Заказ 472
Издательско-полиграфический центр
Набережночелнинского института «Казанского (Приволжского) федерального университета»
_____
423810, Набережные Челны, проспект Мира, 68/19
Тел. / факс (8552) 39-65-99 e-mail: ic-nchi-kpfu@mail.ru