КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

ЛЕКЦИЯ 6. ОСНОВЫ КРИПТОГРАФИИ. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Профессор кафедры
доктор технических наук, старший научный сотрудник
ТУКЕЕВ Дмитрий Леонидович

УЧЕБНЫЕ ВОПРОСЫ

1. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.
2. КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ
3. ПРЕДВАРИТЕЛЬНЫЕ МАТЕМАТИЧЕСКИЕ ЗАМЕЧАНИЯ
4. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ.
5. ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ

ЛИТЕРАТУРА

1. Основы шифрования данных. Методические указания к лабораторным работам /Сост. Лясин Д.Н., Макушкин И.А. – Волгоград: Волгоград. гос. техн. ун-т. – 2008 г. – 18 с.

ВВЕДЕНИЕ

СПОСОБЫ ПЕРЕДАЧИ ИНФОРМАЦИИ АДРЕСАТУ В ТАЙНЕ ОТ ДРУГИХ ЛИЦ

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами (недостижимая задача в современных услових)

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации (разработкой таких средств и методов занимается стеганография).

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в измененном виде, чтобы восстановить ее мог только адресат (разработкой методов шифрования информации с целью ее защиты от незаконных пользователей занимается криптография, являющаяся составной частью криптологии).

1. Основные понятия криптографической защиты информации

Основные задачи криптографиии:

Обеспечение конфиденциальности данных - преобразование данных, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом.

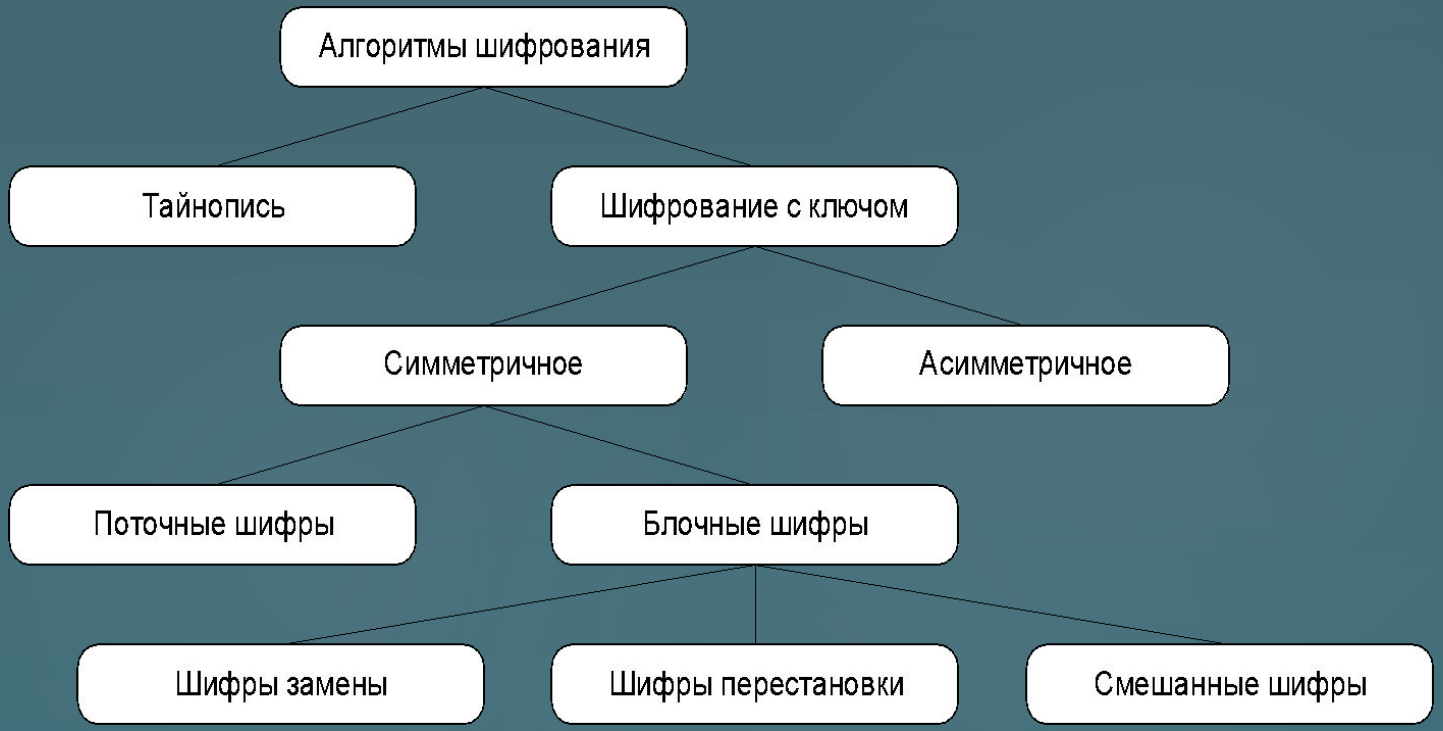
Обеспечение целостности данных — гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права.

Обеспечение аутентификации - проверка подлинности субъектов при обмене данными.

Обеспечение невозможности отказа от авторства — предотвращение возможности отказа субъектов от совершенных ими действий (обычно — невозможности отказа от подписи под документом).

Эта задача неотделима от двойственной — **обеспечение невозможности приписывания авторства.**

2. КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ



по объему информации, неизвестной третьей стороне:

Шифр называется **тайнописью**, *если нарушителю полностью неизвестен алгоритм выполненного над сообщением преобразования,*

Криптографическими *называют алгоритмы шифрования, в которых сам алгоритм преобразований широко известен и доступен для исследований каждому желающему, а шифрование производится на основе* ***ключа****, известного только отправителю и получателю информации.*

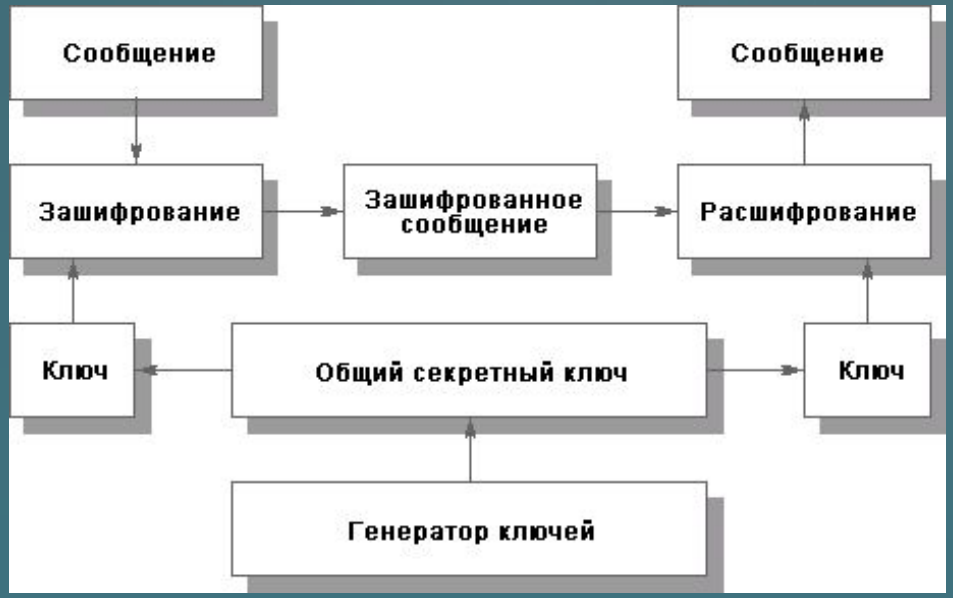
2. КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ

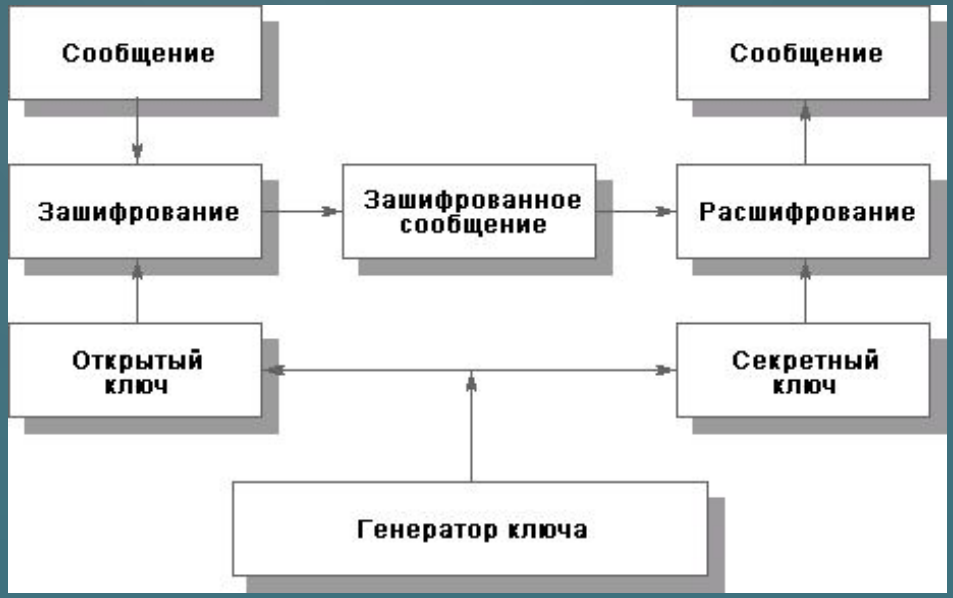
по степени идиентичности ключей для шифрования и дешифрования :

В симметричных криптоалгоритмах ключи, *используемые на передающей и приемной сторонах*, **полностью идентичны**.

Такой ключ несет в себе всю информацию о зашифрованном сообщении и поэтому не должен быть известен никому, кроме двух участвующих в защищенном обмене информацией сторон!

В асимметричном шифровании для шифрования применяется **один ключ**, а **для дешифрования – другой**.





2. КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ

по схеме обработки потока информации:

Поточный шифр (stream ciphers) обрабатывает информацию побитно - получив порцию из произвольного количества бит, может зашифровать/дешифровать ее. **Поточные шифры** удобны в каналах связи, где процесс передачи информации может обрываться в произвольный момент и затем через некоторый промежуток времени продолжаться дальше.

Побитовая обработка информации является неэффективной, когда имеется возможности для параллельной обработки.

В этих условиях применяют **блочные шифры**.

Блочные шифры (block ciphers) могут применяться только для обработки информации строго определенного объема. Размеры блока: 64, 128 или 256 бит.

Шифрование блоков произвольного размера невозможно!

Блочные шифры

- шифры замены (подстановки) - характеризуются тем, что отдельные части сообщения (буквы, слова, числа и др.) заменяются другими буквами, числами, символами и т.д.
- шифр перестановки - преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих;
- комбинированные шифры.

2. КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ

Типы шифров подстановки :

1. **Одноалфавитный шифр** подстановки (шифр простой замены) — шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.
2. **Однозвучный шифр** подстановки похож на одноалфавитный за исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов.
3. **Полигаммный шифр** подстановки заменяет не один символ, а целую группу.
4. **Многоалфавитный шифр** подстановки состоит из нескольких шифров простой замены.

Шифр простой замены - простой подстановочный шифр (моноалфавитный шифр) — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста.

Шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которой она генерируется.

К шифрам простой замены относятся многие способы шифрования, возникшие в древности или средневековье.

Для вскрытия подобных шифров используется **частотный криптоанализ.**

3. ПРЕДВАРИТЕЛЬНЫЕ МАТЕМАТИЧЕСКИЕ ЗАМЕЧАНИЯ

Задача 1. Сопоставьте буквы русского и латинского алфавита с их номером в алфавите.

Задача 2. (тест IQ Айзенка 1-36) Вставьте отсутствующие буквы

А	Е		И	З
Г	В		Ё	К

Задача 3. (тест IQ Айзенка 3-35) Вставьте отсутствующие буквы

Б	Е	И	
Ч	Т	Н	

Задача 4. (тест IQ Айзенка 1-39) Продолжите буквенную послед-сть:

А Г А Д А Ё А З А Л А _

Задача 5. (тест IQ Айзенка 2-10) Вставьте пропущенную букву

А Г Ж Л С _

Задача 6. (тест IQ Айзенка 2-39) Вставьте пропущенную букву

Б Д _ П Ш

Задача 7. (тест IQ Айзенка 3-10) Вставьте пропущенную букву

Л М Н К Р З Ф _

3. ПРЕДВАРИТЕЛЬНЫЕ МАТЕМАТИЧЕСКИЕ ЗАМЕЧАНИЯ

Задача 8. Найти: -17mod 26= … 48 mod 26= … 279mod 26= …
-17mod 33= … 48 mod 33= … 279mod 33= …
= ОСТАТ(48;26)

Задача 9. Найти мультипликативно-обратное $3^{-1}(\text{mod } 26)$= …
Решение: 3 * X = 1 mod 26 => X = (1 + 26*k)/3,
k = 1,2… пока X не станет целым… X = 9

В сложных случаях – алгоритм нахождения НОД Евклида!

17^{-1}mod 33= … 2^{-1}mod 33= … 5^{-1}mod 39= … 4^{-1}mod 39= …

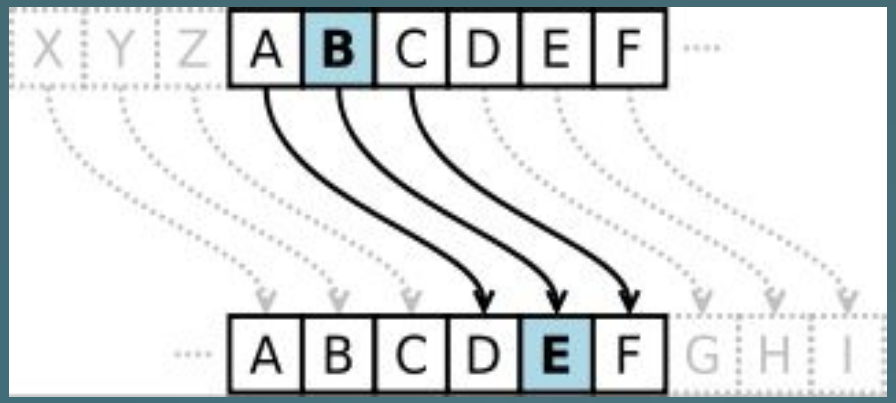
Для применения функции ОСТАТ(…;…) от степенных функций можно воспользоваться выражением:

x= x1 + x2 => a^x = a^(x1+x2)

mod (x;d) = mod[mod(x1;d)*mod(x2;d)]

3. ШИФР ЦЕЗАРЯ

При шифровании исходного текста каждая буква заменяется на другую букву того же алфавита. Замена осуществляется путем смещения по алфавиту от исходной буквы на К букв. Цезарь использовал шифр замены при смещении К= 3.



Число всех возможных замен **N!**,

где N – число букв в алфавите.

Для латинского алфавита
$26! \approx 4 \cdot 10^{26} \approx 2^{218}$.

A	B	C	D	E	F	Q	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
F	I	L	O	R	U	X	A	D	Q	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

И	Д	Е	Т	Б	Ы	Ч	О	К	К	А	Ч	А	Е	Т	С	Я

С	М	Н	Ы	Й	Д	А	Ч	У	У	И	А	И	Н	Ы	Ъ	З

И	Д	Е	Т	Б	Ы	Ч	О	К	К	А	Ч	А	Е	Т	С	Я

3. ШИФР ЦЕЗАРЯ

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

3. ШИФР ЦЕЗАРЯ

Шифр Цезаря с ключевым словом

В данной разновидности шифра Цезаря ключ задается числом *k* (0<=*k*<=*n*-1) и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, **начиная с *k*-й позиции**, **ключевое слово**. Оставшиеся буквы записываются в алфавитном порядке **после ключевого слова**. В итоге мы получаем подстановку для каждой буквы. Требование, чтобы все буквы ключевого слова были различными не обязательно, необходимо только записывать ключевое слово без повторения одинаковых букв

ключевое слово – ‘ключ’
k=2

Исходный алфавит	а	б	в	г	д	е	ё	ж	…	э	ю	я
Измененный алфавит	э	я	**к**	**л**	**ю**	**ч**	а	б	…	ь	ы	ъ

Исходный текст: пример шифрования

Зашифрованный текст: ймгжчм фгрмикэзгъ

4. АФФИННАЯ КРИПТОСИСТЕМА

Обобщением системы Цезаря является аффинная криптосистема. Она определяется двумя числами *a* и *b*, где 0<=*a, b*<=*n*-1, *n* - мощность алфавита. Числа *a* и *n* должны быть взаимно просты, например для алфавита русского языка (N = 33) коэффициент *a* может принимать только значения, взаимно простые с числом 33: 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32.

ПРИМЕР **n = 33, a = 2, b = 5,** мамамылараму

РЕШЕНИЕ: процедура шифрования $Ш_i = (a*T_i + b)(mod\ 33) = (2*T_i + 5)(mod\ 33)$

процедура дешифрования $T_i = (Ш_i - b)* a^{-1} (mod\ 33)$

$a^{-1} (mod\ 33) = 2^{-1} (mod\ 33) = 17 =>$

процедура дешифрования $T_i = (Ш_i - 5)* 17 (mod\ 33)$

исходный текст	М	А	М	А	М	Ы	Л	А	Р	А	М	У
исходный текст в числах	14	1	14	1	14	29	13	1	18	1	14	21
результат шифр-я без mod	33	7	33	7	33	63	31	7	41	7	33	47
шифрованный текст в числах	33	7	33	7	33	30	31	7	8	7	33	14
шифрованное сообщение	я	ё	я	ё	я	ь	э	ё	ж	ё	я	м
шифрованный текст в числах	33	7	33	7	33	30	31	7	8	7	33	14
результат дешифр-я без mod	476	34	476	34	476	425	442	34	51	34	476	153
исходный текст в числах	14	1	14	1	14	29	13	1	18	1	14	21
исходный текст	М	А	М	А	М	Ы	Л	А	Р	А	М	У

5. КВАДРАТ ПОЛИБИЯ

Еще одной модификацией одноалфавитной замены является квадрат Полибия, в котором символ алфавита заменяется парой чисел или символов по определенному правилу. Рассмотрим прямоугольник, часто называемый доской Полибия.

В такой прямоугольник записывается алфавит, причем схема записи держится в тайне и составляет ключ шифрования. Для того чтобы получались приближенные к квадрату матрицы (6x6, 5x7, 6x5), в алфавит могут включаться знаки препинания или исключаться редко используемые символы (такие как ‘ё’, ‘й’).

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

В процессе шифрования каждая буква открытого текста представляется в шифротексте парой букв, указывающих строку и столбец, в которых расположена данная буква.

Так представлениями букв В, Г, П, У будут АВ, АГ, ВВ, ГА соответственно.

Если использовать приведенный выше квадрат в качестве ключа шифрования, то фраза «ПРИМЕР ШИФРОВАНИЯ» будет зашифрована в «ВВВГБВБЕАЕВГЕБГЕБВГБВГВБАВААВАБВЕА».

5. МЕТОД ЧАСТОТНОГО КРИПТОАНАЛИЗА

один из методов криптоанализа, основывающийся на предположении о том, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам и т.д. в случае полиалфавитных шифров. Например, для вскрытия параметров *a* и *b* аффинной криптосистемы потребуется найти соответствие двух букв – наиболее часто встречающейся в шифротексте и второй по частоте.

Наиболее известным случаем его применения в реальной жизни, возможно, является дешифровка египетских иероглифов Ж.-Ф. Шампольоном в 1822 году.

Варианты:

По буквам: **о — 11.35%; е — 8.93%; а — 8.23%; н — 6.71%; и — 6.48%; т — 6.17%; с — 5.22%; л — 4.95%; в — 4.47%; р — 4.17%**

По словам - и, не, в, что, он, я, на, с, она, как, но, его, это, к, а, все, ее, было, так, же, то, сказал, за, ты, о, у, ему, мне, только, по, меня, бы, да, вы, от, был, когда, из, для, еще, теперь, они, сказала, уже, него, нет, была, ей, быть, ну, ни, если, очень, ничего, вот, себя, чтобы, себе, этого, может, того, до, мы, их, ли, были, есть, чем, или, ней

5. Шифры Виженера и Гронсфельда

В XVI веке французский дипломат Блез де Виженер предложил модификацию шифра замен, которая впоследствии получила его имя. В данном шифре ключ задается фразой из *d* букв. Ключевая фраза подписывается с повторением под сообщением. Букву шифротекста необходимо находить как сумму по mod числа буквы сообщения и числа соответствующей буквы ключа.

ш	и	ф	р		в	и	ж	е	н	е	р	а
26	10	22	18	34	3	10	8	6	15	6	18	1
к	л	ю	ч	к	л	ю	ч	к	л	ю	ч	к
12	13	32	25	12	13	32	25	12	13	32	25	12
38	23	54	43	46	16	42	33	18	28	38	43	13
4	23	20	9	12	16	8	33	18	28	4	9	13
г	х	т	з	к	о	ж	я	р	ь	г	з	л
4	23	20	9	12	16	8	33	18	28	4	9	13
12	13	32	25	12	13	32	25	12	13	32	25	12
-8	10	-12	-16	0	3	-24	8	6	15	-28	-16	1
26	10	22	18	34	3	10	8	6	15	6	18	1
ш	и	ф	р		в	и	ж	е	н	е	р	а

Принципиальным отличием данного шифра от всех предыдущих является то, что он относится к классу многоалфавитных алгоритмов – как нетрудно заметить, одной и той же букве шифротекста могут соответствовать различные символы открытого текста в зависимости от того, каким символом ключа они были замаскированы.

Шифр Гронсфельда повторяет процедуру шифрования Виженера, но вместо порядкового номера символа ключа в алфавите использует непосредственное десятичное значение заданного числа.

5. ШИФРОВАНИЕ БИГРАММАМИ

В начале XVI века аббат из Германии Иоганн Трисемус предложил шифровать по две буквы за раз. Шифры, использующие подобный принцип, были названы **биграм-мными**. Наиболее известный шифр биграммами называется Playfair. Он применялся Великобританией в I МВ. Открытый текст разбивался на пары букв (биграммы) и текст шифровки строился из него по следующим трём очень простым правилам:

ключевая фраза – ‘шифрование’

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

открытый текст:

МЕ|ТО|Д_|БИ|ГР|АМ|М_|

шифротекст:

ЙД|ХФ|Е-|НР|БО|ДЖ|К-|

1. Если обе буквы биграммы исходного текста принадлежат одной колонке таблицы, то буквами шифра считаются буквы, которые лежат под ними. Так биграмма ИН дает текст шифровки НЗ. Если буква открытого текста находится в нижнем ряду, то для шифра берется соответствующая буква из верхнего ряда и биграмма НЯ дает шифр ЗИ. (Биграмма из одной буквы или пары одинаковых букв тоже подчиняется этому правилу, и текст ОО дает шифр ГГ).
2. Если обе буквы биграммы исходного текста принадлежат одной строке таблицы, то буквами шифра считаются буквы, которые лежат справа от них. Так биграмма АБ дает текст шифровки НГ. Если буква открытого текста находится в крайней правой колонке, то для шифра берется буква из крайней левой колонки той же строки и биграмма АД дает шифр НА.
3. Если обе буквы биграммы открытого текста лежат в разных рядах и колонках, то вместо них берутся такие две буквы, чтобы вся их четверка представляла прямоугольник. Например, биграмма ЕК шифруется как БИ (КЕ зашифруется ЙБ).

5. ШИФРОВАНИЕ БИГРАММАМИ

ШИФРОВАНИЕ БИГРАММАМИ С ДВОЙНЫМ КВАДРАТОМ

В 1854 году англичанин Чарльз Уитстон разработал новую шифровку биграммами, которую называют двойной квадрат. Шифрование здесь происходит аналогично шифру Playfair, но биграммы шифруются по двум таблицам, случайным образом заполненных алфавитами. Для пары символов из исходного сообщения строится прямоугольник в двух таблицах по правилу – первая буква в левой таблице является одним углом, вторая в правой - другим. Буквы биграммы шифра берутся из двух оставшихся вершин прямоугольника. Если обе буквы лежат в одних и тех же строках, то буквы шифра берут из той же строки, но в следующем столбце таблицы (для последнего столбца – из первого столбца).

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

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

открытый текст: МЕ|ТО|Д_|БИ|ГР|АМ|М_|

шифротекст: ФВ|ЪФ|Х-|ХК|Б,|ЖУ|З-|

6. ИСПОЛЬЗОВАНИЕ КНИЖНЫХ ШИФРОВ

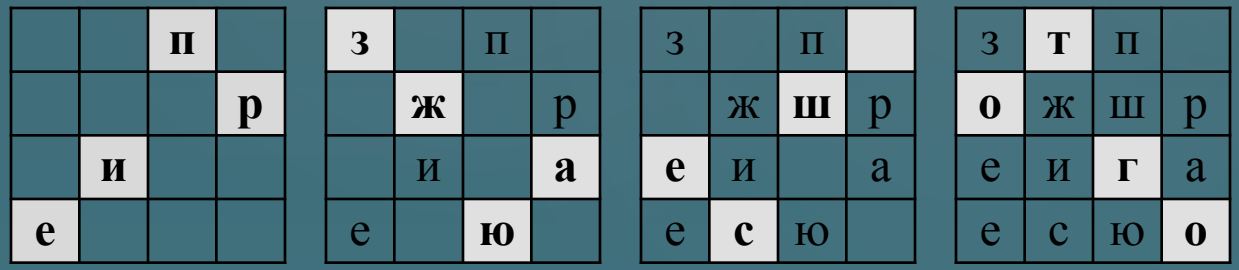
При использовании подобных шифров в качестве ключа использовалось содержимое книг, экземпляры которых (или возможность доступа) имелись у обеих обменивающихся сторон. Участники конфиденциального обмена заранее договаривались о смещении в книге (номер страницы, номер строки, смещение в строке, длина кодового слова), которое будет использоваться в качестве шифра. Информацию о позиции ключа в книге можно включать в передаваемое сообщение и в открытом виде при условии, что в секрете держится название самой книги. Для повышения стойкости шифра к взлому желательно обеспечить смену ключа для каждого нового сообщения.

7. ШИФРЫ ПЕРЕСТАНОВОЧНОГО ТИПА

КВАДРАТ КАРДАНО

В XVI веке итальянский математик и философ Дж. Кардано предложил новый тип шифра, основанный на очень простой и в то же время надежной перестановке букв открытого текста. Для шифрования он преложил использовать квадрат с прорезанными в нем несколькими ячейками. Ячейки прорезались таким образом, чтобы при повороте квадрата на 90, 180 и 270 градусов в прорезях поочередно появлялись все позиции исходного квадрата, причем по одному разу. Шифр получил название **квадрата Кардано.**

При шифровании квадрат накладывается на лист бумаги сначала в исходном положении и в прорези записывается первая часть сообщения, затем квадрат поворачивается на 90° и в прорези вписывается вторая часть, и т.д. После того как будут заполнены все ячейки квадрата, шифротекст считывается их него построчно



Открытый текст:
приезжаю шестого

Шифротекст:
зтп ожшреигаесюо

Для дешифрации сообщения необходимо иметь точную копию квадрата, использовавшегося при шифровании (расположение прорезей на квадрате и составляет ключ)

7. ШИФРЫ ПЕРЕСТАНОВОЧНОГО ТИПА

ПЕРЕСТАНОВОЧНЫЙ ШИФР С КЛЮЧЕВЫМ СЛОВОМ

Буквы ключевого слова без повторений записываются в первую строку таблицы, определяя таким образом количество ее столбцов. Буквы сообщения записываются в таблицу построчно. Сформированная таким образом таблица сортируется по столбцам, критерием сортировки является порядок следования символа первой строки в алфавите. После сортировки шифрованный текст переписывается по столбцам.

Дешифрация осуществляется по известному ключу обратными преобразованиями шифротекста в таблице: сначала шифротекст вписывается в таблицу по столбцам, затем столбцы переставляются, после чего открытый текст извлекается из таблицы построчно.

Ш	И	Ф	Р
П	Е	Р	Е
С	Т	А	Н
О	В	О	Ч
Н	Ы	Й	
Ш	И	Ф	Р

Ключевая фраза: шифр

И	Р	Ф	Ш
Е	Е	Р	П
Т	Н	А	С
В	Ч	О	О
Ы		Й	Н
И	Р	Ф	Ш

Открытый текст:
перестановочный шифр

Шифротекст:
етвыиенч рраойфпсонш

7. ПРОПОРЦИОНАЛЬНЫЕ ШИФРЫ

К одноалфавитным методам подстановки относятся пропорциональные шифры, в которых уравнивается частота появления зашифрованных знаков для защиты от раскрытия с помощью частотного анализа. Для знаков, встречающихся часто, используется относительно большое число возможных эквивалентов. Для менее используемых исходных знаков может оказаться достаточным одного или двух эквивалентов. При шифровании замена для символа открытого текста выбирается либо случайным, либо определенным образом (например, по порядку).

При использовании пропорционального шифра в качестве замены символам обычно выбираются числа. Например, поставим в соответствие буквам русского языка трехзначные числа, как указано на таблица 2.5

Символ	Варианты замены					Символ	Варианты замены					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Пробел	751	769	758	801	849	35

БОЛЬШОЙ СЕКРЕТ

10175713256210321376275 1-8007617541341307 59

8. ШИФР СЛОЖНОЙ ЗАМЕНЫ

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита может быть преобразован в несколько различных символов шифровальных алфавитов **М.**

1. Подготовка таблицы шифрования

а	б	в	…	я
Ма	Мб	Мв		Мя

Ма, Мб, Мв, …, Мя –
попарно не пересекающиеся множества

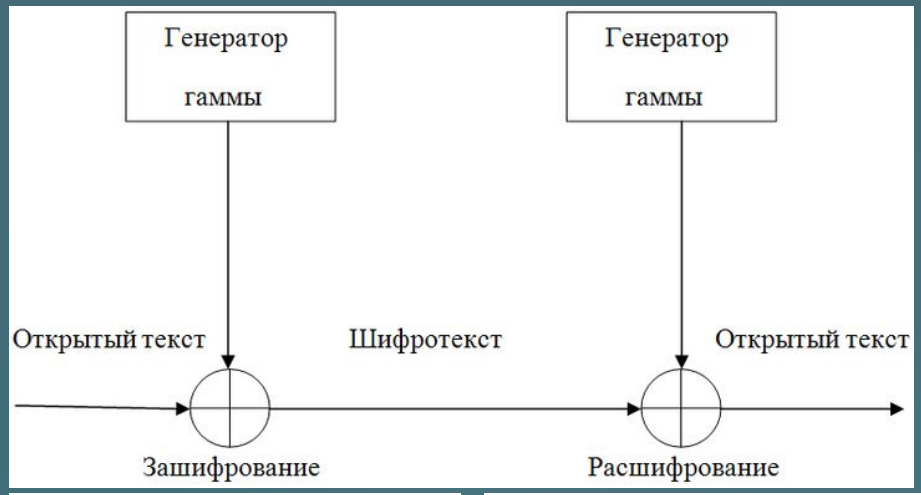
1. АБВГДЕ..... .....ЭЮЯ
2. БВГДЕЖ..... .....ЮЯА
3. ВГДЕЖЗ..... .....ЯАБ
4. ГДЕЖЗИ..... .....АБВ
5. ДЕЖЭИК..... .....БВГ
6. ЕЖЗИКЛ..... .....ВГД
7. ....
8. ЯАБВГД..... .....ЬЭЮ

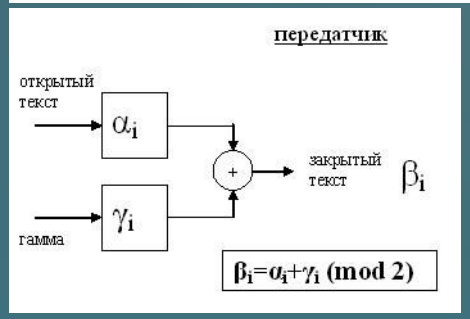
Степень обеспечиваемой защиты теоретически пропорциональна длине периода в последовательности используемых алфавитов М.

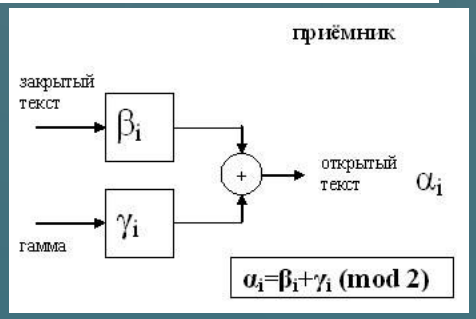
9. ГАММИРОВАНИЕ

Гаммирование - класс шифров многоалфавитной замены, в которых с помощью секретного ключа k генерируется последовательность символов - **гамма** $g=g_1g_2\ldots g_i\ldots$.

Расшифрование осуществляется применением к символам **шифртекста** и **гаммы** обратной операции.







Под гаммированием понимают процесс наложения по определенному закону (чаще всего с использованием операции сложения по модулю 2) гаммы шифра на открытые данные. Гамма шифра – это псевдослучайная последовательность целых чисел, для генерации которых наиболее часто применяется так называемый линейный конгруэнтный генератор. Закон функционирования такого генератора описывается соотношением:

$$T_i = (T_{i-1} \cdot A + C) \bmod M \qquad (1)$$

где T_i – текущее число последовательности;
T_{i-1} - предыдущее число последовательности;
A, C и M – константы; M – модуль;
A – множитель; C – приращение;
T_0 – порождающее число.

Требования к гамме:

Для каждого сообщения - новую гамму (повторное использование гаммы недопустимо).
Для формирования гаммы использовать аппаратные ГСЧ на основе физических процессов.
Длина гаммы должна быть не меньше длины защищаемого сообщения.

9. ГАММИРОВАНИЕ

Текущее псевдослучайное число получают из предыдущего числа умножением его на коэффициент A, сложением с приращением C и вычислением целочисленного остатка от деления на модуль M. Данное уравнение генерирует псевдослучайные числа с периодом повторения, который зависит от выбираемых значений параметров A, C и M. Значение модуля M берется равным 2^n, либо равным простому числу, например $M = 2^{31} - 1$. Приращение C должно быть взаимно простым с M, коэффициент A должен быть нечетным числом.

ЗАДАЧА 1

Зашифровать фамилию и полное имя студента методом гаммирования.

Таблица 1

Константа	Значение
T_0	7
A	9
C	Сумма двух последних цифр № зачетки
M	64

Таблица 2

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

9. ГАММИРОВАНИЕ

Шифрование текста методом гаммирования выполняется в следующей последовательности:

1. Определить константы шифрования по табл. 1.
2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.
3. Сгенерировать гамму шифра в соответствии с выражением (1).
4. Полученные числа (шифруемый текст и гамма шифра) перевести в двоичный. Замечание. Каждое число представляется байтом.
5. Наложить гамму шифра на шифруемый текст по формуле (2):

$$Ш_i = C_i \oplus T_i \qquad (2)$$

где $Ш_i$ – i - ый символ шифрограммы, представленный в двоичном коде;
C_i – ый символ исходного текста, представленный в двоичном коде.

6. Полученную шифрограмму перевести в десятичный код и по табл. 2 получить текстовую форму шифрограммы. Замечание. В процессе выполнения операции сложение по модулю 2 могут получиться числа больше 32. В этом случае рекомендуется выполнить операцию mod32. Однако при дешифровке необходимо использовать исходное число.

9. ГАММИРОВАНИЕ

Шифрование текста методом гаммирования:

Исходный текст: *Гаммирование*

Исходный текст в шестнадцатеричном виде:

83 A0 AC AC A8 E0 AE A2 A0 AD A8 A5

Гамма (Ключ): *Весна (82 A5 E1 AD A0)*

Гаммирование

Исх. биты	1000	0011	1010	0000	1010	1100
Гамма	1000	0010	1010	0101	1110	0001
Результат	0000	0001	0000	0101	0100	1101

Исх. биты	1010	1100	1010	1000	1110	0000
Гамма	1010	1101	1010	0000	1000	0010
Результат	0000	0001	0000	1000	0110	0010

Исх. биты	1010	1110	1010	0010	1010	0000
Гамма	1010	0101	1110	0001	1010	1101
Результат	0000	1011	0100	0011	0000	1101

Исх. биты	1010	1101	1010	1000	1010	0101
Гамма	1000	0010	1010	0101	1110	0001
Результат	0010	1111	0000	1101	0100	0101

Закодированный текст в шестнадцатеричном виде:

01 05 4D 01 08 62 0B 43 0D 2F 0D 45

При использовании метода гаммирования ключом является последовательность, с которой производится сложение – гамма. Если гамма короче, чем сообщение, предназначенное для зашифрования, гамма повторяется требуемое число раз. Так в примере на рис. 2.6 длина исходного сообщения равна двенадцати байтам, а длина ключа – пяти байтам. Следовательно, для зашифрования гамма должна быть повторена 2 раза полностью и еще один раз частично.

9. ГАММИРОВАНИЕ

Шифрование текста методом гаммирования:

10. АБСОЛЮТНО СТОЙКИЙ ШИФР И ГАММИРОВАНИЕ

Абсолютно стойким является гаммирование с бесконечной равновероятной случайной гаммой, т.е. процедура шифрования, удовлетворяющая условиям:

1. все символы гаммы полностью случайны и появляются в гамме с равными вероятностями;
2. длина гаммы равна длине открытого текста или превышает ее;
3. каждый ключ (гамма) используется для шифрования только одного текста, а потом уничтожается.