Криптография и криптоанализ

проф. А.В. Цыганов, СПбГУ, 2009

История симметричного шифрования

Доска Полибия – древнейший из известных методов шифрования:

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

A -> AA, B-> AB, … G-> BB и т.д.

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).

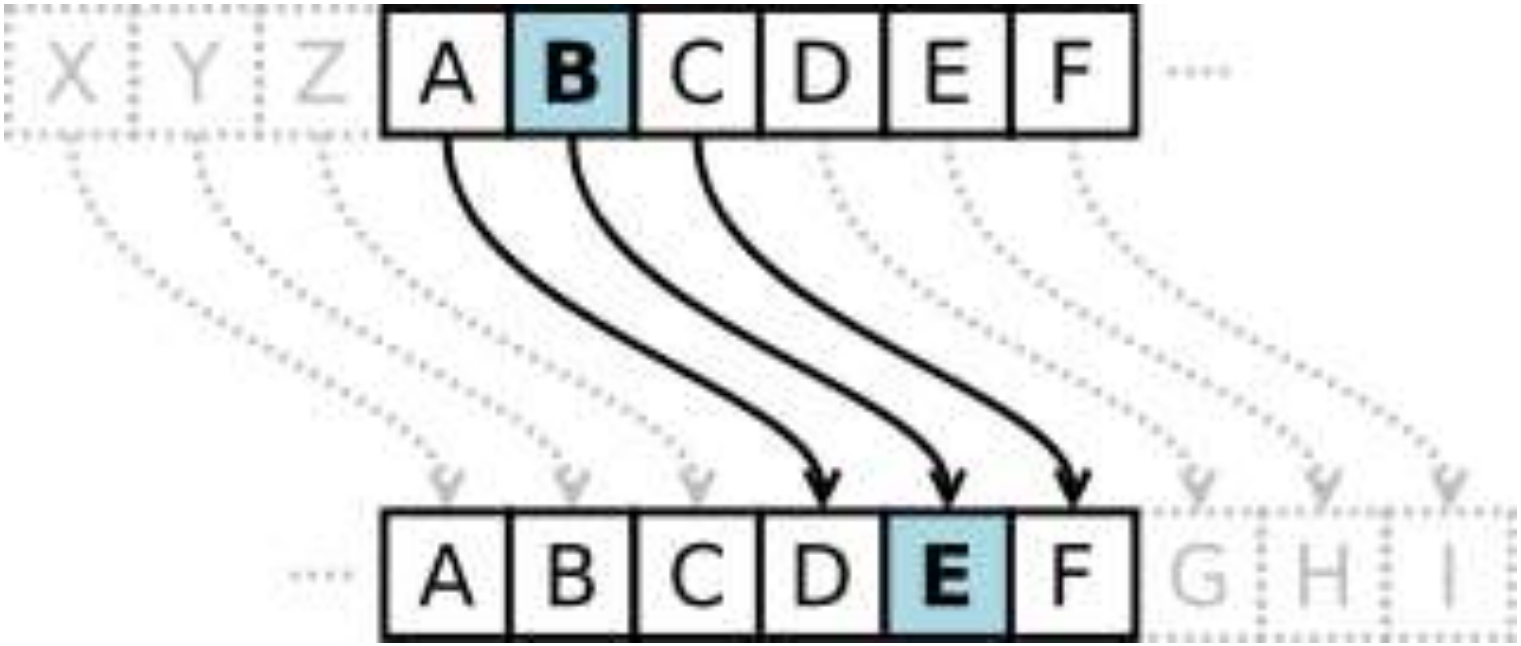
Выберем в качестве ключа слово БАНДЕРОЛЬ

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

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифротекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифротекста берут самую верхнюю букву из того же столбца.

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций.

Шифр Цезаря можно классифицировать как **шифр подстановки**, при более узкой классификации — **шифр простой замены.**



Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

$$y = x + k \ (mod \ n)$$

$$x = y - k \ (mod \ n),$$

где

x — символ открытого текста,

y — символ шифрованного текста,

n — мощность алфавита (кол-во символов)

k — ключ.

Пример:

Исходное сообщение: «**Криптография**»

Ключ: 5

Сообщение	**К**	**Р**	**И**	**П**	**Т**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 + 5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	**П**	**Х**	**Н**	**Ф**	**Ч**	**У**	**З**	**Х**	**Е**	**Щ**	**Н**	**Д**

Будучи одноалфавитным шифром подстановки, шифр Цезаря подвержен частотному анализу. Но ещё одна большая его слабость — это недостаточное количество возможных ключей (всего 33 для русского алфавита и 26 для английского), что делает возможной атаку грубой силой.

Криптоаналитик может выписать открытый текст для всех вероятных ключей, один из этих вариантов и будет расшифровкой сообщения – ***файл Mathematica***!

Частотный анализ

Одним из методов атак является ***частотный анализ***.

Распределение букв в **криптотексте** сравнивается с распределением букв в алфавите исходного сообщения.

Буквы с наибольшей частотой в криптотексте заменяются на букву с наибольшей частотой из алфавита.

Вероятность успешного вскрытия повышается с увеличением длины криптотекста.

Существуют множество различных таблиц о распределении букв в том или ином языке, но ни одна из них не содержит окончательной информации - даже порядок букв может отличаться в различных таблицах. Распределение букв очень сильно зависит от типа теста: проза, разговорный язык, технический язык и т.п.

Практически в каждом языке примерно девять букв заполняют около 70% любого текста – остальное распределение зависит от содержания и формы текста.

Русский		Английский		Немецкий		Французский		Итальянский		Финский	
Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
о	0.1090	e	0.1251	e	0.1846	e	0.1587	e	0.1179	a	0.1206
е	0.0872	t	0.0925	n	0.1142	a	0.0942	a	0.1174	i	0.1059
а	0.0751	a	0.0804	i	0.0802	i	0.0841	i	0.1128	t	0.0976
и	0.0751	o	0.0760	r	0.0714	s	0.0790	o	0.0983	n	0.0864
н	0.0642	i	0.0726	s	0.0704	t	0.0726	n	0.0688	e	0.0811
т	0.0642	n	0.0709	a	0.0538	n	0.0715	l	0.0651	s	0.0783
с	0.0545	s	0.0654	t	0.0522	r	0.0646	r	0.0637	l	0.0586
р	0.0484	r	0.0612	u	0.0501	u	0.0624	t	0.0562	o	0.0554
в	0.0460	h	0.0549	d	0.0494	l	0.0534	s	0.0498	k	0.0520
Всего	0.6235	Всего	0.6990	Всего	0.7263	Всего	0.7405	Всего	0.7500	Всего	0.7359

Простейшая защита против атак, основанных на подсчете частот, обеспечивается в системе омофонов (HOMOPHONES) - однозвучных подстановочных шифров, в которых один символ открытого текста отображается на несколько символов шифротекста, их число пропорционально частоте появления буквы.

Шифруя букву исходного сообщения, мы выбираем случайно одну из ее замен. Следовательно простой подсчет частот ничего не дает криптоаналитику.

Однако доступна информация о распределении пар и троек букв в различных естественных языках.

Криптоанализ, основанный на такой информации будет более успешным.

Полиалфавитные подстановочные шифры
были изобретены Лином Баттистой (Lean Battista) в 1568 году.

Основная идея многоалфавитных систем состоит в том, что на протяжении всего текста одна и та же буква может быть зашифрована по-разному.

Т.е. замены для буквы выбираются ***из многих алфавитов*** в зависимости от положения в тексте. Это является хорошей защитой от простого подсчета частот, так как не существует единой маскировки для каждой буквы в криптотексте.

В данных шифрах используются множественные однобуквенные ключи, каждый из которых используется для шифрования одного символа открытого текста.
Первым ключом шифруется первый символ открытого текста, вторым - второй, и т.д. После использования всех ключей они повторяются циклически.

Система шифрования Вижинера

Система Вижинера впервые была опубликована в 1586г. и является одной из старейших и наиболее известных многоалфавитных систем.

Свое название она получила по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Ключ – набор из **d** букв. Шифрование по формуле

$$c(i)=m(i)+k(i) \bmod n$$

где **k(i) –** буква ключа полученная сокращением числа **i** по модулю **d**

Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением.
В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера.

Сообщение **ПРИЛЕТАЮСЕДЬМОГО**

Ключ **АМБРОЗИЯАМБРОЗИЯ**

Шифртекст **ПЪЙЫУЩИЭССЕКЬХЛН**

Если d=1 – получаем **шифр Цезаря**.

Шифры Бофора подобны **шифру Виженера**:

Ключ – набор из **d** букв. Шифрование по формуле

$$c(i)=k(i)-m(i) \bmod n$$
$$c(i)=m(i)-k(i) \bmod n$$

где **k(i) –** буква ключа полученная сокращением числа **i** по модулю **d**

Шифр с автоключом

Дальнейшей модификацией системы Виженера является система шифров с *автоключом(auto-key),* приписываемая математику XVIв. Дж. Кардано.

Шифрование начинается с помощью "первичного ключа" (который является настоящим ключом в нашем смысле) и продолжается с помощью сообщения или криптограммы, смещенной на длину первичного ключа, затем производится сложение по модулю, равному мощности алфавита.

Сообщение	П Р И В Е Т Ф И З И К И
Первичный ключ	С П
Автоключ	П Р И В Е Т Ф И З
Шифротекст	С У Ч Х Ф В Ч Т Н Ю П В Ы

Метод Казиски - криптоанализ

Примерно в 1860г. немецким криптоаналитиком Ф.У.Казиски(Kasisky) был изобретен метод вскрытия систем с неизвестным периодом с помощью обнаружения одинаковых слов в криптотексте.

Допустим, слово ЫВАП появляется дважды с 13 буквами между двумя появлениями.

Это может быть случайно, а может означать тот факт, что одинаковая часть сообщения зашифрована начиная с той же позиции ключа.

Тогда расстояние между двумя Ы равно 16 и кратно длине ключа. поэтому возможная длина ключа равна 2, 4, 8, 16.

Когда получается несколько таких предположений о длине ключа, некоторые из которых могут оказаться неправильными, то можно будет сделать верное предположение о длине ключа.

Более длинные повторяющиеся слова предпочтительнее. Также преимуществом для криптоаналитика является повторение слов более одного раза.

Шифры простой замены - шифр Атбаш

Шифр простой замены, использованный для еврейского алфавита и получивший оттуда свое название.

Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю.

(*алеф*(первая буква) заменяется на *тау* (последнюю), *бет*(вторая) заменяется на *шин*(предпоследняя) из этих сочетаний шифр и получил свое название).

Шифр Атбаш для английского алфавита:
Исходный алфавит:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Алфавит замены:
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Шифры простой замены **–**
шифр с использованием кодового слова

Шифр с использованием кодового слова является одним из самых простых как в реализации так и в расшифровывании.

Идея заключается в том что выбирается ***кодовое слово***, которое пишется впереди, затем выписываются остальные буквы алфавита в своем порядке.

Шифр с использованием кодового слова WORD.

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

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

Шифры сложной замены

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены.

Многоалфавитные шифры замены предложил и ввел в практику криптографии **Леон Батист Альберти**, который также был известным архитектором и теоретиком искусства. Его книга "Трактат о шифре", написанная в 1566г., представляла собой первый в Европе научный труд по криптологии.

Криптологи всего мира почитают **Альберти** основоположником криптологии

Блочные шифры – код Хилла.

Вместо букв пишем числа, например A = 0, B =1, ..., Z=25,

Блок из **n** букв рассматривается как вектор, который при шифровании умножается на **n × n** матрицу по mod 26 (в английском алфавите).

Пример: сообщение **ACT** и ключ **GYBNQKURP** :

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

криптограмма будет **POH**

Биграммный шифр Плейфейр (playfair, в переводе "честная игра“)

Шифр Плейфейр, изобретенный в 1854г., является наиболее известным биграммным шифром замены. Он применялся Великобританией во время первой мировой войны.

Основой шифра Плейфейр является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Текст **ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ**

Биграммы **ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ**

Криптограмма: **ГП ДУ ОВ ДЛ НУ ПД ДР ЦЫ ГА ЧТ**

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

Шифр "двойной квадрат" Уитстона

В 1854г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом".

Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним процедуру шифрования этим шифром на примере.

1. Пусть имеются две таблицы со случайно расположенными в них алфавитами.
2. Перед шифрованием исходное сообщение разбивают на биграммы.
3. Каждая биграмма шифруется отдельно.
4. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице.
5. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах.
6. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

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

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

Рис. 2.10. Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат"

М: ПР ИЛ ЕТ АЮ _Ш ЕС ТО ГО

С: ПЕ ОВ ЩН ФМ ЕШ РФ БЖ ДЦ

Шифр Вернама

Шифр Вернама, или **одноразовый блокнот**, был изобретен в 1917 году Мейджором Джозефом Моборном (Major Joseph Mauborn) и Гильбертом Вернамом (Gilbert Vernam) из AT&T (American Telephone & Telegraph).

В классическом понимании одноразовый блокнот является большой неповторяющейся последовательностью символов ключа, распределенных случайным образом. Первоначально это была одноразовая лента для телетайпов.

Отправитель использовал каждый символ ключа для шифрования только одного символа открытого текста. Шифрование представляет собой сложение по модулю **n** (мощность алфавита) символа открытого текста и символа ключа из одноразового блокнота. Каждый символ ключа используется только один раз и для единственного сообщения, иначе даже если использовать блокнот размером в несколько гигабайт, при получении криптоаналитиком нескольких текстов с перекрывающимися ключами он сможет восстановить исходный текст.

Главным недостатком данной системы является то, что для каждого бита переданной информации должен быть заранее подготовлен бит ключевой информации, причем эти биты должны быть случайными.

При шифровании большого объема данных это является серьезным ограничением. Поэтому данная система используется только для передачи сообщений наивысшей секретности.

Чтобы обойти проблему предварительной передачи секретного ключа большого объема, придумано много различных схем генерации длинных потоков псевдослучайных цифр из нескольких коротких потоков в соответствии с некоторым алгоритмом.

Класс шифров Вернама - единственный класс шифров, для которого доказана (Шенноном) невскрываемость в абсолютном смысле этого термина.

Блочные шифры

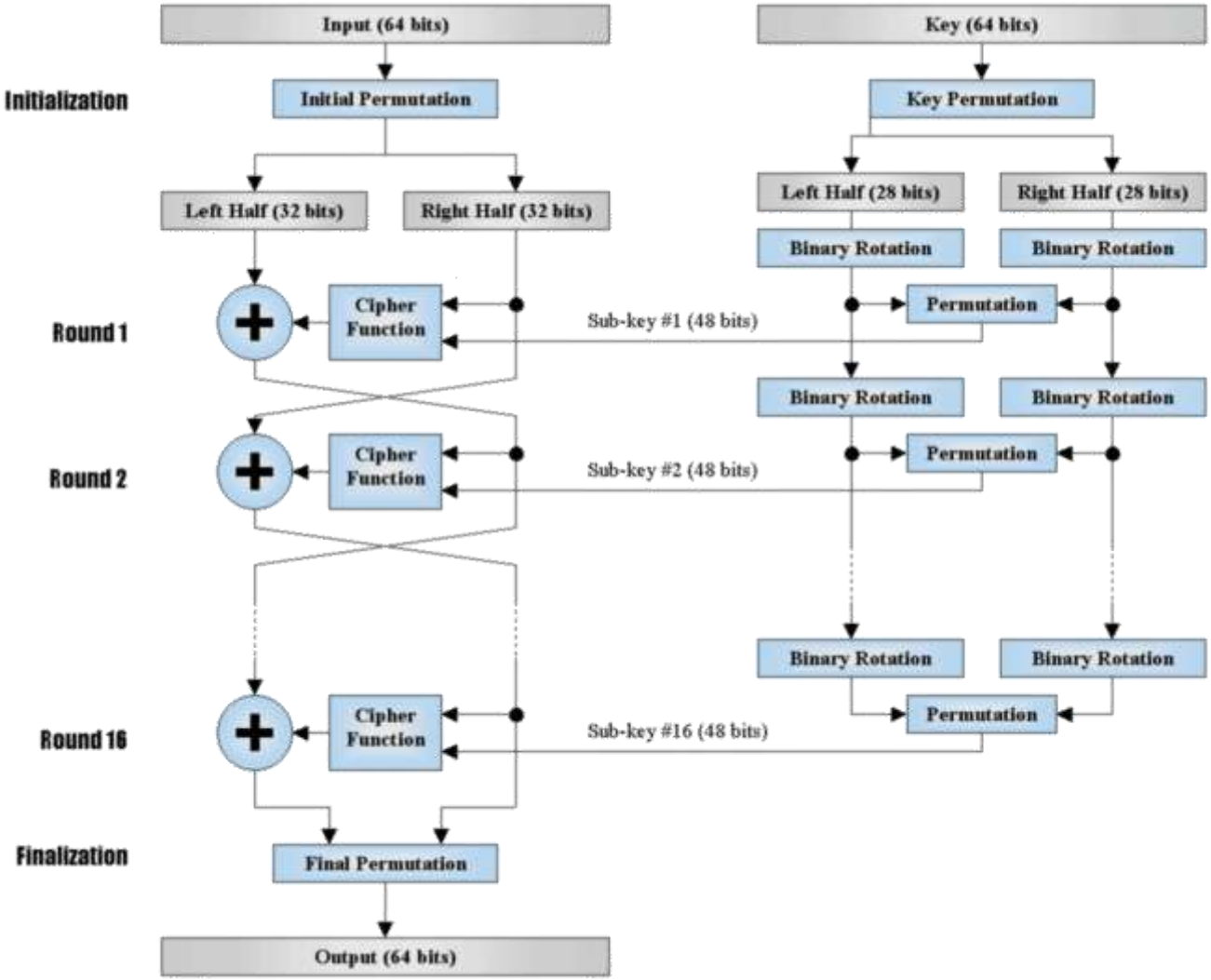
Блочные шифры представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста.

Блочные шифры на практике встречаются чаще, чем "чистые" преобразования того или иного класса в силу их более высокой криптостойкости.

Режим **электронной шифровальной книги** (electronic codebook) - это наиболее очевидный способ использования блочного шифра: блок открытого текста заменяется блоком шифротекста.

В режиме **сцепления блоков шифра** перед шифрованием над открытым текстом и предыдущим блоком шифротекста выполняется операция побитового сложения (XOR).

Алгоритм DES: более подробно



Ассимметричное шифрование

Основы криптографии с ***открытыми ключами*** были выдвинуты Уитфилдом **Диффи** (Whitfield Diffie) и Мартином **Хеллманом** (Martin Hellman), и независимо Ральфом **Мерклом** (Ralph Merkle).

Их вкладом в криптографию было убеждение, что ключи можно использовать парами - **ключ шифрования** и **ключ дешифрирования** - и что может быть невозможно получить один ключ из другого.

Диффи и Хеллман впервые представили эту идею на Национальной компьютерной конференции **1976**г., через несколько месяцев была опубликована их основополагающая работа "New Directions in Cryptography" ("Новые направления в криптографии").

Большинство безопасных алгоритмов с открытыми ключами основано на т.н. **необратимых функциях**

(*под этим понимается не теоретическая необратимость, а невозможность получить обратное значение используя современную технику за обозримый интервал времени*).

Все действующие сейчас системы опираются на один из следующих типов необратимых преобразований:

1. Разложение больших чисел на простые множители (**RSA**)

2. Вычисление логарифма в конечном поле (**криптосистема Эль-Гамаля**)

3. Вычисление корней алгебраических уравнений (**на основе эллиптических уравнений**)

Алгоритм RSA:

основные понятия

I. **Простое число** – делится только на 1 и на само себя

II. **Взаимопростые числа** не имеют ни одного общего делителя, кроме 1.

III. Результат операции **i** mod **j** – остаток от целочисленного деления **i** на **j**

Например:

26 mod 10= 2x10+6 mod 10=6

Алгоритм RSA: создание ключей

1. Возьмем два больших простых числа **p** и **q**

2. Определим число **n = p q**

3. Выберем большое случайное число **d,** которое должно быть взаимопростым с **(p-1)(q-1)** – *функцией Эйлера*
4. Определим такое число **e** для которого является истинным соотношение

   (e*d) mod(p-1)(q-1)=1

5. Назовем **(e.n) –** открытым (public)
   (d,n) – закрытым (private) ключом

6. Забудем **p** и **q**!!!!!!

Алгоритм RSA:

Шифрование состоит в разбивке сообщения на блоки из **n** символов

$$M(i),\ i=0,1,\ldots n-1$$

Каждое **M(i)** в каждом блоке надо зашифровать по правилу

$$C(i)=M(i)^e \bmod n$$

Чтобы расшифровать эти данные используя секретный ключ **(d,n)** необходимо вычислить в каждом блоке

$$M(i)= C(i)^d \bmod n$$

Стойкость алгоритма шифрования RSA основана на трудоемкости разложения произведения двух больших простых чисел на множители.

Пример:

Пусть **p = 3, q = 11**.
Тогда **n = pq = 33**, функция Эйлера **(p-1)(q-1) = 20**.
По этим числам выберем ***d = 3, e = 7***.

Рассмотрим шифрование последовательности **M=123** с помощью ключа (***7,33***).
Шифрование:

1) $y = \mathrm{mod}\ (1^7, 33) = 1$;
2) $y = \mathrm{mod}\ (2^7, 33) = \mathrm{mod}\ (128, 33) = 29$;
3) $y = \mathrm{mod}\ (3^7, 33) = \mathrm{mod}\ (2187, 33) = 9$.

C= 1, 29, 9.

Расшифровка с помощью ключа (***3,33***)

1) $x = \mathrm{mod}\ (1^3, 33) = 1$;
2) $x = \mathrm{mod}\ (29^3, 33) = \mathrm{mod}\ (24389, 33) = 2$;
3) $x = \mathrm{mod}\ (9^3, 33) = \mathrm{mod}\ (729, 33) = 3$.

Далее файл реальным шифрованием

Алгоритм RSA:

Если **n** – количество битов в модуле, то количество времени (памяти) для операций с

- ✓открытым ключом пропорционально $\mathbf{n^2}$
- ✓секретным ключом $\mathbf{n^3}$
- ✓создание ключей $\mathbf{n^4}$

Программная реализация DES работает быстрее по крайней мере в 100 раз, аппаратная от 1.000 до 10.000 раз!!!

Атака Винера на RSA

Мы уже отмечали, что в алгоритме RSA для ускорения операций с открытым ключом используют малые шифрующие экспоненты.

В некоторых же приложениях этой криптосистемы существеннее ускорить процессы расшифровывания.

Поэтому имеет смысл выбирать небольшую расшифровывающую экспоненту **d**. Ясно, что при этом получается большое значение открытой экспоненты **e**.

Слишком маленькое число в качестве секретной экспоненты **d** мы брать не можем, поскольку атакующий определит ее простым перебором – однако и “не очень маленькое” тоже можно найди достаточно легко.

Пусть у нас есть модуль ***n = pq***, причем ***q < p < 2q***.

Допустим, что наша расшифровывающая экспонента удовлетворяет неравенству:

$$d < \frac{1}{3} n^{1/4}$$

и нападающему это известно.

Кроме того, ему дана шифрующая экспонента **e** которая по определению

$$ed = 1 \pmod{\varphi},$$

где $\varphi(n) = (p - 1)(q - 1)$ ***функция Эйлера***.

Тогда существует число ***k***, такое, что

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

Таким образом, раскладывая число **e/n** в непрерывную дробь, можно узнать расшифровывающую экспоненту **d** , поочередно подставляя знаменатели подходящих дробей в выражение

$$M^{e^d} = M \ (mod \ n)$$

для некоторого случайного числа **M**. Получив равенство, найдем **d**.

Общее число подходящих дробей, которое нам придется при этом проверить, оценивается как **O (ln N)**.

Таким образом, изложенный метод дает **линейный по сложности алгоритм** определения секретного ключа в системе ***RSA***.

Таким образом, раскладывая число **e/n** в непрерывную дробь, можно узнать расшифровывающую экспоненту, поочередно используя знаменатели подходящих дробей в качестве ключа.

В качестве примера пусть

n = 9449868410449

e = 6792605526025

d =569

Разложение числа **e/n** имеет вид - искомый знаменатель найден на седьмом шаге

$$1, \frac{2}{3}, \frac{3}{4}, \frac{5}{7}, \frac{18}{25}, \frac{23}{32}, \frac{409}{569}, \frac{1659}{2308}, \ldots$$

Цепная дробь (или **непрерывная дробь**) — это математическое выражение вида

e/n= $$[a_0; a_1, a_2, a_3, \cdots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

Цепные дроби позволяют эффективно находить хорошие рациональные приближения вещественных чисел.

Как и ранее, мы видим, что во всех IT технологиях математика играет ключевую роль и, поэтому, ее надо учить……

Алгоритм Эль-Гамаля базируется на трудности вычисления дискретного логарифма.

Генерация ключей

1. Генерируется случайное простое число ***p*** длины ***n***.
2. Выбирается произвольное целое число ***g***, являющееся первообразным корнем по модулю ***p***.
3. Выбирается случайное число ***x*** из интервала **(1,*p*),** взаимно простое с ***p*-1**.
4. Вычисляется $y = g^x \bmod p$.
5. открытым ключом является тройка **(*p*,*g*,*y*),**
6. закрытым ключом — число ***x***.

Первообразный корень по модулю ***m*** — целое число ***g*** такое, что

$$g^{\phi(m)} \equiv 1 \mod m$$

где **ϕ(*m*)** - функция Эйлера

Шифрование - *алгоритм Эль-Гамаля*

Сообщение **M** шифруется так:

1. Выбирается случайное секретное число ***k***, взаимно простое с ***p* – 1**.
2. Вычисляется

$$a = g^k \bmod p,$$
$$b = y^k M \bmod p,$$

где ***M*** — исходное сообщение

Пара чисел **(*a*,*b*)** является **шифротекстом**.

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаль длиннее исходного сообщения M вдвое.

Расшифрование

Зная закрытый ключ ***x***, исходное сообщение можно вычислить из шифротекста (***a,b***) по формуле:

$$M = b/a^x \bmod p$$

Учитывая тот факт, что:

$$a^x \equiv g^{kx} \pmod p$$

и

$$b/a^x \equiv y^k M/a^x \equiv g^{xk} M/g^{xk} \equiv M \pmod p ,$$

то вышеприведенные формулы верны – ***k*** сокращается!!!!

Алгоритм Диффи-Хелмана.

Сначала генерируются два больших простых числа **n** и **q**.

Эти два числа не обязательно хранить в секрете.

Далее один из партнеров **P1** генерирует случайное число **x** и **посылает** другому участнику будущих обменов **P2** значение

$$A = q^x \bmod n$$

По получении **A** партнер **P2** генерирует случайное число **y** и посылает **P1** вычисленное значение

$$B = q^y \bmod n$$

Партнер **P1**, получив **B**, вычисляет

$$K_x = B^x \bmod n,$$

а партнер **P2** вычисляет

$$K_y = A^y \bmod n.$$

Алгоритм гарантирует, что числа K_y и K_x равны и могут быть использованы в качестве секретного ключа для шифрования.

Ведь даже перехватив числа A и B, трудно вычислить K_x или K_y.

Алгоритм Диффи-Хелмана, обеспечивая конфиденциальность передачи ключа, не может гарантировать того, что он прислан именно тем партнером, который предполагается.

Для решения этой проблемы был предложен протокол **STS** (station-to-station).

Этот протокол для идентификации отправителя использует технику электронной подписи. Подпись шифруется общим секретным ключом, после того как он сформирован.

Криптоанализ

Существует только один путь стать хорошим разработчиком криптографических алгоритмов --- быть хорошим криптоаналитиком и взламывать алгоритмы.

Множество. Снова и снова.

Только после того, как обучающийся продемонстрирует способности к криптоанализу чужих алгоритмов, он сможет серьезно браться за разработку собственных алгоритмов.

Брюс Шнайер (Bruce Schneier)

Криптоанализ

это отрасль знаний, целью которой является поиск и исследование методов взлома криптографических алгоритмов, а также сама процедура взлома.

Взлом шифра не обязательно метод поиска практических путей для перехватчика в целях восстановления открытого текста из шифртекста.

Взлом шифра это просто найденная слабость в шифре, которая может использоваться проще, чем простой перебор.

Никогда не забывайте, что простой перебор может требовать 2^128 шифрований, а атака - 2^110 шифрований для вскрытия.

Взлом может также требовать нереального количества частично известного или выбранного открытого текста 2^56 блоков или нереальных объемов хранилища – 2^80.

Невозможно понять что-нибудь в криптоанализе без хорошего знания основ **теории вероятности** и **статистики**.

Другие предметы, типа **дискретной математики** и компьютерных наук также полезны, хотя и не являются строго необходимыми.

Студенты должны знать или быть готовыми изучить **линейную алгебру, теорию групп, теорию сложности, комбинаторику и теорию графов**. Изучать их полезно параллельно с криптоанализом.

Преобразование сообщения в криптограмму всегда использует следующие принципы:

Рассеивание (**diffusion**) –
т.е изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;

Перемешивание (**confusion**) –
использование преобразований, затрудняющих получение статистических зависимостей между шифротекстом и открытым текстом.

При взломе необходимо это использовать!!!!!

Различные типы криптоанализа

- Ciphertext Only – анализ на основе только шифротекста
- Known Plaintext – анализ на основе невыбранного открытого текста
- Chosen Plaintext – анализ на основе выбранного открытого текста
- Chosen Ciphertext – анализ на основе выбранного шифротекста

На практике

Реальный криптоанализ основан на трех вещах:

- ✓ **Изучение системы шифрования в целом**
- ✓ **Изучение особенностей исходного текста**
- ✓ **Изучение особенностей ключевой системы**

Поиск ключа

- **Brutal-Force Attack** – атака методом “грубой силы”, т.е. полным перебором ключей

- Основная цель любого метода криптоанализа – улучшить время **Brutal-Force Attack**, или улучшить имеющееся соотношение время/память

- **Key-recovery** – метод нахождения наиболее вероятного раундового ключа,
с помощью перебора различных исходных текстов.
Используется в большинстве методов криптоанализа

Различные атаки

- Дифференциальный криптоанализ
- Линейный криптоанализ
- Модификации дифференциального и линейного анализов
- Интерполяционный криптоанализ
- Методы, основанные на слабости ключевых разверток

Алгоритмы (стандарты) шифрования периодически меняются (что видно на примере шифров LUCIFER, DES, FEAL, клиппер-чипов), а секретная информация часто имеет свойство стареть, то есть не представляет большого интереса для нарушителя спустя какое-то время после ее передачи по каналам связи в зашифрованном виде.

Поэтому зависимость эффекта от нахождения способа раскрытия ключей данного шифра во времени имеет максимум: в начале срока своего действия криптоалгоритм не имеет широкого распространения, а в конце срока он перестает быть популярным, а основной объем зашифрованной информации не представляет интереса.

Источники дополнительных сведений

Что и где почитать:

- Bruce Schneier “Self-Study Course in Block Cipher Cryptanalysis”, 2000
  http://www.counterpane.com/self-study.html
  - курс молодого бойца, т.е. для тех, кто хочет реально заняться криптоанализом
- http://www.distributed.net
  - знаменитые взломщики RC5 – просто посмотреть и насладиться =)
- Francois-Xavier Standaert & others “Cryptanalysis of Block Ciphers: the Survey”, 2001
  http://logic.pdmi.ras.ru/~yura/crypto/01crypto.pdf
  - самый полный обзор методов криптоанализа, однако много опечаток и непонятных мест
- Dave Rudolf “Development and Analysis of Block Ciphers and the DES System”, 2002
  http://www.cs.usask.ca/grads/dtr467/400
  - очень понятное введение в основы блочных шифров, внятно описан DES
- М. Анохин, «Блочные криптографические алгоритмы»
  http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html
  - отличный краткий обзор истории и современного состояния криптоанализа, ко всему прочему (УРА!) на русском языке