ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Практическая работа 2 - Основы криптографии

Учебные вопросы

1. Основные термины криптографии.
2. Шифр Цезаря.
3. Шифр Виженера.
4. Симметричные криптосистемы
5. Асимметричные криптосистемы шифрования.
6. Криптографические хеширующие алгоритмы.
7. Криптографические протоколы.

1. Основные термины криптографии

- **Криптография** - это наука о сохранении секретов.
- В сущности, криптографию можно рассматривать как способ сохранения больших секретов (которые неудобно хранить в тайне из-за их размеров) при помощи секретов малых (которые прятать проще и удобней).
- Под «большими секретами» имеется в виду, как правило, так называемый открытый текст, а «малые секреты» обычно называют криптографическими ключами.

Основные термины криптографии

- **Шифром** называют систему или алгоритм, трансформирующий произвольное сообщение в такую форму, которую не сможет прочитать никто кроме тех, кому это сообщение предназначено.
- При шифровании и расшифровке используется **ключ** (key), который и есть тот «маленький секрет».
- **Пространством** ключей называют множество всех возможных ключей, доступных для использования в алгоритме.
- Исходное, незашифрованное сообщение называют **открытым** текстом (plaintext)
- **Зашифрованным** текстом (ciphertext). соответственно, называют сообщение, полученное в результате шифрования.

Основные термины криптографии

Разработку и применение шифров называют **криптографией**, в то время как науку о раскрытии шифров - **криптоанализом**. Поскольку проверка шифров на стойкость является обязательным элементом их разработки, криптоанализ также является частью процесса разработки.

Криптология - это наука, предметом которой являются математические основания как криптографии, так и криптоанализа одновременно.

Криптоаналитической атакой называют использование специальных методов для раскрытия ключа шифра и/или получения открытого текста. Предполагается, что атакующей стороне уже известен алгоритм шифрования, и ей требуется только найти конкретный ключ.

Основные термины криптографии

Другая важная концепция связана со словом **«взлом».** Когда говорят, что некоторый алгоритм был «взломан» , это не обязательно означает, что найден практический способ раскрытия шифрованных сообщений. Может иметься в виду в виду, что найден способ существенно уменьшить ту вычислительную работу, которая требуется для раскрытия шифрованного сообщения методом «грубой силы», то есть простым перебором всех возможных ключей.

При осуществлении такого взлома. практически шифр все же может оставаться стойким, поскольку требуемые вычислительные возможности будут все еще оставаться за гранью реального. Однако, хотя существование метода взлома не означает еще реальной уязвимости алгоритма, обычно такой алгоритм более не используют.

Основные термины криптографии

- **ГАММИРОВАНИЕ – процесс наложения по определенному закону гаммы шифра на открытые данные.**
- **ГАММА ШИФРА – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для шифрования открытых данных и расшифрования зашифрованных данных.**
- **ШИФРОВАНИЕ ДАННЫХ – процесс зашифрования и расшифрования данных.**
- **ЗАШИФРОВАНИЕ ДАННЫХ – процесс преобразования открытых данных в зашифрованные с помощью шифра.**
- **РАСШИФРОВАНИЕ ДАННЫХ – процесс преобразования закрытых данных в открытые с помощью шифра.**

Основные термины криптографии

- **ДЕШИФРОВАНИЕ – процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме.**
- **ИМИТОЗАЩИТА – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка, которая представляет собой последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.**
- **КЛЮЧ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма.**
- **СИНХРОПОСЫЛКА – исходные открытые параметры алгоритма криптографического преобразования.**
- **КРИПТОСТОЙКОСТЬ – характеристика шифра, определяющая его стойкость к дешифрованию. Обычно она определяется периодом времени, необходимым для дешифрования.**

2. ШИФР ЦЕЗАРЯ

- **Шифр Цезаря**, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.
- Шифр Цезаря — это вид шифра подстановкиШифр Цезаря — это вид шифра подстановки, в котором каждый символШифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.
- Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.
- Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр ВиженераШаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13Шаг шифрования,

ШИФР ЦЕЗАРЯ

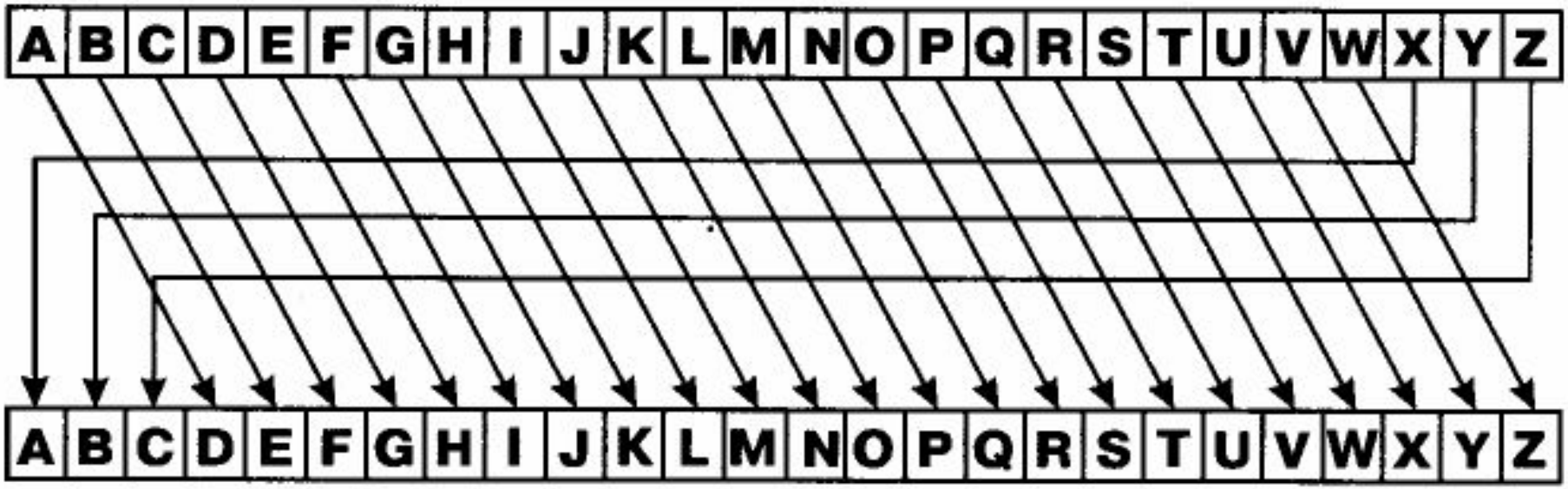


Рис. Шифр Цезаря

Ключ: 3

Открытый текст:

P = HELLO CAESAR CIPHER

Зашифрованный текст:

C = KHOOR FDHVDU FLSKHU

ШИФР ЦЕЗАРЯ

Определение: сдвиговый шифр (обобщенный шифр Цезаря)
При произвольном ключе k, где

$k \in Z_{26}$ **(так обозначается множество целых чисел,** $0 \le k \le 25$**)**
и произвольном открытом тексте p в виде кортежа, где

$p = (p_1, p_2, p_3, \ldots, p_m)$ **и** $p_i \in Z_{26}$ **для** $0 \le i \le m$,
результирующий шифрованный текст c будет представлен кортежем

$c = (c_1, c_2, c_3, \ldots, c_m)$ **и** $c_i \in Z_{26}$ **для** $0 \le i \le m$,

При этом функция шифрования $E_k(p)$ для сдвигового шифра определяется следующим образом

$$c_i = E_k(p_i) = p_i + k (mod\ 26) \text{ для } 0 \le i \le m.$$

А функция дешифрования $D_k(c)$ определяется, как

$$p_i = D_k(c_i) = c_i - k (mod\ 26) \text{ для } 0 \le i \le m.$$

Шифр является обратимым, так как

$D_k(E_k(x)) = x$ **для** $c_i - k (mod\ 26)$ **для всех** $x \in Z_{26}$

ШИФР ЦЕЗАРЯ

АТАКА «ГРУБОЙ СИЛЫ» НА ШИФР ЦЕЗАРЯ

Атакой методом **«грубой силы»** называют способ раскрытия шифра, при котором поиск ведется во всем возможном пространстве значений ключа до тех пор, пока не будет получен осмысленный результат.

Для того чтобы проделать это с шифром Цезаря, вам необходимо задаться значением ключа 1 и продолжать перебирать все числа до 25, пока не будет получен осмысленный текст.

Конечно варианты k=0 и k= 26 будут бессмысленными, поскольку в этих случаях зашифрованный и открытый тексты будут идентичными. Пример программы CaesarCipherBruteForceAttack представляет собой реализацию этой атаки.

ПРОСТОЙ ПОДСТАНОВОЧНЫЙ ШИФР

Простой подстановочный шифр в свое время не помог королеве Марии.

В подстановочном шифре каждый символ заменяется заранее определенным символом подстановочного алфавита, что относит его, как и шифр Цезаря, к моноалфавитным подстановочным шифрам.

Это означает, что существует однозначное соответствие между символами в открытом тексте и символами в тексте зашифрованном. Такое свойство шифра делает его уязвимым для атаки, основанной на частотном анализе.

ПРОСТОЙ ПОДСТАНОВОЧНЫЙ ШИФР

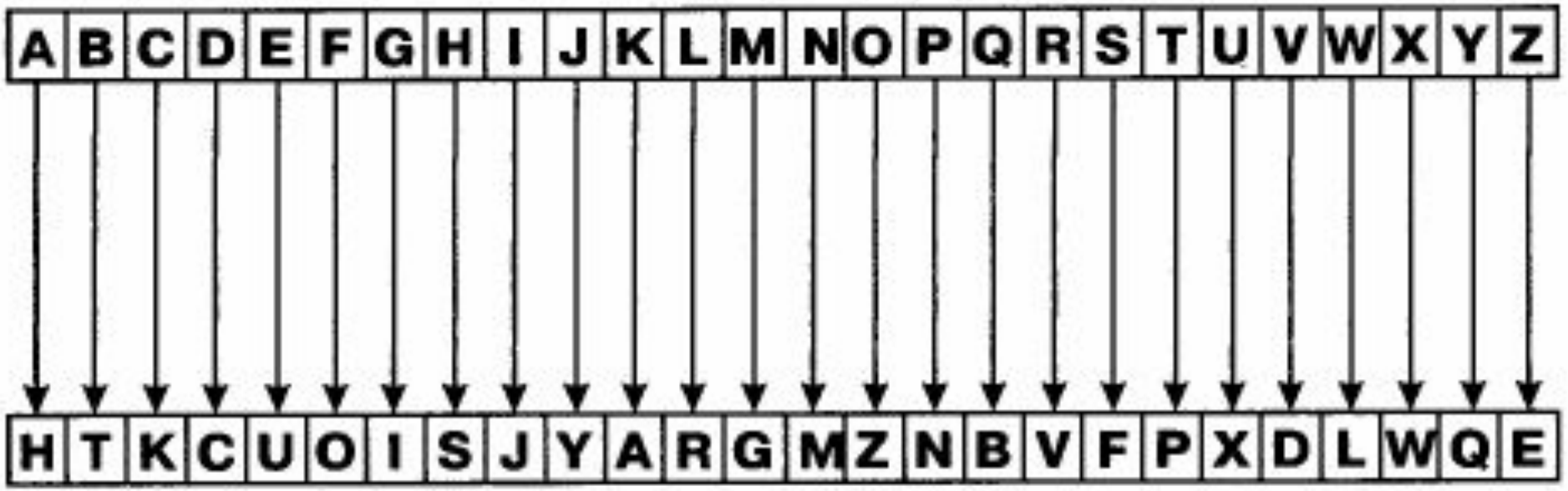


Рис. Простой подстановочный шифр

- **Ключ:**
- **HTKCUOISJYARGMZNBVFPXDLWQE**
- **Открытый текст:**
- **P = HELLO SIMPLE SUB CIPHER**
- **Зашифрованный текст:**
- **C = SURRZ FJGNRU FXT KJNSUV**

ЧАСТОТНЫЙ АНАЛИЗ: РАСКРЫТИЕ ПОДСТАНОВОЧНОГО ШИФРА

Для раскрытия простых подстановочных шифров обычно используют атаку на основе частотного анализа, в которой используются статистические методы.

Здесь используется тот факт, что вероятность появления в открытом тексте определенных букв или сочетаний букв зависит от этих самых букв или сочетаний букв.

Например, в английском языке буквы A и E встречаются гораздо чаще других букв. Пары букв TH, HE, SH и CH встречаются гораздо чаще других пар, а буква Q, фактически, может встретиться только в сочетании QU.

Это неравномерное распределение вероятностей связано с тем, что английский язык (как и вообще все естественные языки) весьма избыточен. Эта избыточность играет важную роль: она уменьшает вероятность ошибок при передаче сообщений. Но, с другой стороны избыточность облегчает задачу атакующей стороне.

Пример кода **SimpleSubCipherFrequencyAttack** демонстрирует принцип этой атаки.

3. Шифр ВИЖЕНЕРА

С изобретением телеграфа в середине 1800х годов интерес к криптографии стал расти, поскольку ненадежность моноалфавитных подстановочных шифров была уже хорошо известна.

Решение, найденное в ту эпоху, заключалось в использовании шифра Виженера, который, как это ни странно, к тому моменту был известен уже на протяжении почти 300 лет. Этот шифр был известен во Франции, как «нераскрываемый шифр), и это был действительно выдающийся шифр своего времени.

Фактически, шифр Виженера оставался нераскрытым почти три столетия, с момента его изобретения в 1586 г. и до момента его взлома в 1854, когда Чарльз Бэббидж сумел, наконец, раскрыть его.

Шифр ВИЖЕНЕРА

Шифр Виженера представляет собой полиалфавитный подстановочный шифр. Это означает, что для подстановки используются многие алфавиты, благодаря чему частоты символов в зашифрованном тексте не соответствуют частотам символов в тексте открытом.

Следовательно, в отличие от моноалфавитных подстановочных шифров наподобие шифра Цезаря, шифр Виженера не поддается простому частотному анализу.

В сущности, шифр Виженера меняет соответствие между открытыми и зашифрованными символами для каждого очередного символа. Он Основывается на таблице, вид которой приведен на след. слайде. Каждая строка этой таблицы не что иное, как шифр Цезаря, сдвинутый на число позиций, соответствующее позиции в строке. Строка А сдвинута на 0 позиций, строка В - на 1, и так далее.

Шифр ВИЖЕНЕРА

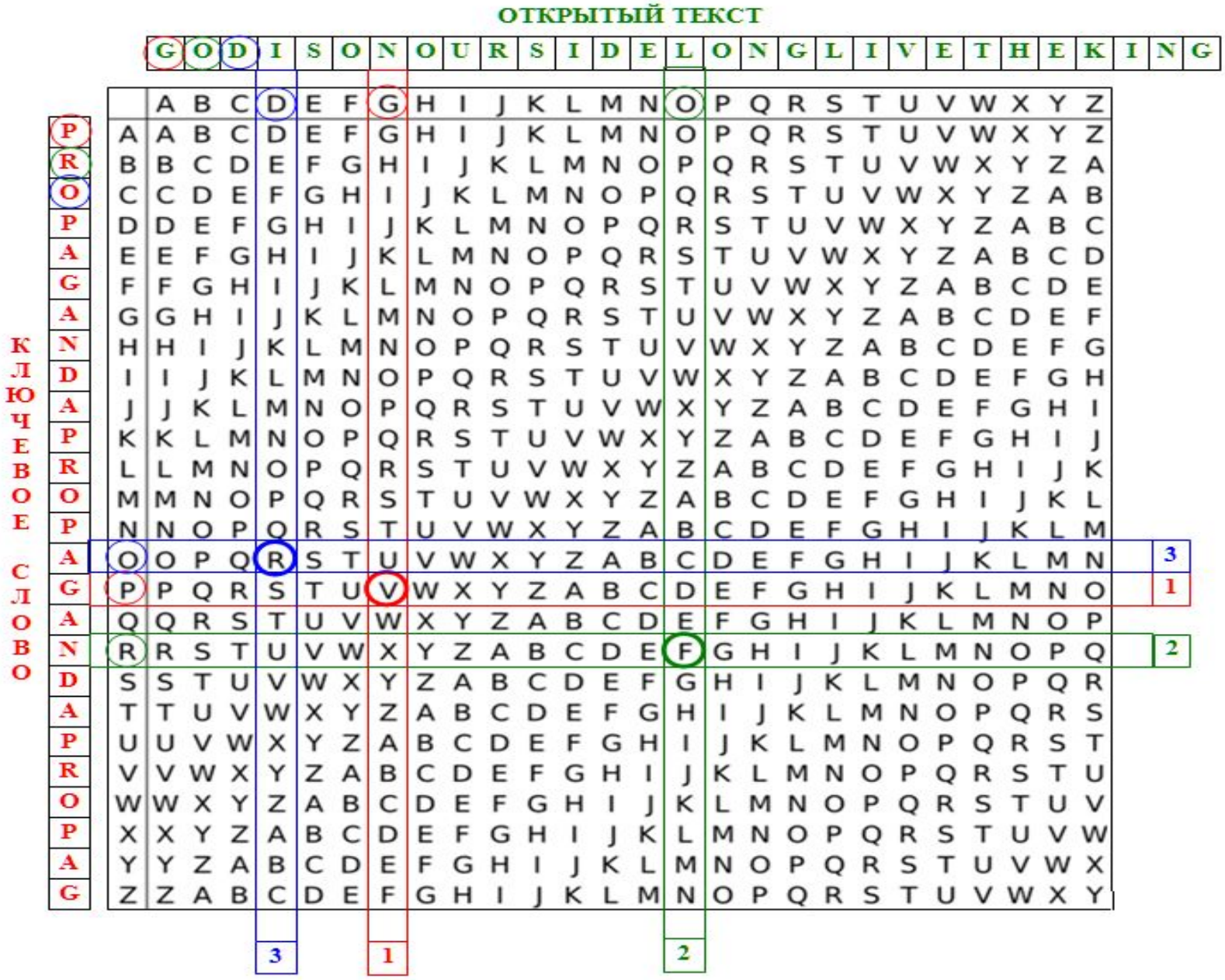
В шифре Виженера такая таблица используется в сочетании с ключевым словом, при помощи которого шифруется текст. Предположим, например, что нам требуется зашифровать фразу GOD IS ON OUR SIDE LONG LIVE THE KING при помощи ключа PROPAGANDA.

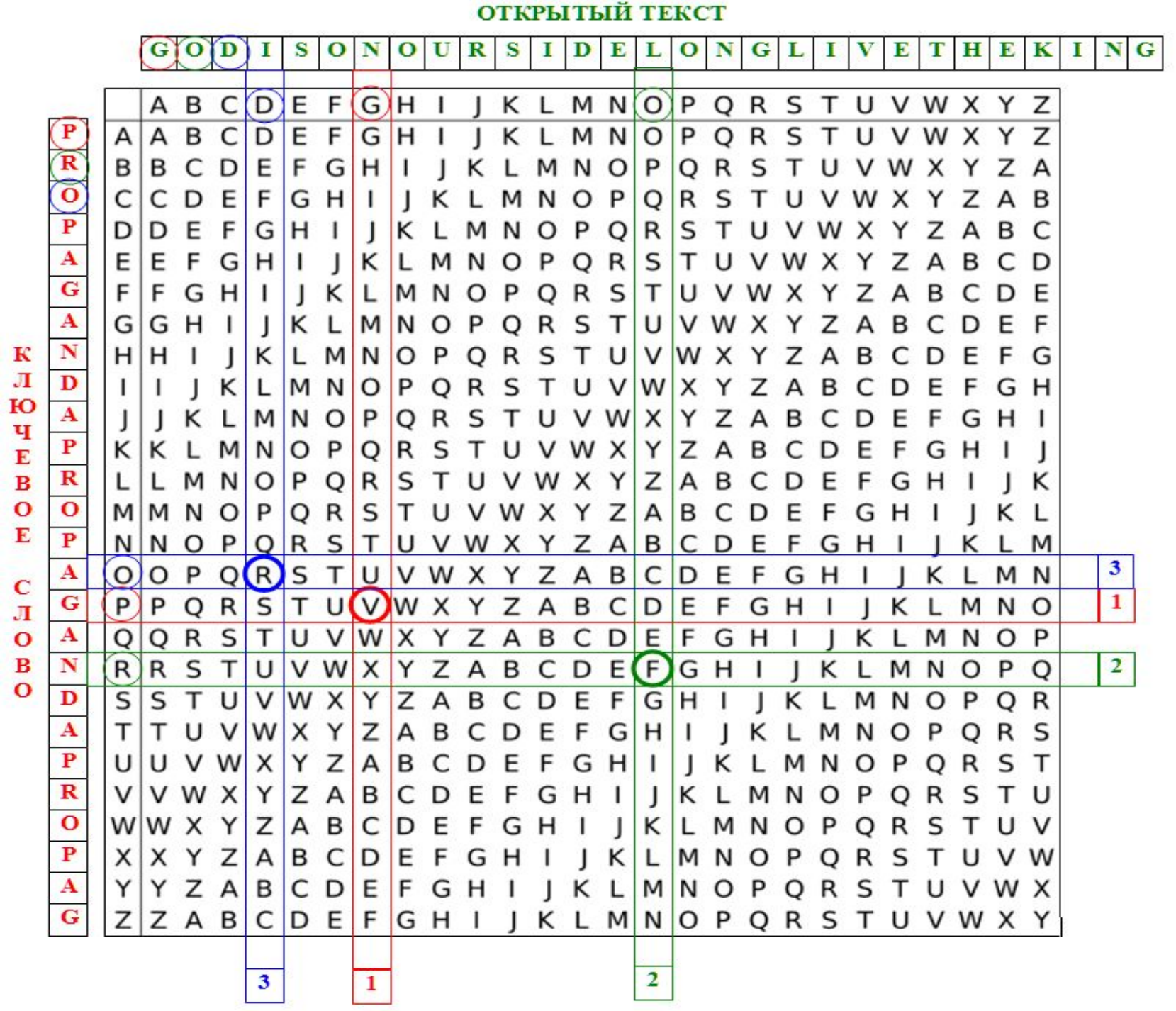
Для шифрования вы повторяете ключ столько раз, сколько необходимо для достижения длины открытоrо текста, просто записывая символы под символами открытого текста. Затем вы получаете поочередно каждый символ зашифрованноrо текста, беря столбец, определенный по символу открытого текста, и пересекая его со строкой, определенной по соответствующему символу ключа.

Шифр ВИЖЕНЕРА

- Пример:
- Открытый текст : GOD IS ON OUR SIDE LONG LIVE THE KING
- Ключ : PRO PA GA NDA PROP AGAN DAPR OPA GAND
- зашифрованный текст: VFR XS UN BXR HZRT LUNT OIKV HWE QIAJ

Пример:									
Открытый текст:	GOD	IS	ON	OUR	SIDE	LONG	LIVE	THE	KING
Ключ:	PRO	PA	GA	NDA	PROP	AGAN	DAPR	OPA	GAND
Зашифрованный текст:	VFR	XS	UN	BXR	HZRT	LUNT	OIKV	HWE	QIAJ




ОТКРЫТЫЙ ТЕКСТ
GODISONOURSIDELONGLIVETHEKING
КЛЮЧЕВОЕ СЛОВО
PROPAGANDA
PROPAGANDA
3
1
2
3
1
2

АТАКА БЭББИДЖА: РАСКРЫТИЕ ШИФРА ВИЖЕНЕРА

Бэббидж обнаружил, что сочетание анализа ключа с частотным анализом текста способно привести к успеху.

Прежде всего производится анализ ключа с целью выяснить длину ключа. В основном это сводится к поиску повторяющихся образцов в тексте. Для этого вы сдвигаете текст относительно самого себя на один символ и подсчитываете число совпавших символов.

Затем должен следовать следующий сдвиг и новый подсчет. Когда эта процедура будет повторена много раз, вы запоминаете величину сдвига, давшую максимальное число совпадений. Случайный сдвиг дает небольшое число совпадений, но сдвиг на величину, кратную длине ключа приведет число совпадений к максимуму.

АТАКА БЭББИДЖА: РАСКРЫТИЕ ШИФРА ВИЖЕНЕРА

Этот факт вытекает из того обстоятельства, что некоторые символы встречаются чаще других, и, кроме того, ключ повторен в тексте много раз с определенным интервалом.

Поскольку символ совпадает с копией самого себя, зашифрованной тем же самым символом ключа, число совпадений будет немного увеличиваться при всех сдвигах, величина которых кратна длине ключа.

Очевидно, что для выполнения этой процедуры требуется текст достаточно большого размера, поскольку расстояние единственности для этого шифра гораздо больше, чем для моноалфавитных подстановочных шифров.

АТАКА БЭББИДЖА: РАСКРЫТИЕ ШИФРА ВИЖЕНЕРА

После того как длина ключа будет, предположительно, определена, следующий шаг будет состоять в частотном анализе. При этом вы разделяете символы шифрованного текста по группам, соответствующим символам ключа, которые использовались для шифрования в каждой из групп, основываясь при этом на предположении о длине ключа.

С каждой группой символов вы можете теперь обращаться, как с текстом, зашифрованным простым сдвиговым шифром наподобие шифра Цезаря, используя атаку методом «грубой силы» или частотный анализ. После того как все группы по отдельности будут расшифрованы, их можно собрать вместе и получить расшифрованный текст.

ЕДИНСТВЕННЫЙ НЕУЯЗВИМЫЙ ШИФР: ОДНОРАЗОВЫЙ ШИФРОВАЛЬНЫЙ БЛОКНОТ

Существует только один шифр, который теоретически безопасен на 100%. Это так называемый «шифровальный блокнот» или «одноразовый блокнот» (OneTime Pad - OTP). Для достижения идеальной безопасности в методе «одноразового блокнота» применяются весьма строгие правила: ключи генерируются на основе **настоящих** случайных чисел, ключи сохраняются в строгом **секрете** и ключи **никогда** не используются повторно.

В отличие от других шифров, метод «одноразового блокнота» (OTP) так же, как и его математические эквиваленты, является единственной системой, неуязвимой для взлома. Метод OTP позволяет достичь идеальной безопасности, однако практическое его использование затруднено проблемой ключей.

ЕДИНСТВЕННЫЙ НЕУЯЗВИМЫЙ ШИФР: ОДНОРАЗОВЫЙ ШИФРОВАЛЬНЫЙ БЛОКНОТ

По этой причине метод «одноразового блокнота» применяют лишь в редких случаях, когда достижение абсолютной секретности важнее всего прочего, и когда требуемая пропускная способность невелика. Такие ситуации достаточно редки, их можно встретить, разве что, в военной области, в дипломатии и в шпионаже.

Сила метода OTP проистекает из того факта, что при любом заданном шифрованном тексте любые варианты исходного открытого текста равновероятны. Иными словами, для любого возможного варианта открытого текста найдется ключ, который в результате применения произведет этот шифрованный текст.

ЕДИНСТВЕННЫЙ НЕУЯЗВИМЫЙ ШИФР: ОДНОРАЗОВЫЙ ШИФРОВАЛЬНЫЙ БЛОКНОТ

Это означает, что если вы попытаетесь найти ключ методом «грубой силы», то есть просто перебирая все возможные ключи, то получите в результате все возможные варианты открытого текста. Здесь будет также и истинный открытый текст, но вместе с ним все возможные варианты осмысленного текста, а это ничего вам не даст.

Атака методом «грубой силы» на шифр OTP бесполезна и неуместна, вот, что вам следует помнить о методе «одноразового блокнота»! Надежда раскрыть шифр OTP возникает лишь в ситуации, когда ключ был использован несколько раз, для шифрования нескольких сообщений, или когда для генерации псевдослучайного ключа был использован алгоритм, дающий предсказуемую последовательность, или же когда вам удастся добыть ключ какими то иными, не криптоаналитическими методами.

Стеганография

Стеганографией называют искусство сокрытия информации таким образом, что сам факт сокрытия остается скрытым. В техническом смысле стеганографию не рассматривают в качестве разновидности криптографии, но все же она может эффективно использоваться для обеспечения секретности коммуникаций.

Пример Steganography представляет собой простую программу, иллюстрирующую типичный прием стеганографии, в котором используется графическое изображение.

Каждый 8-битовый байт исходного изображения представляет один пиксель. Для каждого пикселя определены три байта, представляющие красную, зеленую и синюю компоненты цвета пикселя.

Каждый байт секретного сообщения разделяется на три поля размером 3, 3 и 2 бита. Этими 3х и 2х битовыми полями затем замещаются младшие, наименее значимые разряды трех «цветовых» байтов соответствующего пикселя.

4. Симметричные криптосистемы

- **ПРЕОБРАЗОВАНИЕ ШИФРОВАНИЯ может быть СИММЕТРИЧНЫМ и АСИММЕТРИЧНЫМ относительно преобразования расшифрования.**

- **Соответственно различают два класса криптосистем:**
- **1. СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ (с единым ключом);**
- **2. АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ (с двумя ключами).**

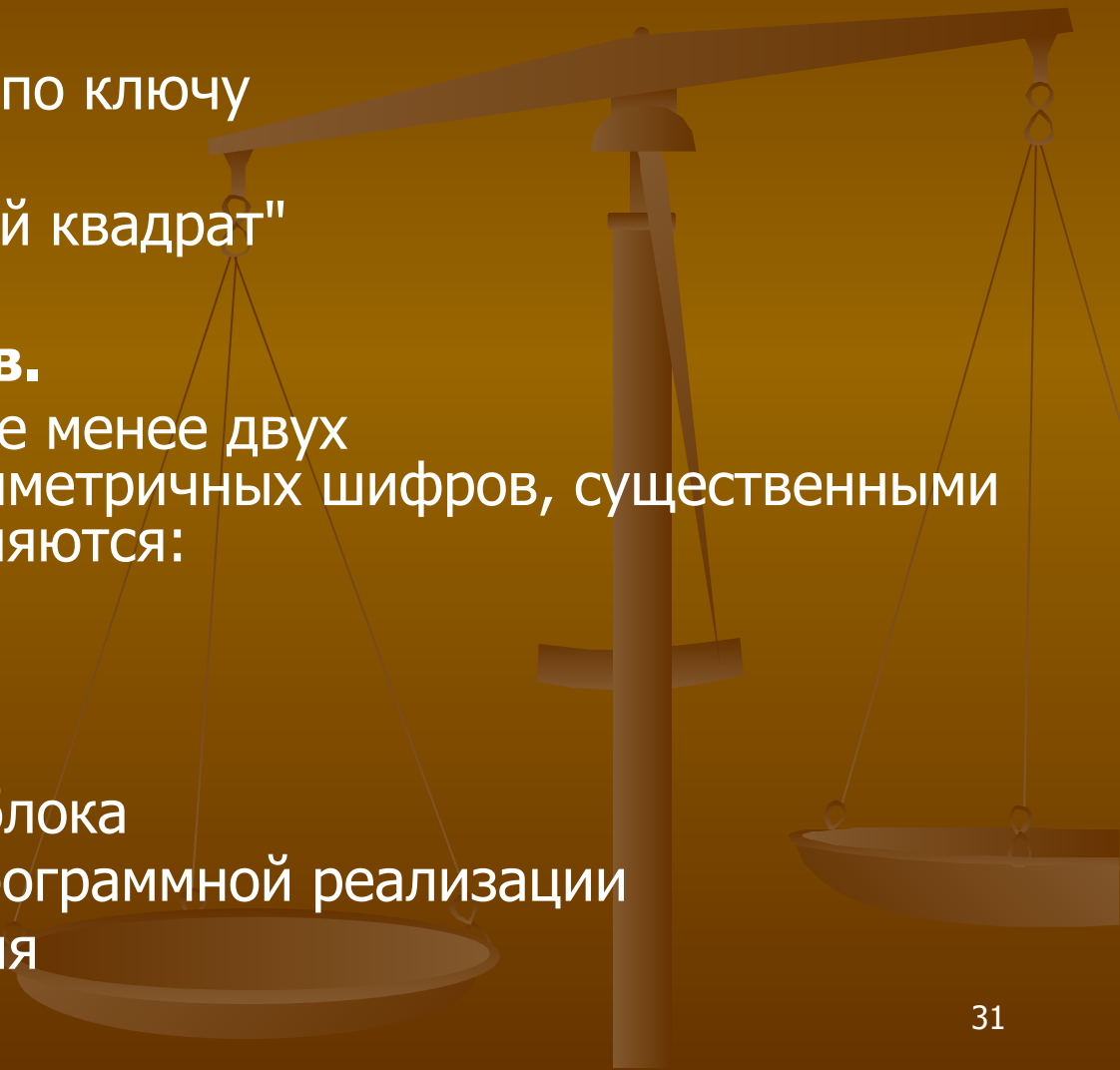
Симметричные криптосистемы

- **Симметри́чные криптосисте́мы** (также **симметричное шифрование**, **симметричные шифры**) (англ. *symmetric-key algorithm*) — способ шифрования, в котором для шифрования) — способ шифрования, в котором для шифрования и расшифровывания) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.
- Алгоритмы шифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом в них является условие,

Симметричные криптосистемы

- Классическими примерами таких алгоритмов являются **симметричные криптографические алгоритмы**, перечисленные ниже:
- Простая перестановка
- Одиночная перестановка по ключу
- Двойная перестановка
- Перестановка "Магический квадрат"

- **Параметры алгоритмов.**
  Существует множество (не менее двух десятков) алгоритмов симметричных шифров, существенными параметрами которых являются:
- стойкость
- длина ключа
- число раундов
- длина обрабатываемого блока
- сложность аппаратной/программной реализации
- сложность преобразования



Симметричные криптосистемы

- Виды симметричных шифров
- **блочные шифры**
- AESAES (англ. *Advanced Encryption Standard*) - американский стандарт шифрования
- ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ
- DESDES (англ. *Data Encryption Standard*) - стандарт шифрования данных в США
- 3DES (Triple-DES, тройной DES)
- RC2RC2 (Шифр Ривеста (Rivest Cipher или Ron’s Cipher))
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (International Data Encryption Algorithm, международный алгоритм шифрования данных)
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)
- CRAB
- 3-WAY
- KhufuKhufu и Khafre
- Kuznechik

Симметричные криптосистемы

- **потоковые шифры**
- RC4 (алгоритм шифрования с ключом переменной длины)
- SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)
- WAKE (World Auto Key Encryption algorithm, всемирный алгоритм шифрования на автоматическом ключе)
- Сравнение с асимметричными криптосистемами
- **Достоинства**
- скорость
- простота реализации (за счёт более простых операций)
- меньшая требуемая длина ключа для сопоставимой стойкости
- изученность (за счёт большего возраста)
- **Недостатки**
- сложность управления ключами в большой сети
- сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам
- Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.
- Важным недостатком симметричных шифров является **невозможность** их использования в механизмах формирования электронной цифровой подписи и сертификатов, так как ключ известен каждой стороне.

Простая перестановка

- Простая перестановка **без ключа** — один из самых простых методов шифрования.
- Делают так:
- **Сообщение записывается в таблицу по столбцам.**
- После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю **нужно договориться об общем ключе в виде размера таблицы**.
- например, **зашифруем фразу "ВРАГ БУДЕТ РАЗБИТ",** разместим текст в "таблице" - по три столбца (и не будем вообще использовать пробелы) - запишем текст столбцами:

1	В	Г	Д	Р	Б
2					
3	Р	Б	Е	А	И
4					
5	А	У	Т	З	Т

при считывании по строкам получим шифровку (разделяем на группы по 4-ре только для визуального удобства - можно вообще не разделять):

- ВГДР БРБЕ АИАУ ТЗТ

- То есть мы получаем перестановкуТо есть мы получаем перестановку (как результат действия подстановки) исходного множества букв (потому так и называется) таким образом:

- ВРАГ БУДЕ ТРАЗ БИТ
- ВГДР БРБЕ АИАУ ТЗТ

- Фактически - чтобы сразу расшифровать такую строку:

- ВРАГ БУДЕ ТРАЗ БИТ

- Достаточно знать **число столбцов в исходной таблице**, то есть **число столбцов и будет являться *ключом*** данной криптосистемы.
- Но, как вы поняли на компьютере такая защита весьма просто ломается путём подбора числа столбцов (проверка - получение связного текста)

Одиночная перестановка по ключу

- Чуть более надёжна чем перестановка без ключа
  Шифровать будем ту же фразу, которую шифровали без ключа
- Ключом у нас будет **слово памир**
- Таблица выглядит исходно выглядит так;

1	П	А	М	И	Р
2	4	1	3	2	5
3	В	Г	Д	Р	Б
4					
5	Р	Б	Е	А	И
6					
7	А	У	Т	З	Т

- Рассмотрим первые две строки:

1	П	А	М	И	Р
2	4	1	3	2	5

- Здесь записано слово - а ниже номера его букв, для случая их сортировки в алфавитном порядке (так называемый "естественный порядок").
- Теперь нам надо просто переставить столбцы в "естественном порядке" то есть так. чтобы цифры во второй строке выстроились по порядку, получим:

1	1	2	3	4	5
2	Г	Р	Д	В	Б
3	Б	А	Е	Р	И
4	У	З	Т	Т	А

- Вот и всё теперь смело записываем шифровку по строкам (для удобства записи группами по 4-ре):
- 1 ГРДВ ББФЕ РИУЗ ТТА
- Чтобы расшифровать - надо просто знать ключевое слово (оно определит число столбцов - по числу его букв + то в каком порядке надо эти столбцы переставить!)

Двойная перестановка

- Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Перестановка «Магический квадрат»

- Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 х 3, если не принимать во внимание его повороты. Магических квадратов 4 х 4 насчитывается уже 880, а число магических квадратов размером 5 х 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

Перестановка «Магический квадрат»

- В квадрат размером 4 на 4 вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

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

- Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «ПриезжаюСегодня.». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка.

Перестановка «Магический квадрат»

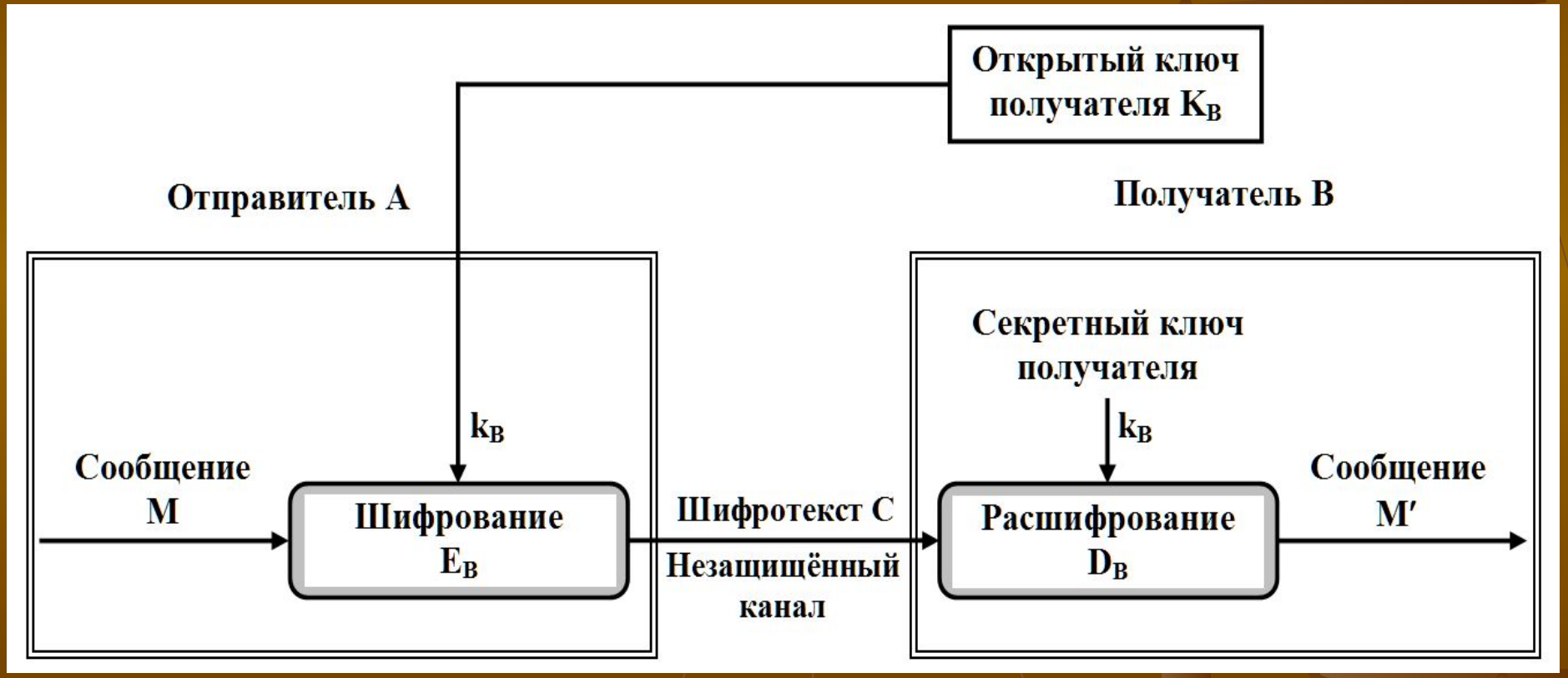
16.	3 и	2 р	13 д
5 з	10 е	11 г	8 ю
9 С	6 ж	7 а	12 о
4 е	15 я	14 н	1 П

- После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно): .ирдзегюСжаоеянП
- При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата». Программа должна генерировать «магические квадраты» и по ключу выбирать необходимый. Размер квадрата больше чем 3х3.

5. Асимметричные криптосистемы шифрования

- Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:
  • *открытый ключ К* используется для шифрования информации, вычисляется из секретного ключа *к*;
  • *секретный ключ к* используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа *К*.
- Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ *к* из открытого ключа *К*. Поэтому открытый ключ *К* может свободно передаваться по каналам связи.
- Асимметричные системы называют также *двухключевыми криптографическими системами*, или *криптосистемами с открытым ключом*.
- Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис.

ОБОБЩЕННАЯ СХЕМА АСИММЕТРИЧНОЙ КРИПТОСИСТЕМЫ ШИФРОВАНИЯ



- **Использование ОДНОГО КЛЮЧА для всех абонентов. Однако это недопустимо по соображениям безопасности, т.к. в случае компрометации ключа под угрозой будет находиться документооборот всех абонентов.**

- **Использование МАТРИЦЫ КЛЮЧЕЙ, содержащей ключи парной связи абонентов.**

Использование МАТРИЦЫ КЛЮЧЕЙ, содержащей ключи парной связи абонентов.

$К_{11}$	$К_{12}$	…	$К_{1n}$
$К_{21}$	$К_{22}$	…	$К_{2n}$
…	…	…	…
$К_{n1}$	$К_{n2}$	…	$К_{nn}$

Набор ключей для абонента 1

Набор ключей для абонента 2

Набор ключей для абонента n

Каждая i-я строка матрицы представляет собой набор ключей конкретного абонента I для связи со всеми остальными N-1 абонентами.

Сетевые наборы должны распространяться *по защищенным каналам* (для этого существуют определенные методы и алгоритмы, обеспечивающие защищенное распределение ключей) или *из рук в руки*.

Симметричный шифр

- **Симметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи совпадают.**
- *Стороны, обменивающиеся зашифрованными данными, должны знать* ***общий секретный ключ***

- **Достоинства:**
- Всего один зашифровывающий / расшифровывающий ключ

- **Недостатки:**
- Процесс обмена информацией о секретном ключе представляет собой брешь в безопасности.
- Для передачи секретного ключа необходим закрытый канал связи.

Ассиметричный шифр

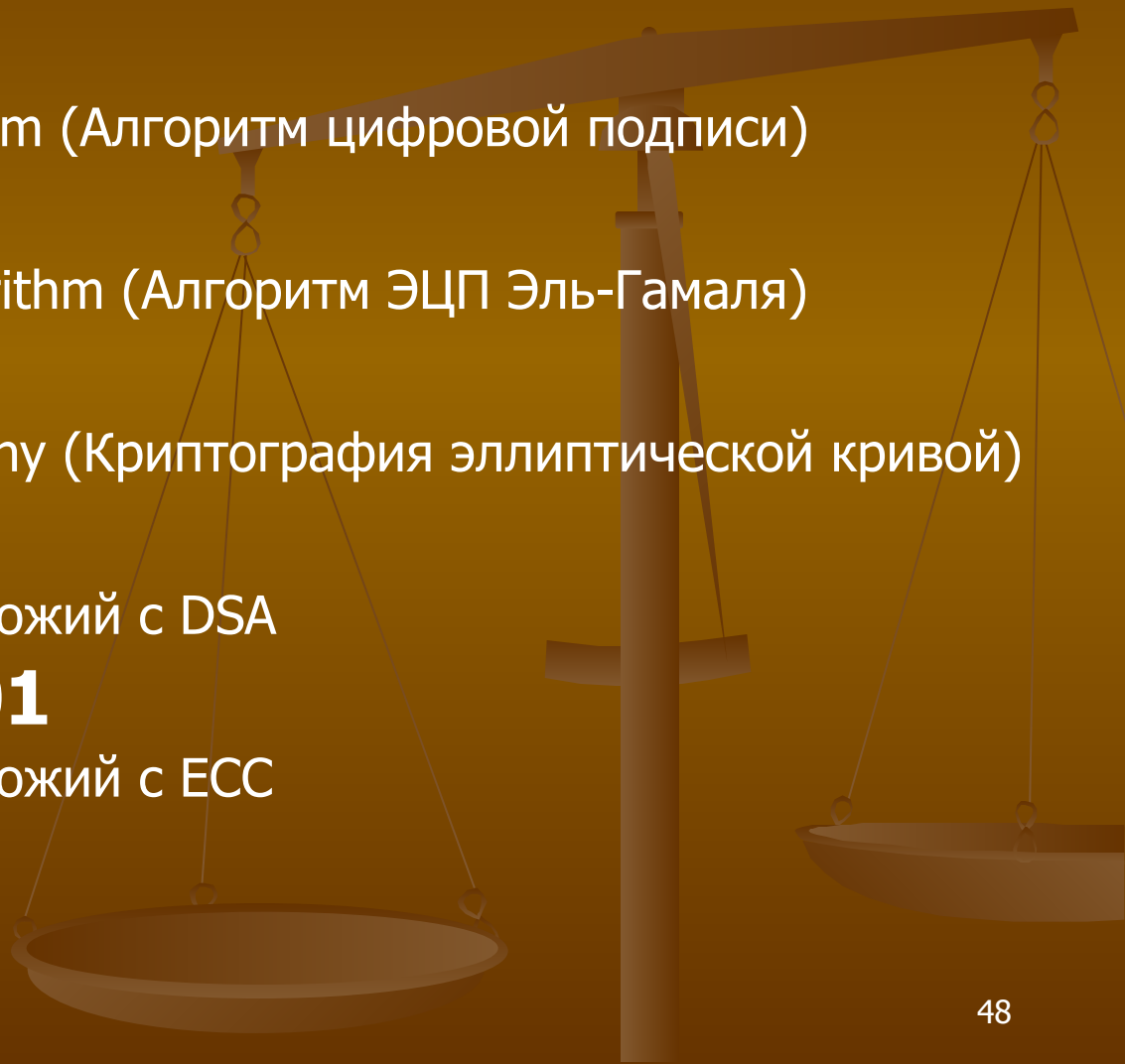
- **Ассимметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи не совпадают.**
- ***Ассиметричное шифрование является односторонним процессом.***
- *Данные шифруются только открытым ключом*
- *Расшифровываются только секретным*
- *Открытый и секретный ключ связаны между собой.*

- **Достоинства:**
- Для передачи ключа не нужен закрытый канал связи.
- Открытый ключ может быть свободно распространен, это позволяет принимать данные от всех пользователей.

- **Недостатки:**
- Ресурсоемкий алгоритм шифрования / дешифрирования

Виды ассиметричных шифров

- **RSA**
  - Rivest-Shamir-Adleman (Ривест-Шамир-Адлеман)
- **DSA**
  - Digital Signature Algorithm (Алгоритм цифровой подписи)
- **EGSA**
  - El-Gamal Signature Algorithm (Алгоритм ЭЦП Эль-Гамаля)
- **ECC**
  - Elliptic Curve Cryptography (Криптография эллиптической кривой)
- **ГОСТ Р 34.10-94**
  - Российский стандарт схожий с DSA
- **ГОСТ Р 34.10-2001**
  - Российский стандарт схожий с ECC



Алгоритм RSA

- RSA (1977 г.) – криптографическая система открытого ключа. Обеспечивает такие механизмы защиты как шифрование и цифровая подпись.
  - Цифровая подпись (ЭЦП) – механизм аутентификации, позволяющий проверить принадлежность подписи электронного документа его владельцу.
- Алгоритм RSA используется в Internet, к примеру в:
  - S/MIME
  - IPSEC (Internet Protocol Security)
  - TLS (которым предполагается заменить SSL)
  - WAP WTLS.

Алгоритм RSA: Теория

- В основу асимметричных криптосистем кладётся одна из сложных математических проблем, которая позволяет строить односторонние функции и функции-лазейки.
- В основе алгоритма RSA лежит вычислительная проблема разложения больших чисел на простые множители.
- Односторонняя функция – функция, которая вычисляется только прямо, т.е. не обращается.
  - Возможно найти $f(x)$, зная x, но невозможно обратное.
- **Односторонней функцией в RSA служит функция для шифрования.**
- Лазейка – некий секрет, зная который можно обратить одностороннюю функцию.
- **Лазейкой в RSA является секретный ключ.**

Алгоритм RSA: Реализация

1. Выбираются два случайных простых числа $\boldsymbol{p}$ и $\boldsymbol{q}$ заданного размера
   - $p = 3$
   - $q = 11$
2. Вычисляется модуль, $\boldsymbol{n}$
   - $n = p \cdot q = 33$
3. Вычисляется значение функции Эйлера $\varphi(n)$
   - $\varphi(n) = (p-1) \cdot (q-1) = 20$

Алгоритм RSA: Реализация

4. Выбирается целое число $1 < e < \varphi(n)$ $[1 < e < 20]$ взаимно простое со значением функции $\varphi(n) = 20$
   - $e = 3$
   - ***e*** – открытая экспонента
5. Вычисляется число ***d***, мультипликативно обратное к числу ***e***, т.е. $d \cdot e \left(\mathrm{mod}\, \varphi(n)\right) = 1$
   - $d = 7$
   - ***d*** – секретная экспонента
6. Открытый ключ $P = \{e, n\}$
7. Секретный ключ $S = \{d, n\}$

Алгоритм RSA: Реализация

- **Шифрование**
- Формула для шифрования $b_i = a_i^e \pmod n$
- Возьмем к примеру сообщение $a = \{C, R, Y, P, T, O\}$
- Запишем его кодом в соответствии с алфавитом
  - $a = \{3, 18, 25, 16, 20, 15\}$
- Результат: $b = \{27, 24, 16, 4, 14, 9\}$
- Пример: $16 = 25^3 + 473 \cdot 33$

$$27 = 3^3 \pmod{33} \qquad 4 = 16^3 \pmod{33}$$

$$24 = 18^3 \pmod{33} \qquad 14 = 20^3 \pmod{33}$$

$$16 = 25^3 \pmod{33} \qquad 9 = 15^3 \pmod{33}$$

Алгоритм RSA: Реализация

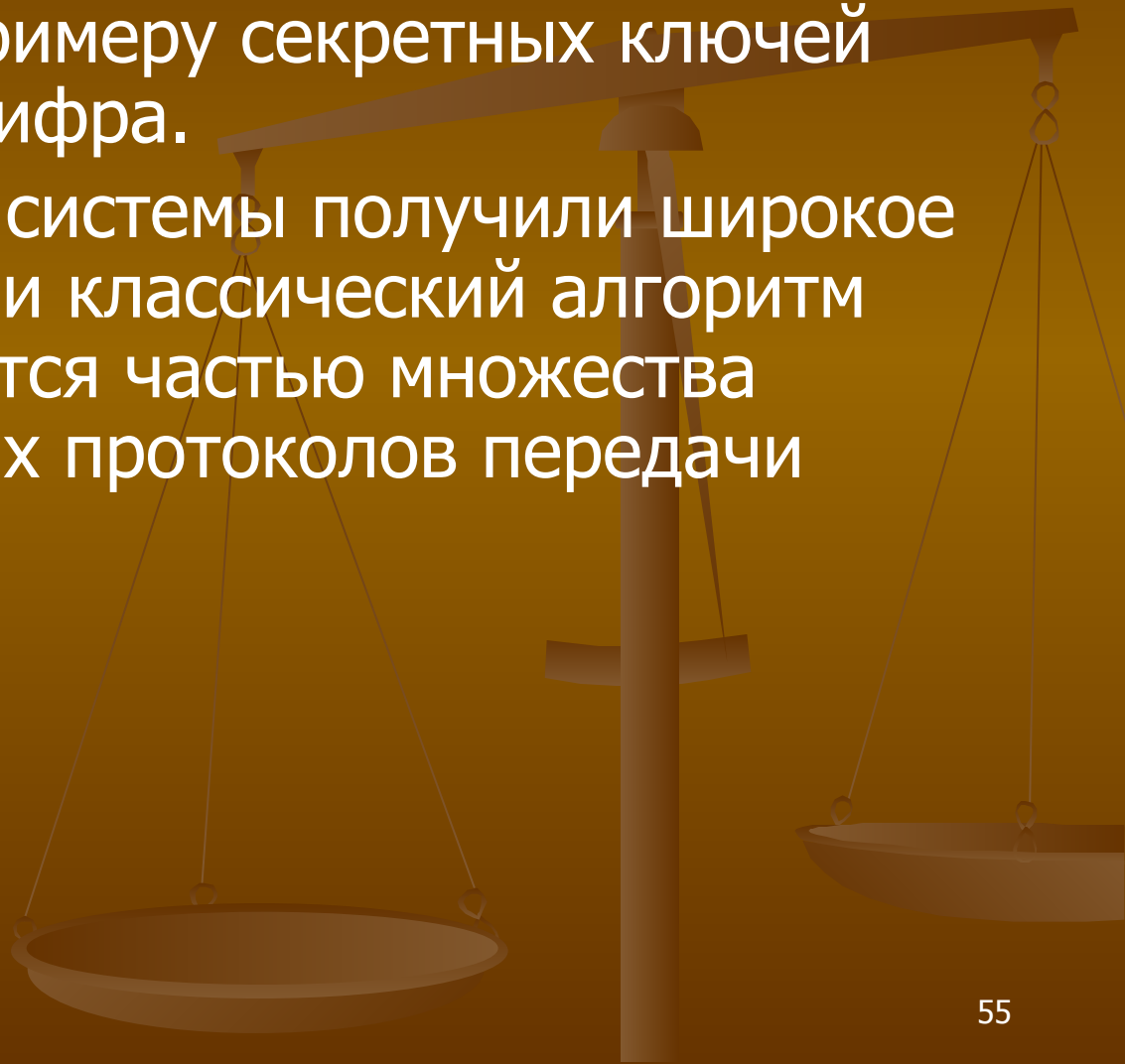
- **Дешифрирование**
- Формула для дешифрирования $a_i = b_i^d \pmod n$
- Шифрованное сообщение $b = \{27, 24, 16, 4, 14, 9\}$
- Результат: $a = \{3, 18, 25, 16, 20, 15\}$
- В соответствии с алфавитом: $a = \{C, R, Y, P, T, O\}$
- Пример: $25 = 16^7 + 8134407 \cdot 33$

$$3 = 27^7 \pmod{33} \qquad 16 = 4^7 \pmod{33}$$

$$18 = 24^7 \pmod{33} \qquad 20 = 14^7 \pmod{33}$$

$$25 = 16^7 \pmod{33} \qquad 15 = 9^7 \pmod{33}$$

- Алгоритмы ассиметричного шифрования используют как вспомогательный инструмент для передачи небольших объемов информации, к примеру секретных ключей симметричного шифра.
- Такие гибридные системы получили широкое распространение и классический алгоритм RSA сейчас является частью множества других безопасных протоколов передачи данных.



6. КРИПТОГРАФИЧЕСКИЕ ХЕШИРУЮЩИЕ АЛГОРИТМЫ

Криптографические хеширующие алгоритмы получают на входе произвольный объем данных и на выходе уменьшают его до заданного размера (обычно это 128, 160 или 256 бит). Результат работы такого алгоритма называют «дайджестом сообщения» или «отпечатком пальца», и он, результат, в высокой степени идентифицирует исходное сообщение, подобно тому, как отпечаток пальца идентифицирует человека.

В идеале криптографический хеширующий алгоритм должен удовлетворять следующим требованиям:

- трудно восстановить входные данные по выходным (то есть алгоритм должен быть односторонним);
- трудно подобрать такие входные данные, которые дали бы на выходе заранее заданный результат;
- трудно найти два варианта входных данных, которые дали бы одинаковые выходные результаты;
- изменение одного бита во входных данных приводит к изменению, примерно, половины битов в результате.

КРИПТОГРАФИЧЕСКИЕ ХЕШИРУЮЩИЕ АЛГОРИТМЫ

Хеш -алгоритм генерирует «отпечаток пальца» фиксированного размера для произвольного объема входных данных.

Результат работы хеш-алгоритма используется в следующих целях:

- с его помощью можно обнаружить изменения, внесенные во входные данные;
- он используется в алгоритмах, реализующих цифровую подпись;
- его можно использовать для трансформации пароля в такое секретное представление, которое можно безопасно передавать по сети или хранить на незащищенном устройстве;
- его можно использовать для трансформации пароля в ключ для использования в алгоритмах шифрования.

КРИПТОГРАФИЧЕСКИЕ ХЕШИРУЮЩИЕ АЛГОРИТМЫ

В библиотеке .NET Security Framework предусмотрены следующие классы для работы с хеширующими алгоритмами:

- System.Security .Cryptography. KeyedHashAlgorithm;
- System.Security.Cryptography.MD5;
- System.Security.Cryptography.SHA1;
- System.Security.Cryptography.SHA256;
- System.Security.Cryptography.SHA384;
- System.Security.Cryptography.SHA512.

Класс KeyedHashAlgorithm - это абстрактный класс, из которого производятся все классы, реализующие конкретные алгоритмы. Хеш с ключом (keyed hash) отличается от обычного криптографическоro хеша тем, что принимает в качестве дополнительных входных данных ключ.

КРИПТОГРАФИЧЕСКИЕ ХЕШИРУЮЩИЕ АЛГОРИТМЫ

Таким образом, для верификации хеша необходимо знать ключ. Есть два производных класса, получаемых из KeyedHashAlgorithm, это HMACSHAl и MACTripleDES.HMACSHA1, они получают ключ произвольного размера и генерируют 20байтовый «код аутентификации сообщения» MAC (Message Authentication Code), используя при этом алгоритм SHA1.

Буквы HMAC расшифровываются, как KeyedHash Message Authentication Code (код аутентификации сообщения при помощи ключевого хеша).

MACTripleDES генерирует код MAC при помощи «тройного DES», используемого в качестве хеширующего алгоритма. Он принимает ключи размером 8, 16 или 24 байта и генерирует 8-байтовый хеш.

Алгоритмы хеширования с ключом полезны в схемах аутентификации и проверки целостности, фактически они являются альтернативой электронной подписи.

7. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

- Криптографические протоколы - это общепринятое соглашение, касающееся набора алгоритмов, последовательности действий и определения функций каждого из участников процесса.
- Например, простой криптографический протокол RSA + Triple DES, мог бы выглядеть следующим образом.

Криптографические протоколы

1. Алиса и Боб генерируют каждый для себя пару ключей RSA (открытый и секретный ключи).
2. Они обмениваются открытыми ключами RSA, оставляя секретные ключи при себе.
3. Каждый из них генерирует собственный ключ Triple DES и шифрует этот ключ при помощи открытого ключа RSA, принадлежащего своему партнеру. Теперь расшифровать сообщение и получить ключ Triple DES можно только при помощи секретного ключа партнера.
4. Они пересылают друг другу зашифрованные ключи Triple DES.
5. Теперь, если Алисе или Бобу потребуется отправить секретное сообщение, каждый шифрует его при помощи ключа Triple DES своего партнера и отсылает его.
6. Партнер получает шифрованное сообщение и дешифрует его при помощи своего ключа Triple DES.

Криптографические протоколы

Другой пример протокола основывается на асимметричном алгоритме RSA и хеш-алгоритме SHA1 и обеспечивает надежную идентификацию отправителя сообщения.

1. Алиса и Боб генерируют каждый для себя пару ключей RSA (открытый и секретный ключи).
2. Они обмениваются открытыми ключами RSA, оставляя секретные ключи при себе.
3. При необходимости отправить сообщение своему корреспонденту каждый из них вычисляет хеш сообщения при помощи алгоритма SHA1, затем шифрует этот хеш собственным секретным ключом RSA и отправляет сообщение вместе с зашифрованным хешем.
4. Когда Алиса или Боб получают сообщение, и если у них возникает необходимость убедиться в том, что отправителем является именно второй партнер, они расшифровывают присоединенный хеш при помощи открытого ключа RSA своего партнера. Затем они заново вычисляют хеш-сообщения и сравнивают полученный результат с расшифрованным хешем. Если оба хеша совпадают, значит, отправителем является владелец использованного открытого ключа RSA.

Криптографические протоколы

В отличии от этих простых сценариев, криптографические протоколы могут подразумевать участие людей, которые не доверяют друг другу полностью, но тем не менее должны взаимодействовать каким-то образом.

Например, это могут быть финансовые транзакции, банковские и торговые операции - везде используются специальные криптографические протоколы, учитывающие особенности конкретной среды.

Зачастую криптографические протоколы становятся компьютерными стандартами или конвенциями.

Криптографические протоколы

Например, протокол Kerberos повсеместно используется для того, чтобы сервер и клиент могли надежно идентифицировать друг друга.

Другой пример - это модель безопасного доступа к коду (CAS Code Access Security) на платформе .NET, в которой исполняемый код снабжен цифровой подписью автора для верификации перед выполнением.

Еще один пример: SSL - протокол защищенных сокетов (Secure Sockets Layer), используемый для безопасных коммуникаций через Internet.

Есть много других примеров, включая PGP (Pretty Good Privacy - достаточно надежная секретность) для шифрования электронной почты или «соглашение о ключах Диффи-Хеллмана» для обмена сеансовыми ключами по незащищенному каналу и без предварительного обмена какой-либо секретной информацией.

Криптоаналитические атаки

- Атака на основе только зашифрованного текста: в распоряжении атакующей стороны имеется только некоторый, случайно выбранный шифрованный текст.
- Атака с открытым текстом: в распоряжении атакующей стороны имеется случайно выбранный открытый текст и соответствующий ему шифрованный текст.
- Атака с выбранным открытым текстом: в распоряжении атакующей стороны имеется выбранный открытый текст и соответствующий ему шифрованный текст.
- Атака с выбранным зашифрованным текстом: в распоряжении атакующей стороны имеется выбранный шифрованный текст и соответствующий ему открытый текст.
- Адаптивная атака с выбранным открытым текстом: атакующая сторона может многократно получать шифрованный текст, соответствующий заданному открытому тексту, основывая каждый очередной выбор на предыдущих вычислениях.