Лекция 4. Основные понятия криптографической защиты. Симметричные алгоритмы шифрования

Вопросы:

1. Основные понятия криптографической защиты информации

2. Симметричные алгоритмы шифрования

3. Требования к системам симметричного шифрования

Рекомендуемая литература

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. – М.: ДМК Пресс, 2008. – 544 с. Стр. 113-136.

2. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Госстандарт СССР, 1989.

3. Румянцев К.Е., Голубчиков Д.М. Квантовая криптография: принципы, протоколы, системы / Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. - 37 с.

Способы передачи информации адресату в тайне от других лиц

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами (современный уровень развития науки и техники пока не позволяет сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации).

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

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

Основные понятия криптографической защиты информации

Криптография – наука о методах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей. Такие методы и способы преобразования информации называются шифрами.

Криптоанализ – наука о методах и способах вскрытия шифров.

Зашифрование – процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование – процесс обратный шифрованию, т.е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Ключ – сменный элемент шифра, который применяется для шифрования конкретного сообщения.

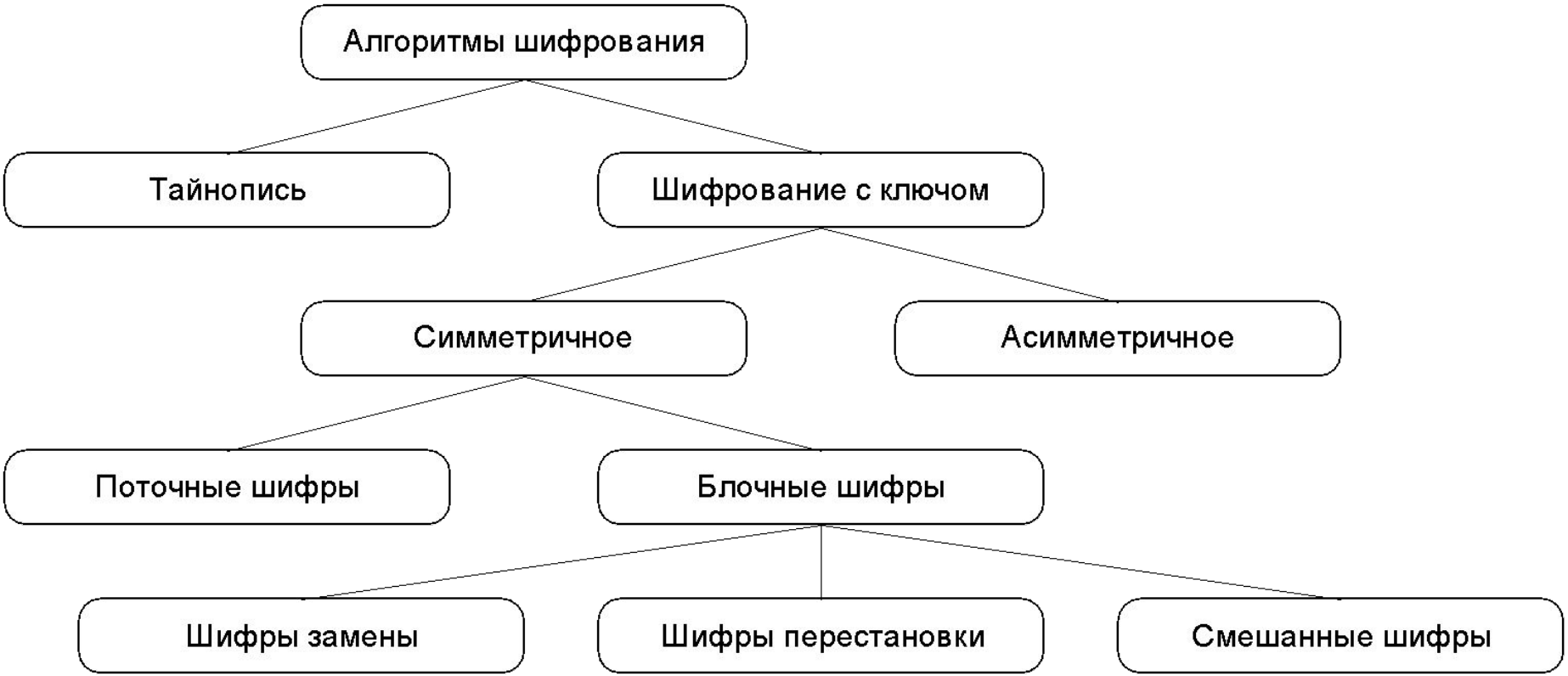
Стойкость шифра – способность шифра противостоять всевозможным атакам.

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.

Криптография используется в следующих *сервисах безопасности:* ***шифровании***, ***контроле целостности***, ***аутентификации*** (Аутентифика́ция — процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей).

Классификация алгоритмов шифрования

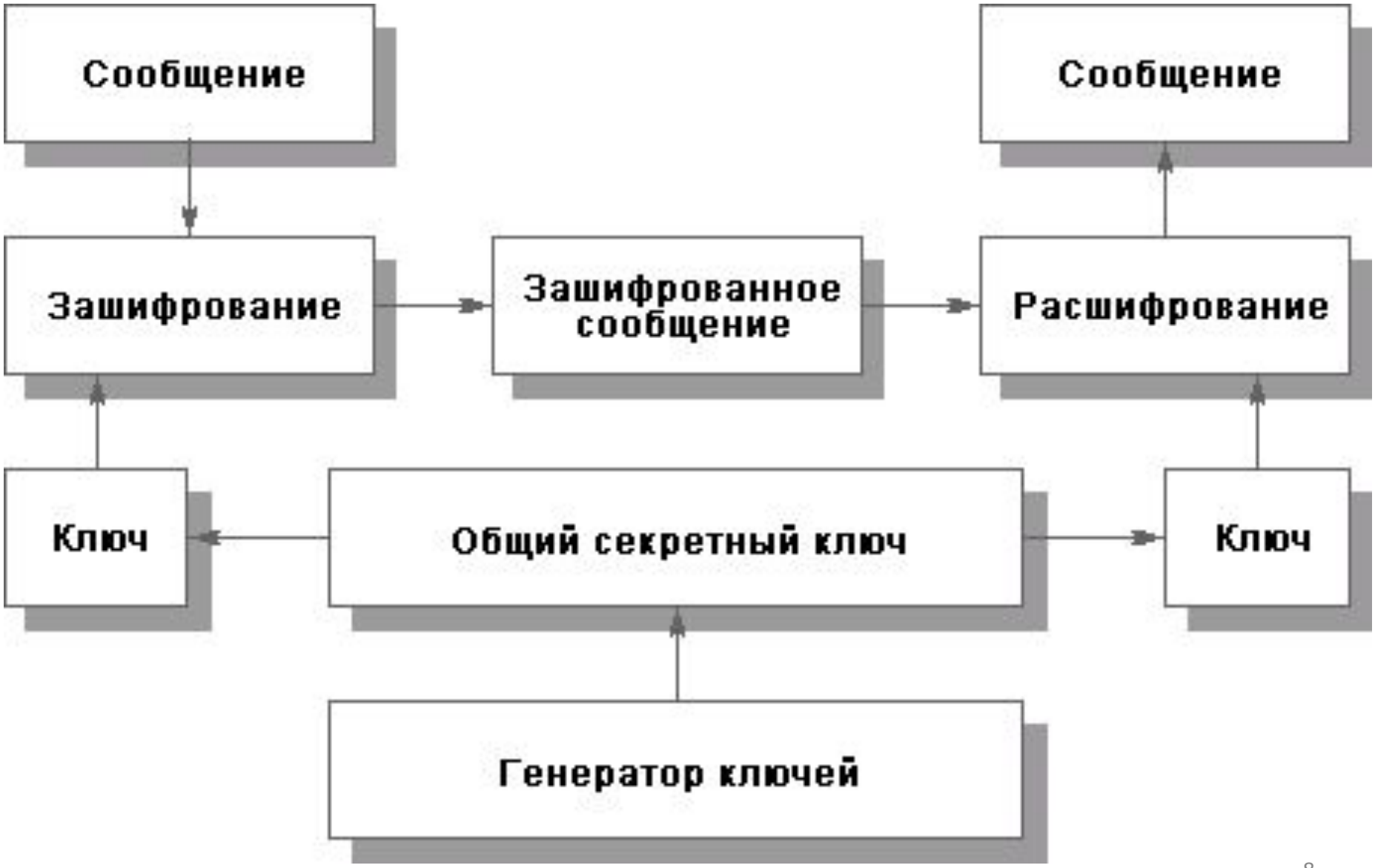


Классификация шифров по объему информации, неизвестной третьей стороне

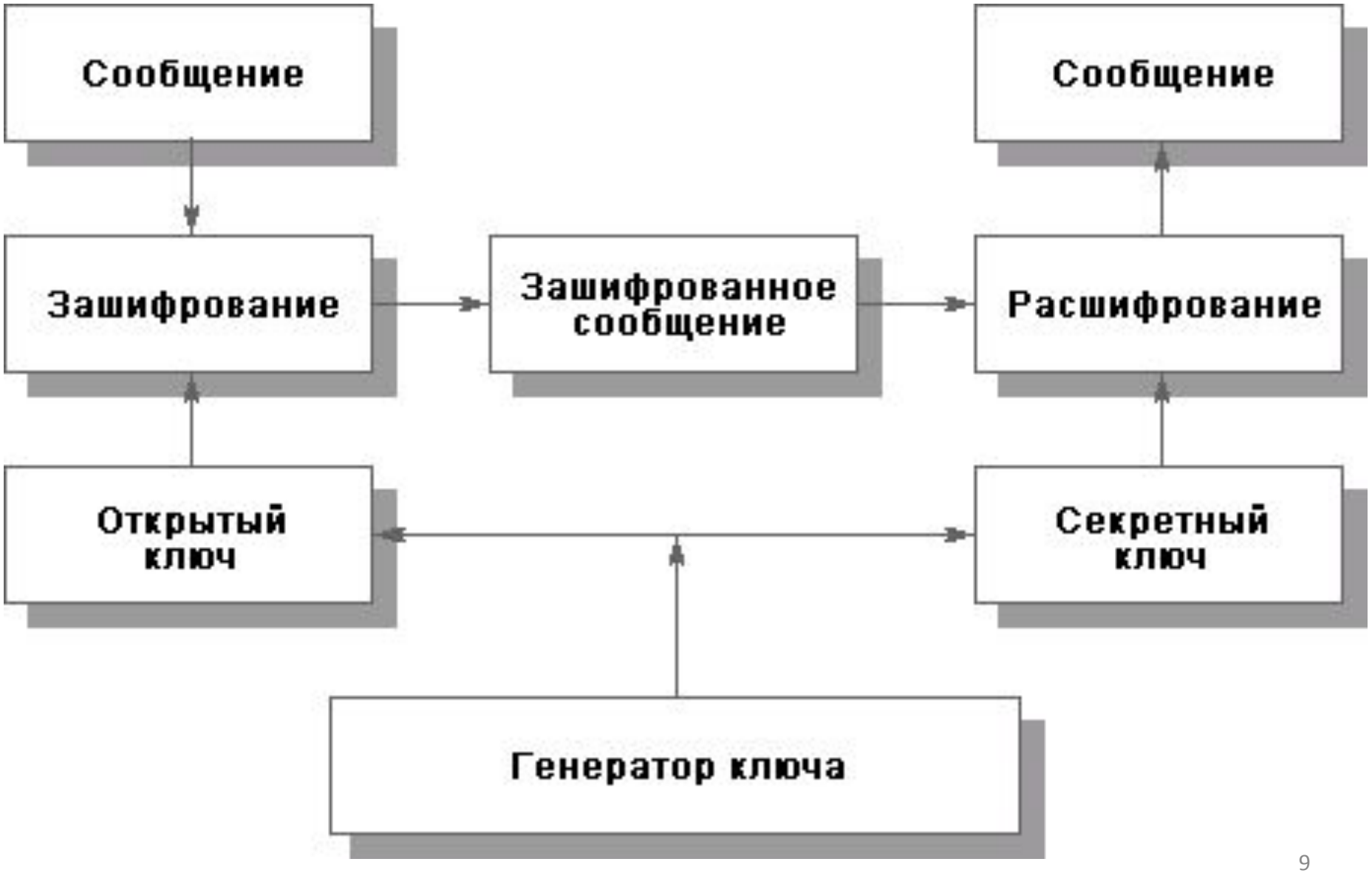
Если нарушителю полностью неизвестен алгоритм выполненного над сообщением преобразования, шифр называется **тайнописью**.

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.

Симметричные методы шифрования



Асимметричные методы шифрования



2. Симметричные алгоритмы шифрования

Классификация симметричных шифров по схеме обработки потока информации

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

Однако побитовая обработка информации является неэффективна в тех случаях, когда вычислительная техника имеет возможности для параллельной обработки. В этих условиях выгоднее применять блочные шифры.

Блочные шифры (block ciphers) могут применяться только над информацией строго определенного объема. Размер блока как правило равен 64, 128 или 256 битам. Шифрование (блоков произвольного размера) невозможно.

Блочные шифры

- шифры замены (подстановки);
- шифры перестановки;
- комбинированные шифры.

Шифры замены характеризуются тем, что отдельные части сообщения (буквы, слова, числа и др.) заменяются другими буквами, числами, символами и т.д.

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется **шифром перестановки**.

Типы шифров подстановки

В классической криптографии различают **четыре типа шифра 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. **Полиграммный** шифр подстановки заменяет не один символ, а целую группу.
4. **Многоалфавитный** шифр подстановки состоит из нескольких шифров простой замены.

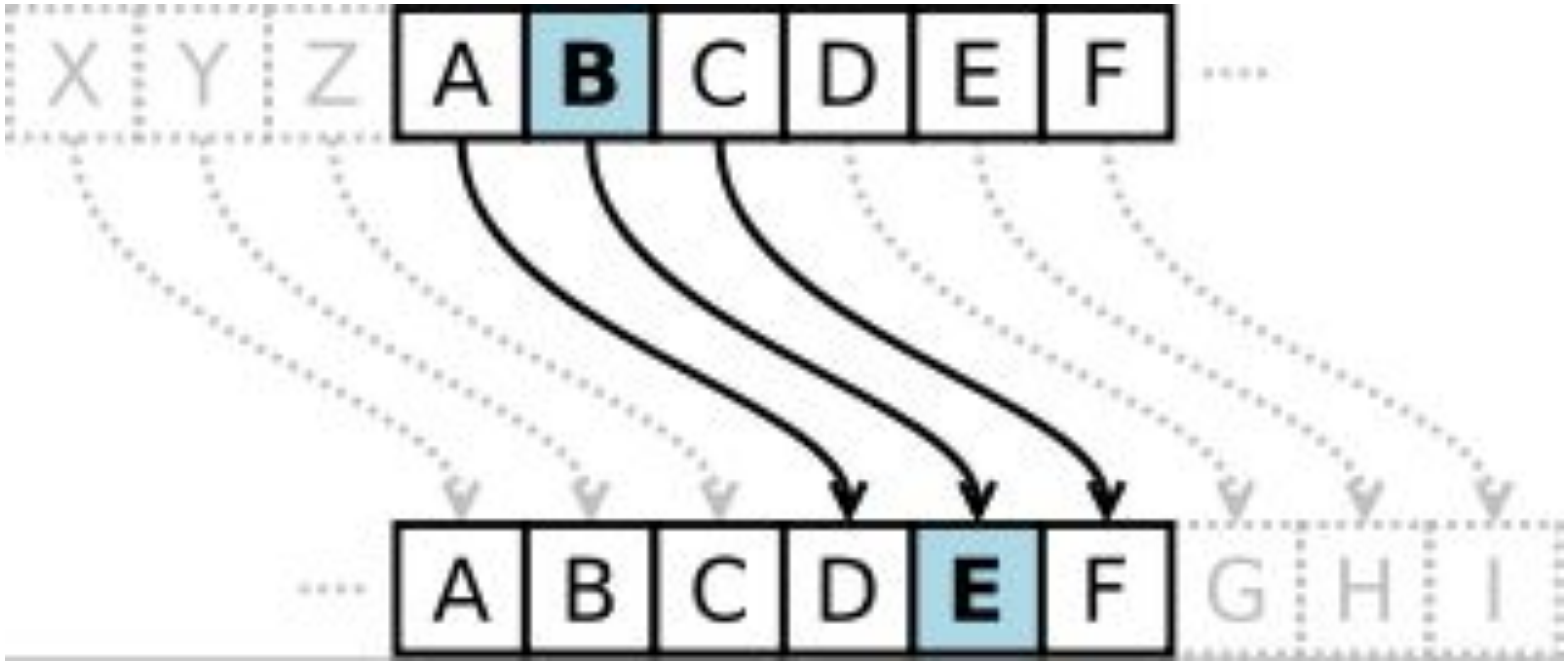
Шифр простой замены

Шифр простой замены (простой подстановочный шифр, моноалфавитный шифр) — класс методов шифрования, которые сводится 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.

Шифр Цезаря – пример шифра простой замены

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. При достижении конца алфавита выполняется циклический переход к его началу. Цезарь использовал шифр замены при смещении К = 3.



Табличный шифр простой замены

A	B	C	D	E	F	Q	H	I	J	К	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

Число всех возможных замен N!, где N – число букв в алфавите. Для латинского алфавита $26! \approx 4 \cdot 10^{26} \approx 2^{218}$.

Русский алфавит

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Р	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

Шифр Гронсфельда

Под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают путем замены буквы сообщения на букву, смещенную по алфавиту на число позиций соответствующее цифре ключа.

Сообщение	В	О	С	Т	О	Ч	Н	Ы	Й	Э	К	С	П	Р	Е	С	С
Ключ	2	7	1	8	2	7	1	8	2	7	1	8	2	7	1	8	2
Шифртекст	Д	Х	Т	Ь	Р	Ю	О	Г	Л	Д	Л	Щ	С	Ч	Ж	Щ	У

Шифр Гронсфельда вскрывается относительно легко, так как в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Шифр сложной замены

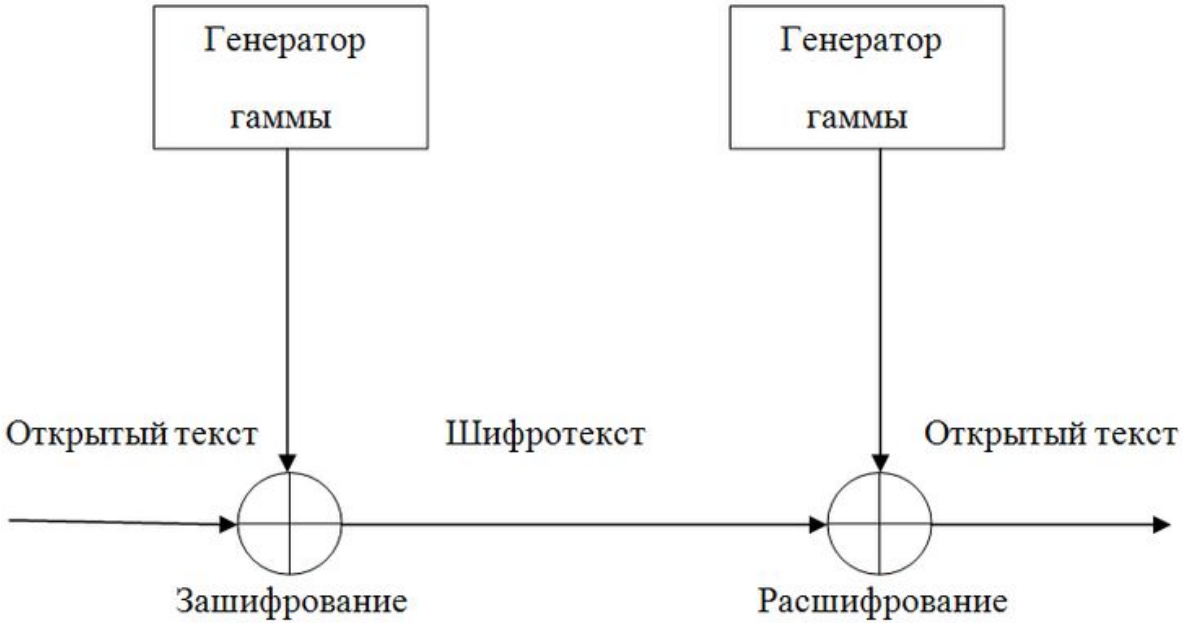
а	б	в	…	я
Ма	Мб	Мв		Мя

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

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

Гаммирование

Гаммирование - класс шифров многоалфавитной замены в которых с помощью секретного ключа k генерируется последовательность символов $g=g_1g_2\ldots g_i\ldots$, эта последовательность называется **гаммой**. При шифровании гамма накладывается на открытый текст $m=m_1m_2\ldots m_i\ldots$, т.е. символы шифртекста получаются из соответствующих символов открытого текста и гаммы с помощью некоторой обратимой операции: $c_i=m_i \cdot g_i$, i=1,2,…
Расшифрование осуществляется применением к символам шифртекста и гаммы обратной операции.



Для зашифрования входной последовательности по этому методу отправитель производит побитовое сложение по модулю 2 ключа k (известный получателю и отправителю) и m-разрядной двоичной последовательности, соответствующей пересылаемому сообщению. Ключ является псевдослучайной последовательностью (гаммой шифра). Таким образом, процессом гаммирования называется процедура наложения на входную информационную последовательность гаммы шифра.

Необходимые и достаточные условия абсолютной стойкости шифра:

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.

Пример Исходный текст: МОДЕЛИ

Гамма: ЦЕЗАРЬ

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Код	01	02	03	04	05	06	07	08	09	10	11	12
Буква	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Код	13	14	15	16	17	18	19	20	21	22	23	24
Буква	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	(пробел)			
Код	25	26	27	28	29	30	31	32	00			

МОДЕЛИ - 13 15 05 06 12 09 ЦЕЗАРЬ - 23 06 08 01 17 29

01101 01111 00101 00110 01100 01001

10111 00110 01000 00001 10001 11101

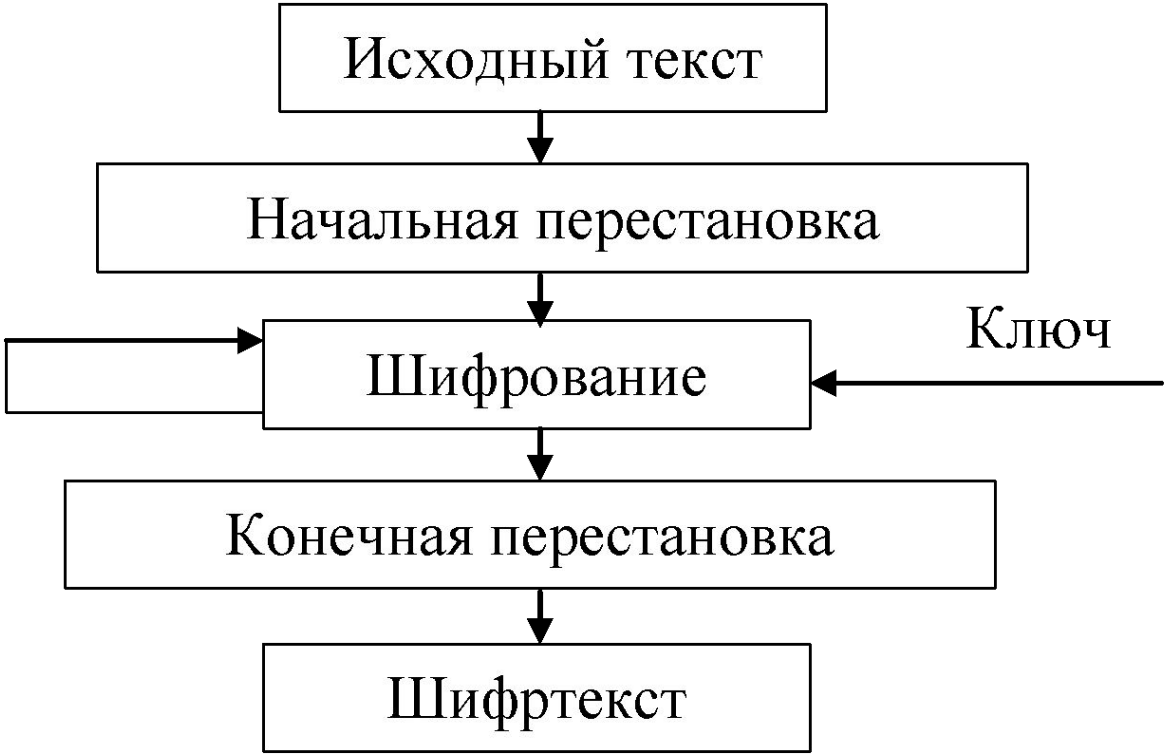
11010 01001 01101 00111 11101 10100

26 09 13 07 29 20

Шифротекст: Щ И М Ж Ь У

Стандарт шифрования DES

Алгоритм DES представляет собой комбинацию двух основных методов шифрования подстановки и перестановки. Основным комбинационным блоком DES является применение к тексту единичной комбинации этих двух методов. Такой блок называется *раундом*. DES включает 16 раундов, то есть одна и та же комбинация методов применяется к открытому тексту 16 раз.



Стандарт шифрования ГОСТ 28147-89

В РФ установлен единый алгоритм криптографического преобразования данных для систем обработки информации в отдельных вычислительных комплексах и сетях ЭВМ. Он определяется положениями ГОСТ 28147-89. Этот алгоритм предназначен для аппаратной и программной реализации, удовлетворяет необходимым требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм реализует шифрование 64-битовых блоков данных с помощью 256-битового ключа, состоящего из восьми 32-битовых подключей. На каждом i-м раунде из 32 используется K_i-й подключ.

ГОСТ может применяться в следующих рабочих режимах: простая замена; гаммирование; гаммирование с обратной связью; выработка имитовставки.

3. Требования к системам симметричного шифрования

Виды атак

- атака со знанием только шифротекста — вид атаки, при которой криптоаналитику известен один или несколько шифротекстов, зашифрованных с использованием одной и той же системы шифрования, с одним и тем же ключом.
- атака со знанием открытого текста — вид атаки, при которой аналитику известны фрагменты открытого текста и информация о том, какие фрагменты шифротекста им соответствуют.
- атака с выбранным открытым текстом — вид атаки, при которой криптоаналитик не только знает открытый текст и шифротекст, но и может для произвольного открытого текста получать соответствующий ему шифротекст.
- адаптивная атака с выбранным открытым текстом — разновидность атаки с выбранным открытым текстом. В этом случае криптоаналитик не только выбирает открытые тексты, но и может изменить свой выбор после анализа полученных данных.
- атака с выбранным шифротекстом — вид атаки, при которой аналитик выбирает шифротекст и может получить соответствующий ему открытый текст.

Требования:

1. Стойкость шифра должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи полного перебора ключей и должно либо выходить за пределы возможностей современных компьютеров (с учетом возможности организации сетевых вычислений) или требовать создания и использования дорогих вычислительных систем;
2. Криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа;
3. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
4. Шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных;
5. Незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;
6. Структурные элементы алгоритма шифрования должны быть неизменными;

7. Шифртекст не должен существенно превосходить по объему исходную информацию; дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

8. Ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

9. Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

10. Любой ключ из множества возможных должен обеспечивать равную криптостойкость (обеспечение линейного (однородного) пространства ключей);

11. Время шифрования не должно быть большим;

12. Стоимость шифрования должна быть согласована со стоимостью закрываемой информации.