Защита информации

Проблема защиты информации

Проблема защиты информации от несанкционированного(самовольного) доступа (НСД) заметно обострилась в связи с широким распространением локальных и особенно глобальных компьютерных сетей.

Защита информации необходима для уменьшения вероятности утечки(разглашения), модификации(умышленного искажения) или утраты (уничтожения) информации, представляющей определенную ценность для её владельца.

Основные понятия

- **Криптология** - наука, которая делится на две науки: криптография и криптоанализ.
- **Криптография** - наука, которая изучает преобразования, которые делают смысл информации непригодным для злоумышленника.
- **Криптоанализ** - наука, которая изучает нахождение смысла информации без доступа к секретному параметру системы (ключу).
- **Ключ** - уникальное состояние некоторого параметра системы, которое позволяет из множества возможних отображений выбрать нужное. Простыми словами, **ключ** - это секретный параметр системы шифрования.
- **Шифр** - мат. функция, которая преобразовывает открытый блок данных на основе секретного параметра (ключа). Другими словами, **шифр** - алгоритм, с помощью которого выполняется и шифрование и расшифрование данных.

Основные понятия

- **Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.
- **Расшифровывание** — процесс нормального применения криптографического преобразования шифрованного текста в открытый.
- **Дешифрование (дешифровка)** — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе шифросистемы, а не только зашифрованного ею открытого сообщения).
- **Криптографическая стойкость** — способность криптографического алгоритма противостоять криптоанализу.

История возникновения шифров

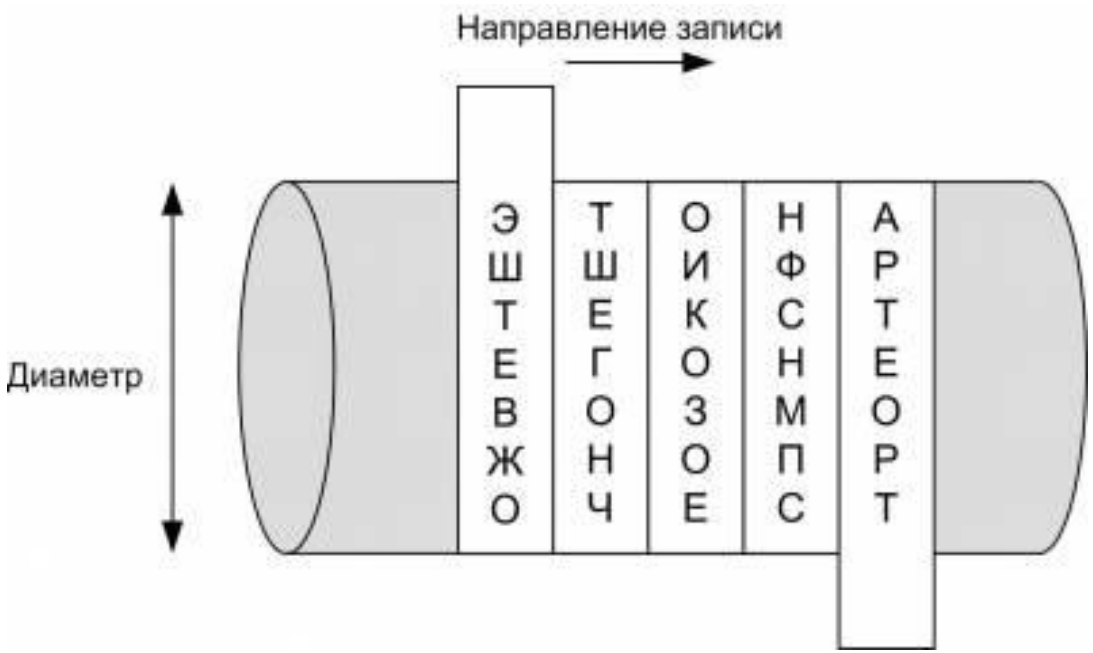
Проблема защиты информации волнует людей несколько столетий. По свидетельству Геродота , уже в v в.до н.э. использовалось преобразование информации методом кодирования.

Одним из первых шифровальных приспособлений была **СКИТАЛА**, которая применялась в v в. До н.э. во время войны Спарты против Афин.

СКИТАЛА -это цилиндр, на который виток к витку наматывалась узкая папирусная лента(без пробелов и нахлестов). Затем на этой ленте вдоль оси цилиндра (столбцами) записывался необходимый для передачи текст. Лента сматывалась с цилиндра и отправлялась получателю. Получив такое сообщение, получатель наматывал ленту на цилиндр такого же диаметра , как и диаметр СКИТАЛЫ отправителя. В результате можно было прочитать зашифрованное сообщение.

Аристотелю принадлежит идея ВЗЛОМА такого шифра. Он предложил изготовить длинный конус и , начиная с основания , обертывать его лентой с шифрованным сообщением , постепенно сдвигая её к вершине. На каком-то участке конуса начнут просматриваться участки читаемого текста. Так определяется секретный размер цилиндра.

Шифр перестановки "Скитала"



В результате преобразования сообщения **ЭТО НАШ ШИФРТЕКСТ, ЕГО НЕВОЗМОЖНО ПРОЧЕСТЬ** при использовании шифра «скитала» получится **ЭШТЕВ ЖОТШЕ ГОНЧО ИКОЗО ЕНФСН МПСАР ТЕОРТ**.

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра

Шифры появились в глубокой древности в виде криптограмм(по-гречески -тайнопись). Порой священные иудейские тексты шифровались методом замены. Вместо первой буквы алфавита записывалась последняя буква, вместо второй – предпоследняя и т.д. Этот древний шифр назывался АТБАШ. Известен факт шифрования переписки Юлия Цезаря (100-44 до н.э.) с Цицероном (106-43 до н.э.).

Шифр Цезаря реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей от неё в алфавите на фиксированной число букв. В своих шифровках Цезарь заменял букву исходного открытого текста буквой, отстоящей от исходной буквы впереди на три позиции.

Применение магических квадратов

В средние века для шифрования перестановкой применялись и магические квадраты. 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. В те времена считалось, что созданные с помощью магических квадратов шифротексты охраняет не только ключ, но и магическая сила.

Применение магических квадратов

ЭТО КРИПТОГРАФИЯ

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

Я	О	Т	А
К	О	Г	П
Т	Р	И	Р
	И	Ф	Э

Шифротекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид: **ЯОТА КОГП ТРИР ИФЭ**

Квадрат ПОЛИБИЯ

В Древней Греции был известен шифр, который создавался с помощью КВАДРАТА ПОЛИБИЯ. Таблица для шифрования представляла собой квадрат с пятью столбцами и пятью строками , которые нумеровались цифрами от 1 до 5.В каждую клетку такой таблицы записывалась одна буква. В результате каждой букве соответствовала пара цифр , и шифрование сводилось к замене буквы парой цифр.

Идею ПОЛИБИЯ проиллюстрируем таблицей с русскими буквами. Число букв в русском алфавите отличается от числа букв от в греческом алфавите , поэтому и размер таблицы выбран иным (квадрат 6×6). Заметим , что порядок расположения символов квадрате Полибия является секретной информацией(ключом).

	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**	**,**	**.**	**-**

Зашифруем с помощью квадрата ПОЛИБИЯ слово КРИПТОГРАФИЯ:

26 36 24 35 42 34 14 36 11 44 24 63

Из примера видно , что в шифрограмме первым указывается номер строки, а вторым- номер столбца

	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	,	.	-

Блез де Виженер - шифр Виженера

Этот шифр удобнее всего представлять себе как шифр Цезаря с переменной величиной сдвига. Чтобы знать, на сколько сдвигать очередную букву открытого текста, заранее договариваются о способе запоминания сдвигов. Сам Виженер предлагал запоминать ключевое слово, величину сдвига. Существует алгоритм шифрования по таблице Виженера

Алгоритм шифрования по таблице Виженера:

- 1-я строка - фраза для шифрования;
- 2-я строка - номера букв фразы для шифрования в русском алфавите;
- 3-я строка- ключевое слово с длиной равной длине фразы;
- 4-я строка - номера букв ключевого слова в алфавите;
- 5-я строка - сумма номеров 2-й и 4-й строк в соответствующих столбцах;
- 6-я строка - результат «вычитания полного оборота» 33 буквы;
- 7-я строка - зашифрованная фраза.

Дешифровка осуществляется по обратному алгоритму, с учётом того, что 5-я строка - разность 2-й и 4-й строки. Если число 2-й строки меньше числа 4-й строки, считаем так: 33 + число 2-й строки – число 4-й строки.

А-1 Б-2 В-3 Г-4 Д-5 Е-6 Ё-7 Ж-8 З-9 И-10 Й-11 К-12 Л-13 М-14 Н-15 О-16 П-17 Р- 18 С-19 Т- 20 У-21 Ф-22 Х-23 Ц- 24 Ч-25 Ш-26 Щ-27 Ъ- 28 Ы-29 Ь-30 Э-31 Ю-32 Я-33

Таблица Виженера

В примере в качестве ключевого используется слово ХОЛМС.
Пусть надо зашифровать сообщение
ПРИХОДИ НЕМЕДЛЕННО
Для этого пишется ключевое слово над шифруемой фразой:

Х	О	Л	М	С	Х	О		Л	М	С	Х	О	Л	М	С	Х	О
П	Р	И	Х	О	Д	И		Н	Е	М	Е	Д	Л	Е	Н	Н	О

Теперь каждую букву сообщения надо сдвинуть вперёд по алфавиту в соответствии с буквой ключевого слова, стоящей над ней. Например, буква Х является двадцать второй буквой алфавита и задаёт сдвиг на двадцать одну позицию вперёд. Вместо буквы П исходного текста получится буква Д зашифрованного сообщения. Вторая буква — Р— исходного сообщения сдвигается в соответствии с буквой О ключевого слова на 14 позиций вперёд и заменяется на букву Ю. И так далее:
ДЮУБЯЩЦ ШСЭЪТЦСЮВЬ

Современная криптография

Для современной криптографии характерно использование **открытых** алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных **алгоритмов** шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма криптографически стойки.

Распространенные алгоритмы:

- **симметричные** DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и др.;
- **асимметричные** RSA и Elgamal (*Эль-Гамаль*);
- **хэш-функций** MD4, MD5, SHA-1, ГОСТ Р 34.11-94.

Симметричное шифрование (с секретным ключом)

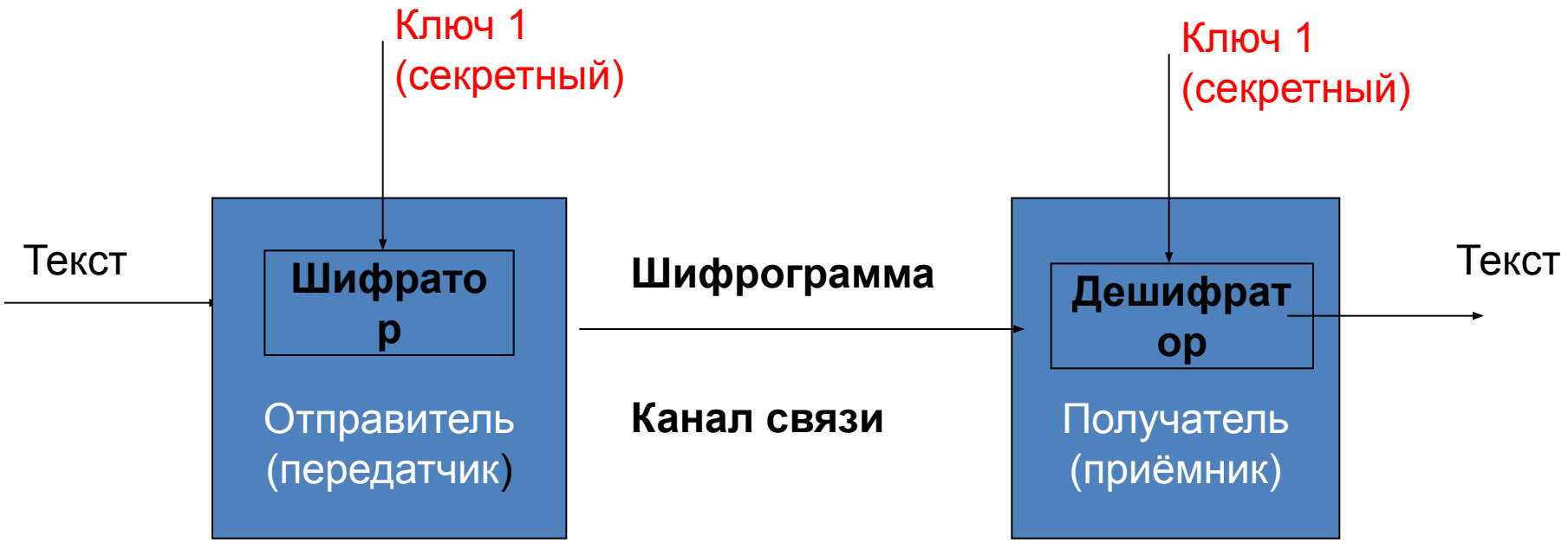
В шифраторе отправителя и дешифраторе получателя используется один и тот же ключ.

Шифратор образует шифрограмму, которая является функцией открытого текста. Дешифратор получателя сообщения выполняет обратное преобразование по отношению к преобразованию , сделанному в шифраторе.

Секретный ключ хранится в тайне и передаётся по каналу, исключающему перехват ключа криптоаналитиком противника или коммерческого конкурента.

При оценке эффективности шифра обычно руководствуется правилом голландца О. Керкхоффа (1835-1903), согласно которому стойкость шифра определяется только секретностью ключа ,т.е устойчивость к криптоанализу.

Симметричное шифрование (с секретным ключом)



В США для передачи секретных сообщений наибольшее распространение получил стандарт DES (Data Encryption StandarD).

Стандарт DES является блочным шифром.

Он шифрует данные блоками по 64 бита. При шифровании используется ключ длиной 56 битов. Данный стандарт подвергался многократному детальному криптоанализу. Для его взлома были разработаны специализированные ЭВМ стоимостью, достигавшей 20 млн долларов.

4. Асимметричное шифрование

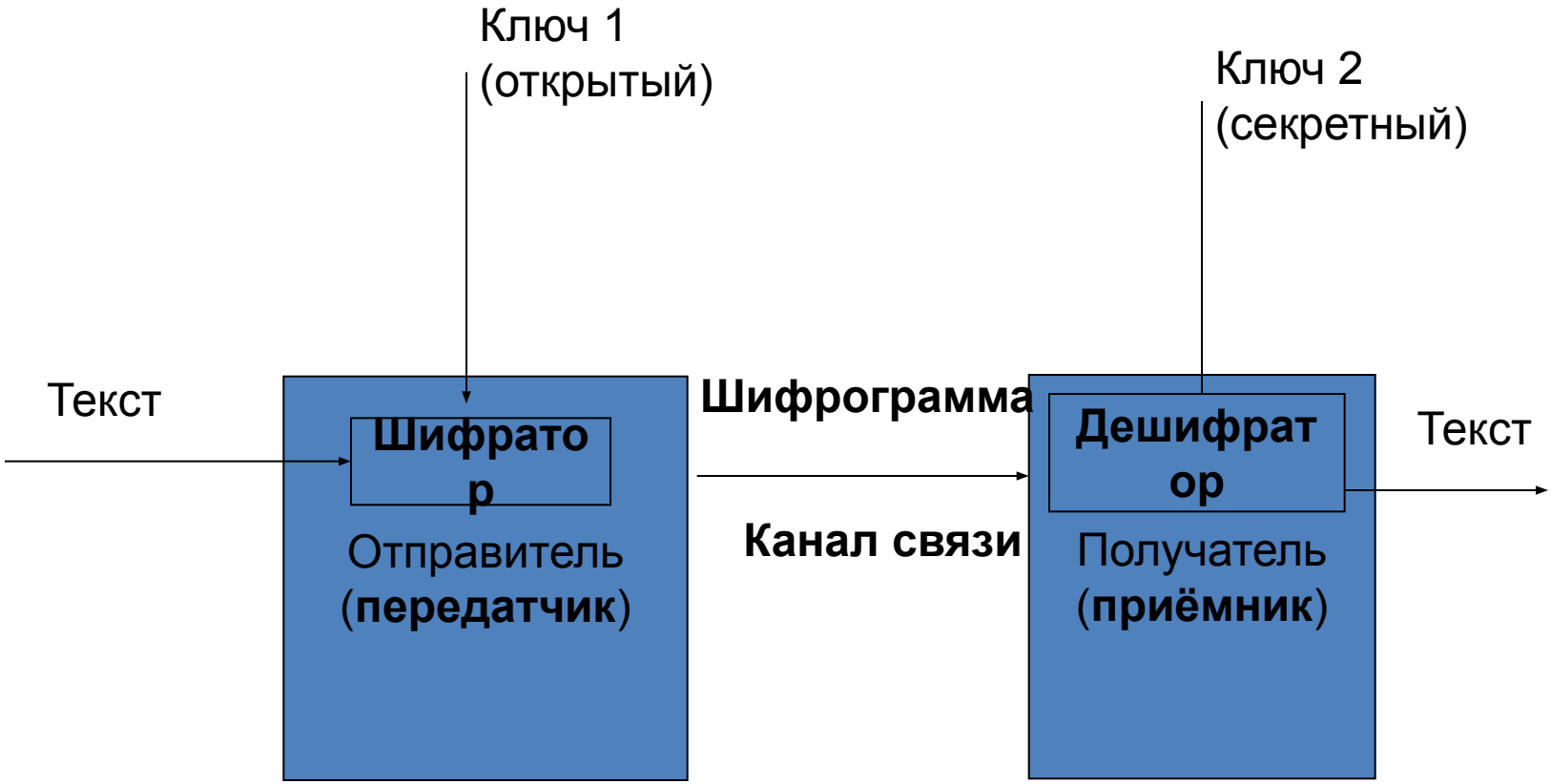
Несимметричные (с двумя ключами или с открытым ключом).

Получатель вначале по **открытому** каналу передаёт отправителю **открытый** ключ, с помощью которого отправитель шифрует информацию. При получении информации получатель дешифрирует её с помощью **второго** секретного ключа.

Перехват **открытого** ключами **криптоаналитиком** противника не позволяет дешифровать закрытое сообщение, так как оно рассекречивается лишь вторым секретным ключом.

Секретный ключ2 практически невозможно вычислить с помощью открытого ключа. В асимметричных системах приходиться применять длинные ключи(2048 бита и больше). Длинный ключ увеличивает время шифрования открытого сообщения. Кроме того, генерация ключей становиться весьма длительной. Зато пересылать открытые ключи можно по незащищенным каналам связи. Это особенно удобно для коммерческих партнеров, разделенных большими расстояниями.

Асимметричное шифрование (с открытым и секретным ключами)



Алгоритмы шифрования с открытым ключом так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством, при заданном значении аргумента x относительно просто вычислить значение функции f(x). Все используемые в настоящее время криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований.

1.Разложение больших чисел на простые множители(алгоритм RSA, авторы- Райвест, Шамир и Адлеман- RIVEST,SHAMIR, ADLEMAN.)

2.Вычисление логарифма или возведение в степень(алгоритм DH, авторы- Диффри и Хелман.)

3.Вычисление корней алгебраических уравнений.

В симметричных алгоритмах используется более короткие ключи, поэтому шифрование и дешифрование происходят быстрее. Но в таких системах рассылка ключей является сложной процедурой. Передавать ключи нужно по закрытым (секретным) каналам. Использование курьеров для рассылки секретных ключей дорогая, сложная и медленная процедура.

Практический пример работы RSA

Рассмотрим небольшой пример, иллюстрирующий применение алгоритма RSA.
Пусть требуется зашифровать сообщение “CAB”.
Для простоты будем использовать маленькие числа (на практике применяются гораздо большие). Пошагово проследим процессы шифрования и дешифрования.

1. Выберем $p = 3$ и $q = 11$.
2. Определим $n = 3 * 11 = 33$.
3. Найдем $(p – 1)(q – 1) = 20$. Следовательно, в качестве e можно взять число, взаимно простое с 20, например, $e = 3$.
4. Выберем число d. В качестве такого числа может быть взято любое число, для которого выполняется соотношение
$(d * 3) = 1 (\mathrm{mod}\ 20)$, например 7.

5. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: A -> 1, B-> 2, C-> 3. Тогда исходное открытое сообщение принимает вид M = (3,1,2). Зашифруем сообщение с помощью ключа {7, 33}:

s1 = (3 в степени 7) (mod 33) = 2187 (mod 33) = 9,

s2 = (1 в степени 7) (mod 33) = 1 (mod 33) = 1,

s3 = (2 в степени 7) (mod 33) = 128 (mod 33) = 29.

Зашифрованное сообщение после этого примет вид S = (9, 1, 29).

6. Расшифруем полученное зашифрованное сообщение (9, 1, 29) на основе секретного ключа {3, 33}:

m1 = (9 в степени 3) (mod 33) = 729 (mod 33) = 3,

m2= (1 в степени 3) (mod 33) = 1 (mod 33) = 1,

m3 = (29 в степени 3) (mod 33) = 24389 (mod 33) = 2.

Как можем видеть, дешифрование шифртекста S = (9, 1, 29) привело к исходному открытому тексту M = (3, 1, 2).

Современная история

Шифрование с открытым ключом представляет несомненный интерес, поскольку его легко применять, и оно решает ряд до его появления нерешенных проблем с авторизацией. Точнее, оно решает всего несколько таких проблем.

- **Идентификация пользователя.**
- **Аутентификация документа и т.п.**

1. **Идентификация пользователя.** Мы пользуемся современными средствами связи, позволяющими отправителю оставаться неизвестным, но хотим быть уверенными в том, что тот, с кем мы общаемся, — действительно тот, за кого себя выдает. Для этого используется протокол идентификации. Таковых существует великое множество, и основаны они, в большинстве своем, на принципах RSA или дискретного логарифмирования.

2. **Аутентификация документа.** Автор удостоверяет документ при помощи цифровой подписи. Операция подписи добавляет к сообщению несколько бит, которые являются результатом некоей операции над самим документом и сведениями об авторе, биты эти, как правило, хэшируются с использованием одного из известных алгоритмов MD5 или SHA. Более того, любой, кто имеет доступ к документу, должен иметь и возможность проверить, действительно ли подпись под ним поставлена автором. Для этого используются схемы подписи, наиболее известной среди которых является Elgamal, — также построенная на решении задачи дискретного логарифмирования.

3. И, кроме того, как и шифрование с секретным ключом, шифрование с открытым ключом является криптосистемой, гарантирующей **конфиденциальность информации**.

Известно множество криптосистем с открытым ключом — это Elgamal (названная в честь ее изобретателя Тахира Эльгамаля), Diffie-Hellman (названная, правильно, в честь ее создателей), DSA — Digital Signature Algorithm (изобретенный Дэвидом Кравицом).

Следует заметить ,что , по мнению некоторых специалистов , нет нераскрываемых шифров. Рассекретить(взломать) любую шифрограмму можно либо за большое время , либо за большие деньги. Во втором случае для дешифрования потребуется несколько суперокомпьютеров, что приведет к значительным материальным затратам. Все чаще для взлома секретных сообщений используют распределенные ресурсы Интернета, распараллеливая вычисления и привлекая к расчетам сотни и даже тысячи рабочих станций…