

Тема 4

Криптографические методы
защиты информации в
телекоммуникационных системах

Содержание темы

- Классификация криптографических методов защиты информации.
- Архивация и кодирование информации.
- Шифрование информации.
- Симметричные методы шифрования в телекоммуникационных системах.
- Алгоритмы DES и AES.
- Режимы шифрования.

Содержание темы

- Асимметричные методы шифрования в телекоммуникационных системах.
- Алгоритмы RSA и Эль-Гамала.
- Цифровая подпись.
- Хеш-функции.
- Управление криптографическими ключами: генерация, хранение и распределение ключей.
- Стеганография.

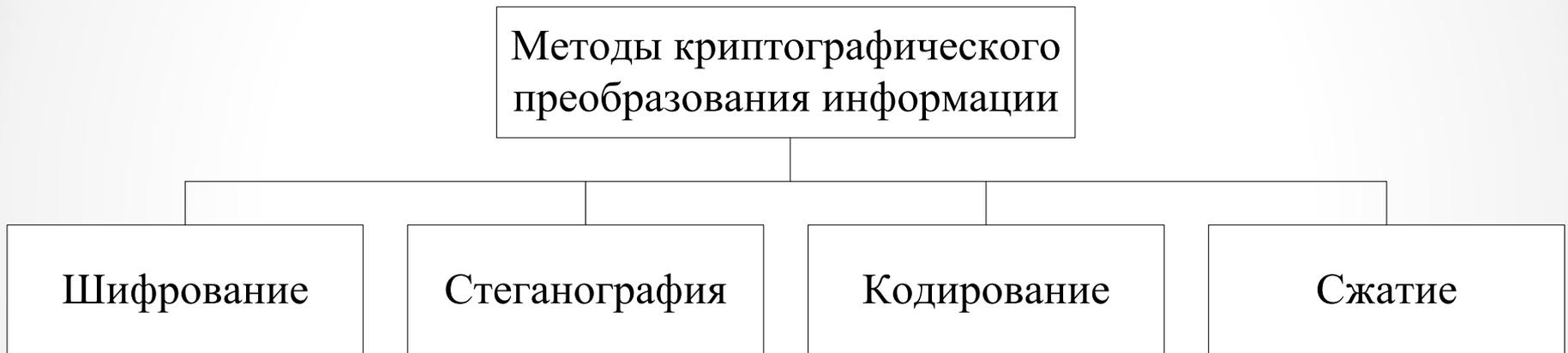
Криптография

Наукой, изучающей математические методы защиты информации путем ее преобразования, является **криптология** [κρυπτοζ – тайный, λογοζ – наука (слово) (греч.)].

Криптология разделяется на два направления – криптографию и криптоанализ.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Криптография



Сжатие (архивация) информации

Целью сжатия является **сокращение объема информации**.

Сжатая информация не может быть прочитана или использована без обратного ее преобразования.

Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как **надежные** средства криптографического преобразования информации.

Кодирование информации

Такой вид криптографического преобразования применим, например, в командных линиях автоматизированных систем управления.

Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Шифрование информации

Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную (шифротекст) или процесс обратного преобразования зашифрованной информации в открытую.



Шифрование информации

Для шифрования информации используются **алгоритм преобразования** и **ключ**.

Как правило, алгоритм для определенного метода шифрования является **неизменным**.

Исходными данными для алгоритма шифрования служат **информация**, подлежащая шифрованию, и **ключ шифрования**.

Шифрование информации

Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую в соответствии с алгоритмом шифрования.

Атака на шифр (криптоанализ) – это процесс дешифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Процесс восстановления первоначального открытого текста на основе зашифрованного без знания ключа называют дешифрованием.

Шифрование информации

Современные методы шифрования должны отвечать следующим **требованиям**:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифротекст не должен существенно превосходить по объему исходную информацию;

Шифрование информации

Современные методы шифрования должны отвечать следующим **требованиям**:

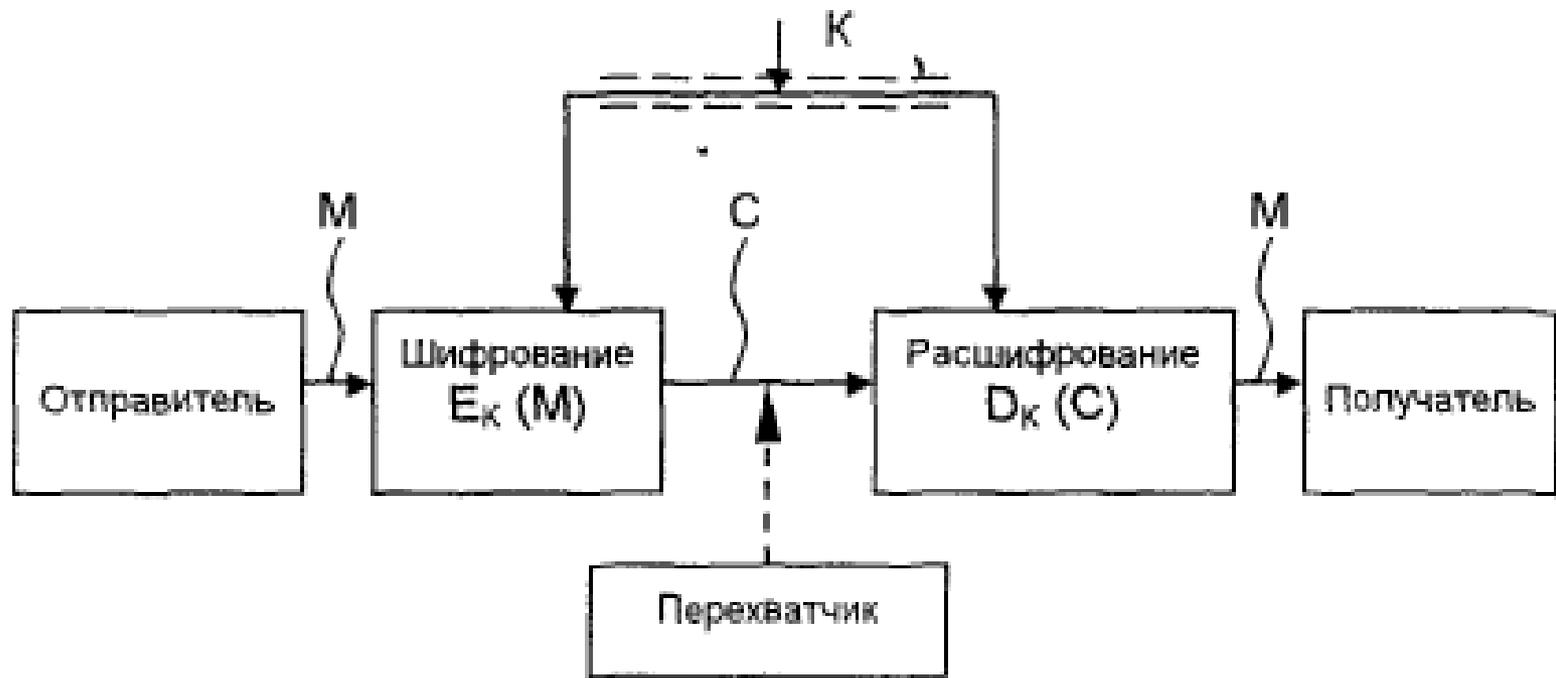
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Симметричные криптосистемы

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ.

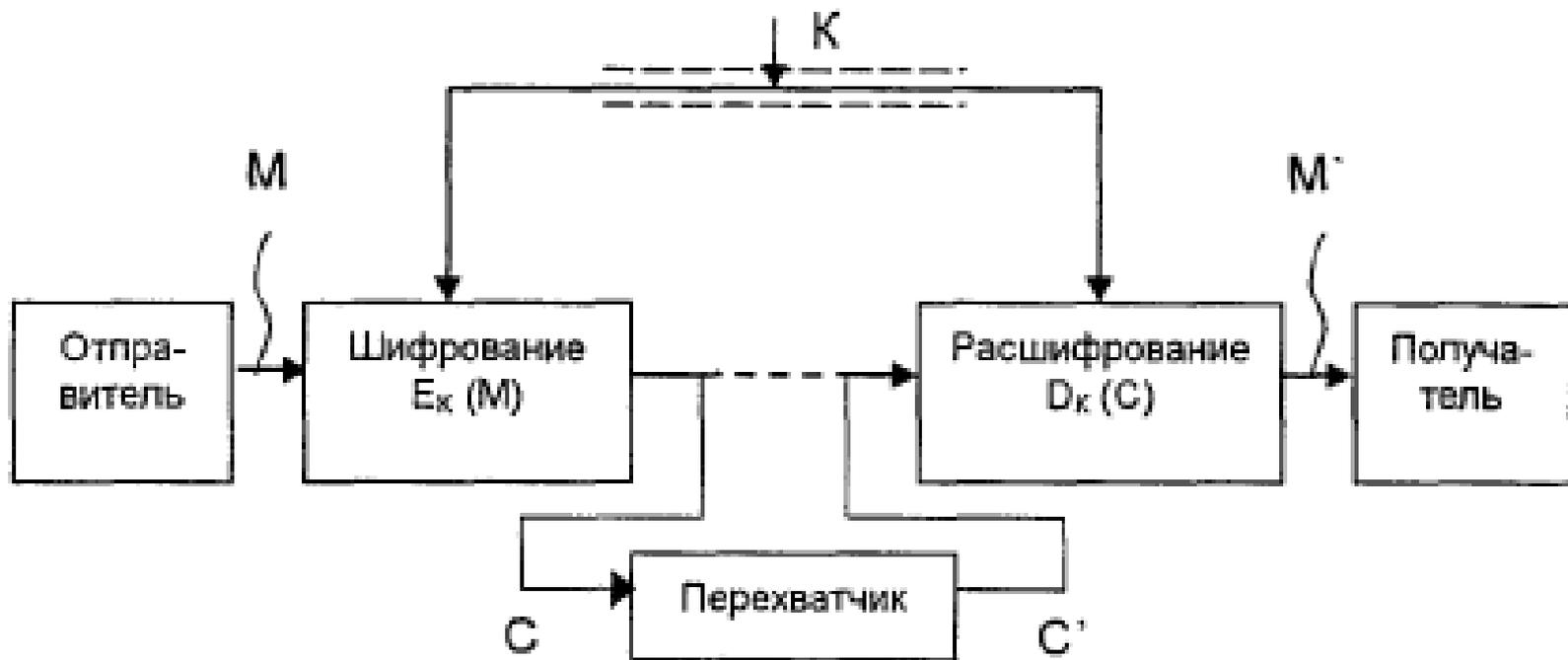


Симметричные криптосистемы



Симметричные криптосистемы

Активный перехватчик



Симметричные криптосистемы

К **традиционным (классическим)** методам шифрования относятся:

- шифры перестановки;
- шифры простой и сложной замены;
- некоторые их модификации и комбинации.

Комбинации шифров перестановок и шифров замены образуют все многообразие применяемых на практике симметричных шифров.

Симметричные криптосистемы

Шифры перестановки.

При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста.

Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами.

Пример: *шифрующие таблицы.*

В	У	Г	Р	Н	В	Е	С
Б	С	О	С	Ы	Е	Т	П
Е	С	С	Т	Й	Р	Т	О
Л	К	У	В	У	С	Р	Р
О	И	Д	Е	Н	И	А	Т
Р	Й	А	Н	И	Т	Н	А

Симметричные криптосистемы

Шифры простой замены.

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены.

В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита по одному правилу на всем протяжении текста.

Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Симметричные криптосистемы

Примеры шифров простой замены:

- Система шифрования Цезаря;

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

- Аффинная система подстановок Цезаря.

A	t	3t+5	B	A	t	3t+5	B	A	t	3t+5	B
A	0	5	F	J	9	6	G	S	18	7	H
B	1	8	I	K	10	9	J	T	19	10	K
C	2	11	L	L	11	12	M	U	20	13	N
D	3	14	O	M	12	15	P	V	21	16	Q
E	4	17	R	N	13	18	S	W	22	19	T
F	5	20	U	O	14	21	V	X	23	22	W
G	6	23	X	P	15	24	Y	Y	24	25	Z
H	7	0	A	Q	16	1	B	Z	25	2	C
I	8	3	D	R	17	4	E				

Симметричные криптосистемы

Шифры сложной замены.

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

Примеры:

- Система шифрования Вижинера
- Диски Альберти, Джефферсона;
- Одноразовые шифры.

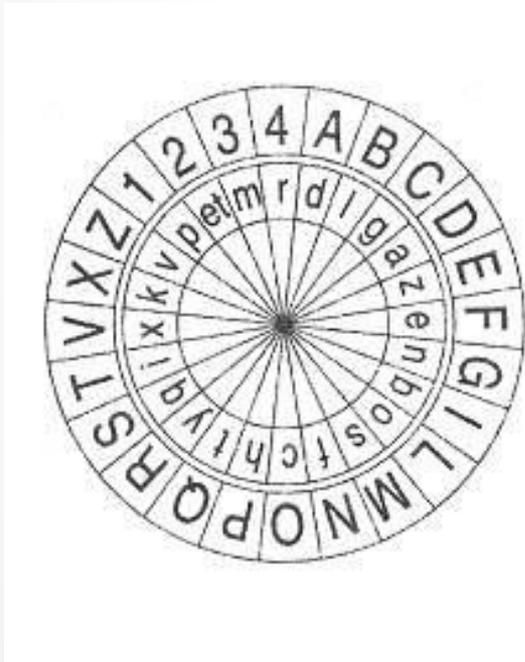
Симметричные криптосистемы

Система
шифрования
Вижинера

Ключ	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z
0	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z
1	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а
2	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б
3	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с
4	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д
5	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е
6	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф
7	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г
8	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х
9	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и
10	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й
11	л	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к
12	м	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л
13	н	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м
14	о	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н
15	п	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о
16	q	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п
17	р	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q
18	с	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р
19	т	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с
20	у	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т
21	в	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у
22	w	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в
23	х	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w
24	у	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х
25	z	а	б	с	д	е	ф	г	х	и	й	к	л	м	н	о	п	q	р	с	т	у	в	w	х	у

Симметричные криптосистемы

Диски Альберти, Джефферсона

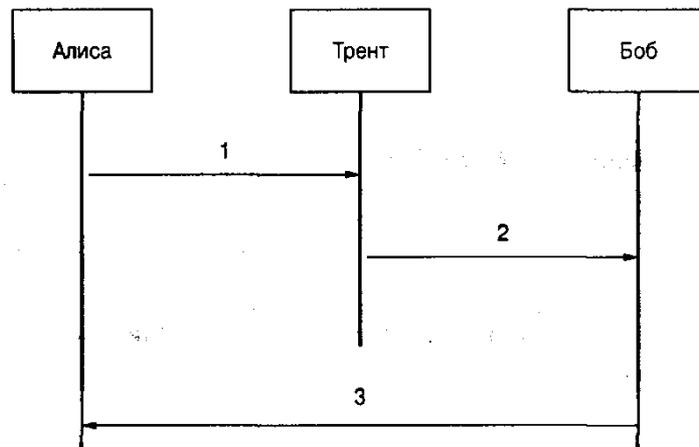


Симметричные криптосистемы

ИСХОДНЫЕ УСЛОВИЯ:

Алиса и Трент имеют общий ключ K_{AT} ; Боб и Трент имеют общий ключ K_{BT} .

ЦЕЛЬ: Алиса и Боб желают создать новый общий секретный ключ K .



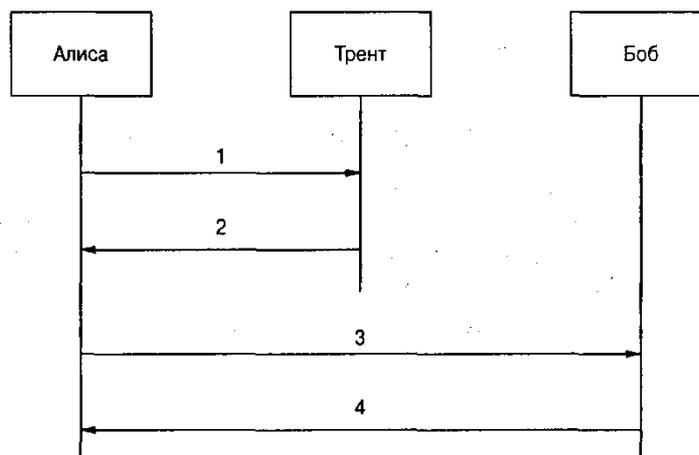
1. Алиса генерирует случайный ключ K , создает сообщение $\{K\}_{K_{AT}}$ и посылает Тренту следующую информацию: *Алиса, Боб, $\{K\}_{K_{AT}}$* .
2. Трент находит в базе данных ключи K_{AT} и K_{BT} , восстанавливает ключ K , создает сообщение $\{K\}_{K_{BT}}$ и посылает Бобу следующую информацию: *Алиса, Боб, $\{K\}_{K_{BT}}$* .
3. Боб расшифровывает сообщение $\{K\}_{K_{BT}}$, восстанавливает ключ K и посылает Алисе сообщение *{Привет, Алиса, я – Боб!} $\}_K$* .

Симметричные криптосистемы

ИСХОДНЫЕ УСЛОВИЯ:

Алиса и Трент имеют общий ключ K_{AT} ; Боб и Трент имеют общий ключ K_{BT} .

ЦЕЛЬ: Алиса и Боб желают установить новый общий секретный ключ K .



1. Алиса посылает Тренту сообщение: *Алиса, Боб*.
2. Трент находит в базе данных ключи K_{AT} и K_{BT} , генерирует случайный ключ K и посылает Алисе следующую информацию: $\{K\}_{K_{AT}}, \{K\}_{K_{BT}}$.
3. Алиса расшифровывает сообщение $\{K\}_{K_{AT}}$ и посылает Бобу информацию: *Трент, Алиса, $\{K\}_{K_{BT}}$* .
4. Боб расшифровывает сообщение $\{K\}_{K_{BT}}$, восстанавливает ключ K и посылает Алисе сообщение *{Привет, Алиса, я – Боб!} $_K$* .

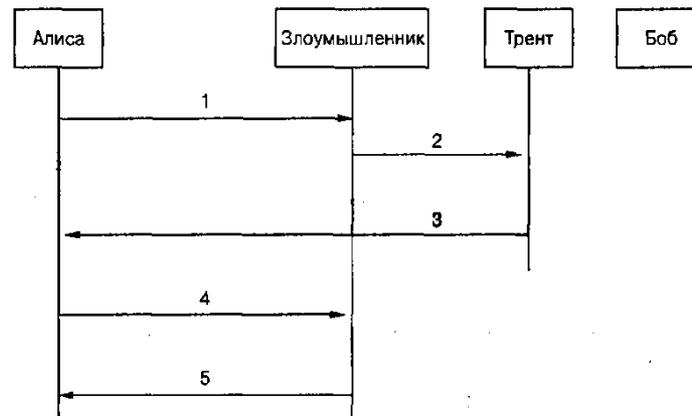
Симметричные криптосистемы

ИСХОДНЫЕ УСЛОВИЯ:

В дополнение к протоколу “Сеансовый ключ от Трента” Злоумышленник и Трент имеют общий ключ K_{MT} .

РЕЗУЛЬТАТ АТАКИ:

Алиса думает, что имеет общий ключ с Бобом, а на самом деле она делит ключ со Злоумышленником.



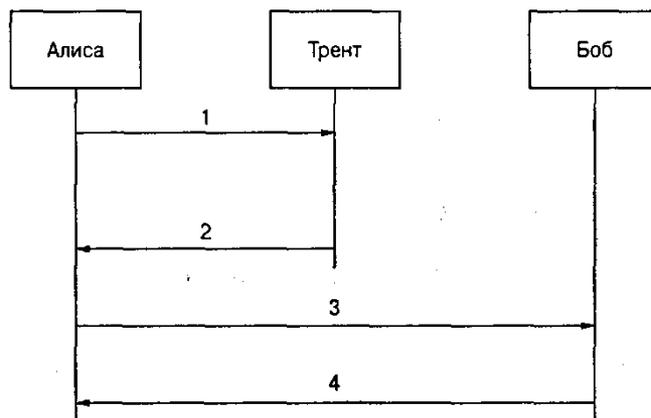
1. Алиса – Злоумышленнику (“Тренту”): *Алиса, Боб.*
2. Злоумышленник (“Алиса”) – Тренту: *Алиса, Злоумышленник.*
3. Трент находит в базе данных ключи K_{AT} и K_{MT} , генерирует случайный ключ K_{AM} и посылает Алисе следующую информацию: $\{K_{AM}\}_{K_{AT}}$, $\{K_{AM}\}_{K_{MT}}$.
4. Алиса расшифровывает сообщение $\{K_{AM}\}_{K_{AT}}$ и посылает Бобу информацию: *Трент, Алиса, $\{K_{AM}\}_{K_{MT}}$.*
5. Злоумышленник (“Боб”) – Алисе: $\{Привет, Алиса, я – Боб!\}_{K_{AM}}$.

Симметричные криптосистемы

ИСХОДНЫЕ УСЛОВИЯ:

Алиса и Трент имеют общий ключ K_{AT} ; Боб и Трент имеют общий ключ K_{BT} .

ЦЕЛЬ: Алиса и Боб желают создать новый общий секретный ключ K .



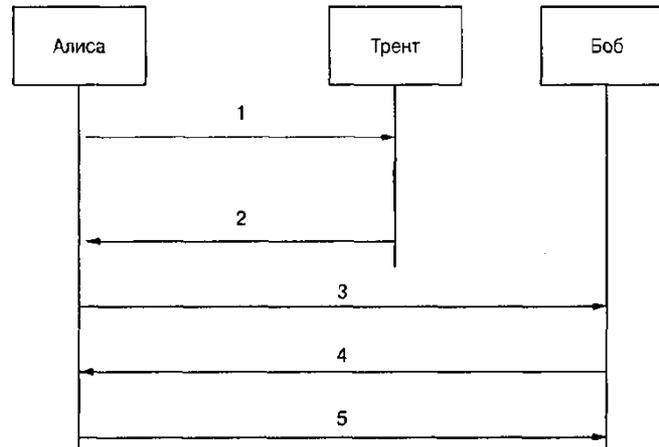
1. Алиса посылает Тренту сообщение: *Алиса, Боб*.
2. Трент находит в базе данных ключи K_{AT} и K_{BT} , генерирует случайный ключ K и посылает Алисе следующую информацию: $\{Боб, K\}_{K_{AT}}$, $\{Алиса, K\}_{K_{BT}}$.
3. Алиса расшифровывает сообщение $\{Боб, K\}_{K_{AT}}$, устанавливает личность Боба и посылает ему информацию: *Трент, $\{Алиса, K\}_{K_{BT}}$* .
4. Боб расшифровывает сообщение $\{Алиса, K\}_{K_{BT}}$, устанавливает личность Алисы и посылает Алисе сообщение $\{Привет, Алиса, я — Боб!\}_K$.

Симметричные криптосистемы

ИСХОДНЫЕ УСЛОВИЯ:

Алиса и Трент имеют общий ключ K_{AT} ; Боб и Трент имеют общий ключ K_{BT} .

ЦЕЛЬ: Алиса и Боб желают создать новый общий секретный ключ K .

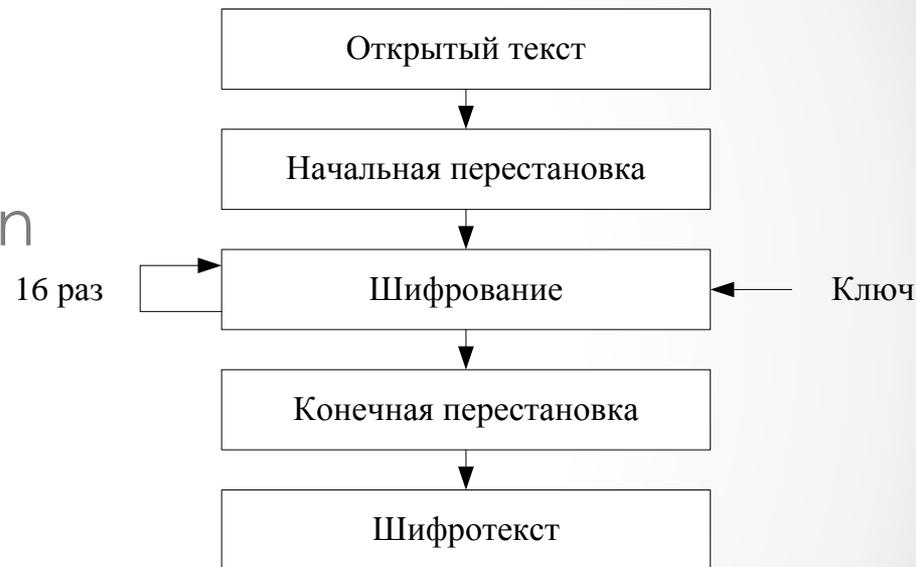


1. Алиса генерирует случайное число N_A и посылает Тренту сообщение: *Алиса, Боб, N_A* .
2. Трент генерирует случайный ключ K и посылает Алисе следующую информацию: $\{N_A, K, \text{Боб}, \{K, \text{Алиса}\}_{K_{BT}}\}_{K_{AT}}$.
3. Алиса расшифровывает сообщение $\{N_A, K, \text{Боб}, \{K, \text{Алиса}\}_{K_{BT}}\}_{K_{AT}}$, проверяет число N_A , устанавливает личность Боба и посылает ему информацию: *Трент, $\{K, \text{Алиса}\}_{K_{BT}}$* .
4. Боб расшифровывает сообщение, устанавливает личность Алисы и посылает ей сообщение $\{\text{Привет, Алиса, я — Боб!}, N_B\}_K$.
5. Алиса посылает Бобу сообщение: $\{\text{Я — Алиса! } N_B - 1\}_K$.

DES

Американский стандарт шифрования данных DES.

Стандарт шифрования данных DES (Data Encryption Standard) опубликован в 1977 г. Национальным бюро стандартов США.



Предназначен для защиты от несанкционированного доступа к **важной, но не секретной** информации в государственных и коммерческих организациях США.

DES

Чтобы воспользоваться алгоритмом **DES** для решения разнообразных криптографических задач, разработаны четыре рабочих режима:

- электронная кодовая книга **ECB (Electronic Code Book)**;
- сцепление блоков шифра **CBC (Cipher Block Chaining)**;
- обратная связь по шифротексту **CFB (Cipher Feed Back)**;
- обратная связь по выходу **OFB (Output Feed Back)**.

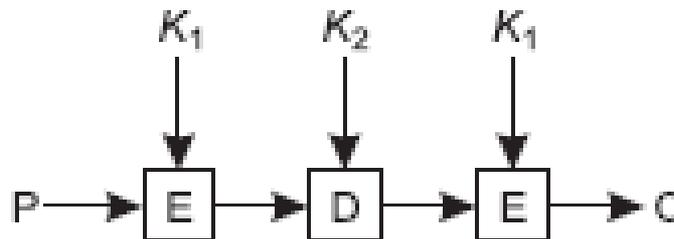
Triple DES

Уже в 1979 году корпорация IBM поняла, что ключ стандарта DES слишком короток.

В тройном DES используются два ключа и три этапа. На первом этапе открытый текст зашифровывается (блок E на рисунке) обычным DES ключом K_1 .

На втором этапе DES работает в режиме дешифрации (блок D), используя ключ K_2 .

На третьем этапе выполняется еще одна операция шифрования с ключом K_1 .



ГОСТ 28147-89

Стандарт шифрования данных (ГОСТ 28147-89).

Алгоритм криптографического преобразования данных был разработан в СССР и опубликован в виде государственного стандарта ГОСТ 28147-89 в 1989 году.

Предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и **не накладывает ограничений на степень секретности защищаемой информации.**

Алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с **256-битовым КЛЮЧОМ.**

ГОСТ 28147-89

Алгоритм предусматривает четыре режима работы:

- шифрование данных в режиме **простой замены**;
- шифрование данных в режиме **гаммирования**;
- шифрование данных в режиме **гаммирования с обратной связью**;
- **выработка имитовставки.**

Симметричные криптосистемы

Современные симметричные криптосистемы:

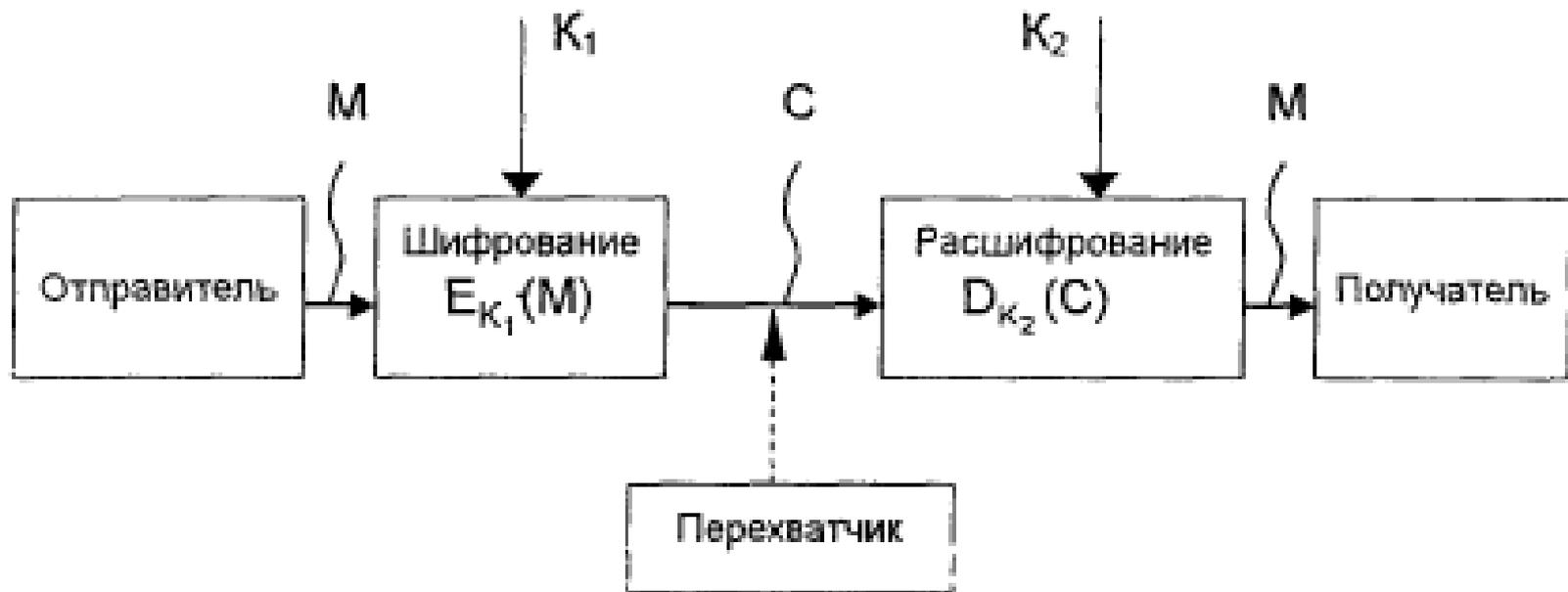
- **TEA** (1994);
- **Twofish** (1998);
- **IDEA** (2000);
- **AES** (2002) и т. п.

Асимметричные криптосистемы

В **асимметричных криптосистемах** используются два ключа – открытый и секретный, которые математически связаны друг с другом



Асимметричные криптосистемы



Асимметричные криптосистемы

Современные асимметричные криптосистемы:

- **RSA** (1977);
- **Эль-Гамала** (1985) и т. п.

Методы шифрования с открытым ключом достаточно трудоемки и в настоящее время не пригодны для поточного шифрования передаваемой информации с большими скоростями.

В основном они применяются для распространения симметричных ключей и генерации электронных цифровых подписей.

Асимметричные криптосистемы

ОБЩИЕ ИСХОДНЫЕ ДАННЫЕ:

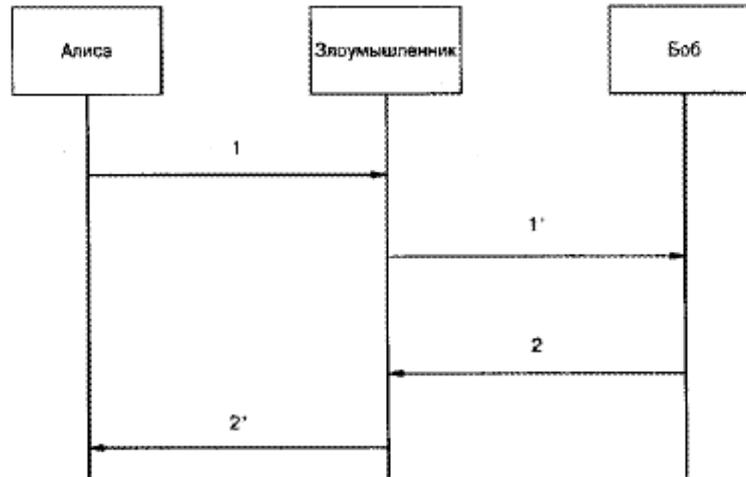
(p, g) : p — большое простое число,
 g — порождающий элемент группы \mathbb{F}_p^* .

РЕЗУЛЬТАТ:

Элемент группы \mathbb{F}_p^* , разделенный между Алисой и Бобом.

1. Алиса генерирует элемент $a \in U[1, p - 1)$, вычисляет число $g_a \leftarrow g^a \pmod{p}$ и посылает его Бобу.
2. Боб генерирует элемент $b \in U[1, p - 1)$, вычисляет число $g_b \leftarrow g^b \pmod{p}$ и посылает его Алисе.
3. Алиса вычисляет значение $k \leftarrow g_b^a \pmod{p}$.
4. Боб вычисляет число $k \leftarrow g_a^b \pmod{p}$.

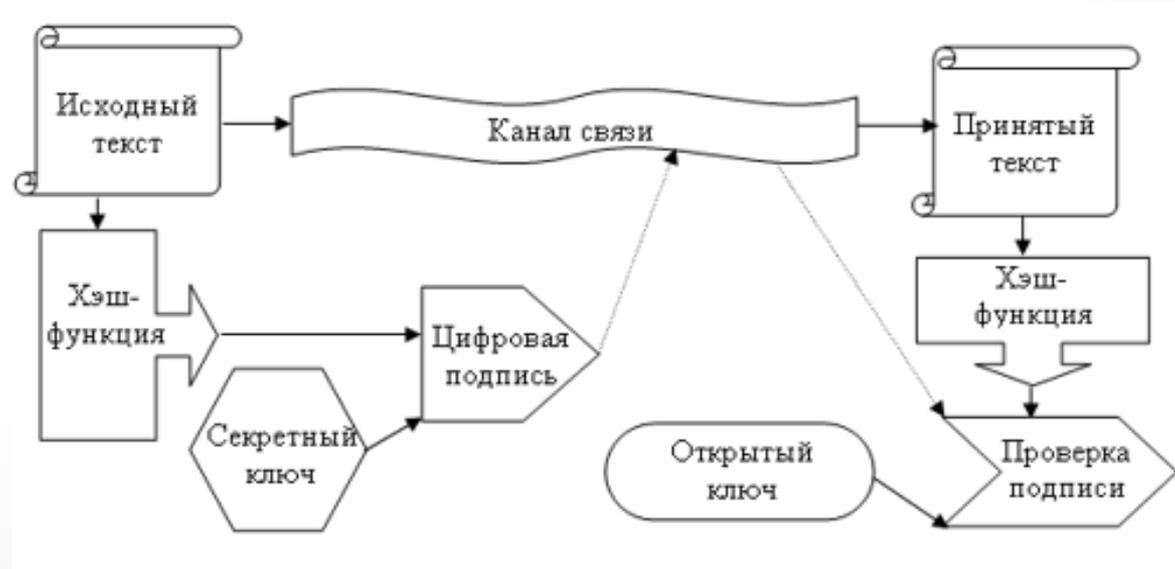
Асимметричные криптосистемы



1. Алиса генерирует элемент $a \in U[1, p-1]$, вычисляет значение $g_a \leftarrow g^a \pmod{p}$ и посылает его Злоумышленнику ("Бобу").
- 1'. Злоумышленник ("Боб") вычисляет значение $g_m \leftarrow g^m \pmod{p}$, где $m \in [1, p-1]$ и посылает его Бобу
2. Боб генерирует элемент $b \in U[1, p-1]$, вычисляет значение $g_b \leftarrow g^b \pmod{p}$ и посылает его Злоумышленнику ("Алисе").
- 2'. Злоумышленник ("Алиса") посылает Алисе число g_m .
3. Алиса вычисляет значение $k_1 \leftarrow g_m^b \pmod{p}$. (* Этот ключ распределен между Алисой и Злоумышленником, поскольку Злоумышленник может вычислить значение $k_1 \leftarrow g_a^b \pmod{p}$. *)
4. Боб вычисляет значение $k_2 \leftarrow g_m^a \pmod{p}$. (* Этот ключ распределен между Бобом и Злоумышленником, поскольку Злоумышленник может вычислить значение $k_2 \leftarrow g_b^a \pmod{p}$. *)

Электронная цифровая ПОДПИСЬ

Электронной цифровой подписью (ЭЦП) называется присоединение к тексту его криптографического преобразования, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.



Электронная цифровая ПОДПИСЬ

Электронной цифровой подписью предназначена для предотвращения следующих атак:

- **активный перехват** (нарушитель, подключившись к сети, перехватывает передаваемую информацию) – возможна также **подмена** и **повтор** ранее передаваемой информации;
- **маскарад** (передача информации от чужого имени);
- **рenegатство** (отказ от авторства информации).

Электронная цифровая ПОДПИСЬ

ЭЦП содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа;
- информацию о лице, поставившем подпись;
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.



Электронная цифровая ПОДПИСЬ

<i>Собственноручная подпись</i>	<i>Цифровая подпись</i>
не зависит от подписываемого текста, всегда одинакова	зависит от подписываемого текста, практически всегда разная
неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	определяется секретным ключом, принадлежащим подписывающему лицу, может быть утеряна владельцем
неотделима от носителя (бумаги), поэтому отдельно подписывается каждый экземпляр документа	легко отделима от документа, поэтому верна для всех его копий
не требует для реализации дополнительных механизмов	требует дополнительных механизмов, реализующих алгоритмы ее вычисления и проверки
не требует создания поддерживающей инфраструктуры	требует создания доверенной инфраструктуры сертификатов открытых ключей

Управление ключами

Управление ключами – это процесс системы обработки информации, вырабатывающий и распределяющий ключи (открытые и секретные) между пользователями.

Настоящим удостоверяю, что открытый ключ
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
принадлежит
Роберту Джону Смиту
Университетская улица 12345
Беркли, СА 94702
1958 род. 5 июля 1958Кг.
Электронный адрес: bob@superdupernet.com

Хеш SHA-1 данного сертификата подписан закрытым ключом Управления сертификации

Управление ключами включает в себя три элемента:

- **генерацию** ключей;
- **накопление** ключей;
- **распределение** ключей.

Стеганография

Методы **стеганографии** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

В основе всех методов стеганографии лежит **маскирование** закрытой информации среди открытых файлов.

Стеганография



Три зебры и дерево



Три зебры, дерево и полный текст пяти пьес Вильяма Шекспира (*Гамлет, Король Лир, Макбет, Венецианский купец и Юлий Цезарь*)

Стеганография

Демонстрация изменения последних двух бит информации на каждом из *R G B* каналов в программе *Adobe Photoshop*.

RGB – красный (**Red**), зеленый (**Green**), синий (**Blue**).

RGB – ff0000 – 255; 0; 0 – 11111111 00000000 00000000;

RGB – 00ff00 – 0; 255; 0 – 00000000 11111111 00000000;

RGB – 0000ff – 0; 0; 255 – 00000000 00000000 11111111;

RGB – e2c812 – 226; 200; 18 – 11100010 11001000 00010010.