Тема 5

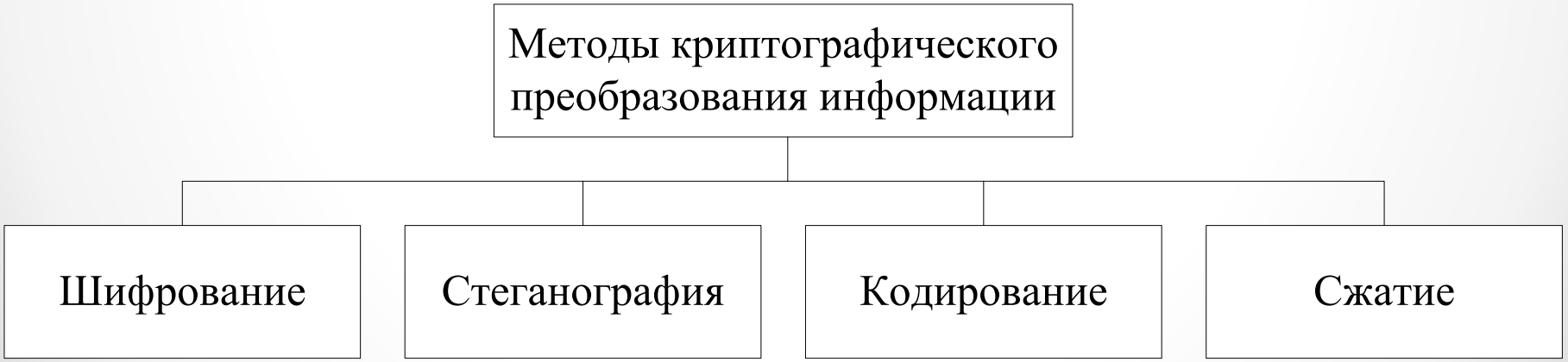
Криптографические методы защиты информации

Содержание темы

- Классификация криптографических методов защиты информации.
- Сжатие (архивация) и кодирование информации.
- Шифрование информации.
- Симметричные и асимметричные криптосистемы.
- Электронная цифровая подпись.
- Хэш-функции.
- Управление криптографическими ключами.
- Стеганография.

Классификация крипто-графических методов

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.



Сжатие (архивация) информации

Целью сжатия является **сокращение объема информации**.

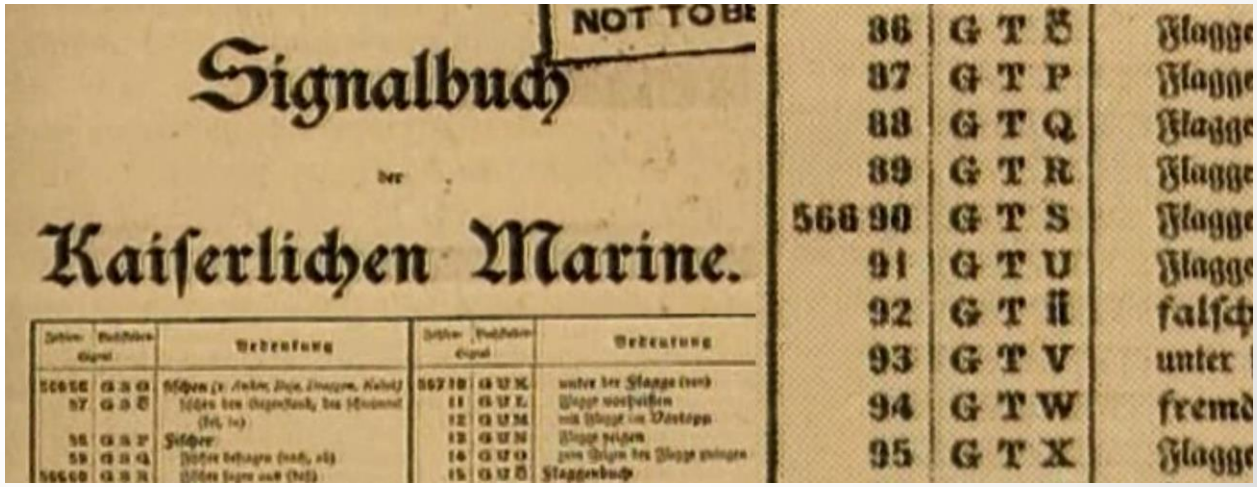
Сжатая информация не может быть прочитана или использована без обратного ее преобразования.

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

Кодирование информации

Содержанием процесса **кодирования информации** является замена смысловых конструкций исходной информации (слов, предложений) кодами.

Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций.



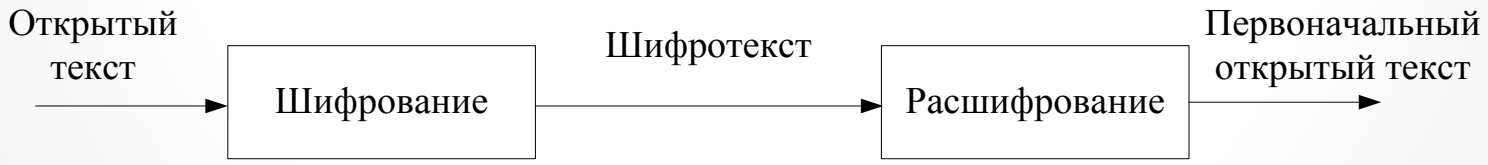
Кодирование информации

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 шифрованного 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

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.*

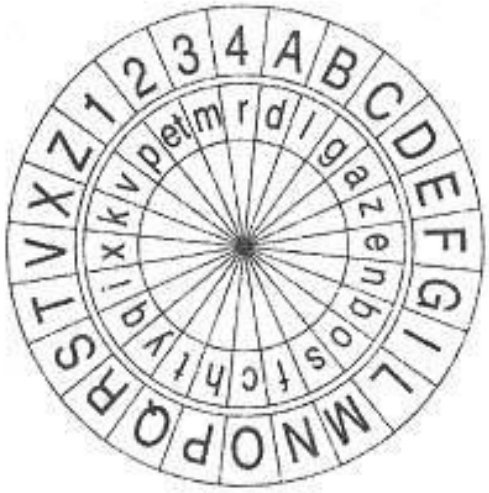
Симметричные криптосистемы

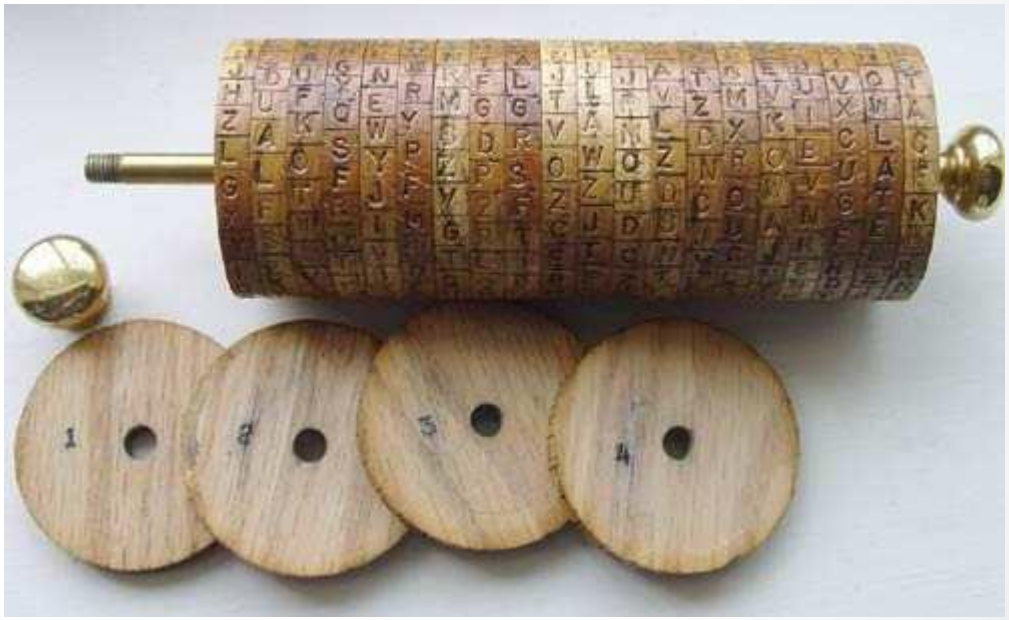
Система шифрования Вижинера

Ключ	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
0	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
1	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	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	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

Симметричные криптосистемы

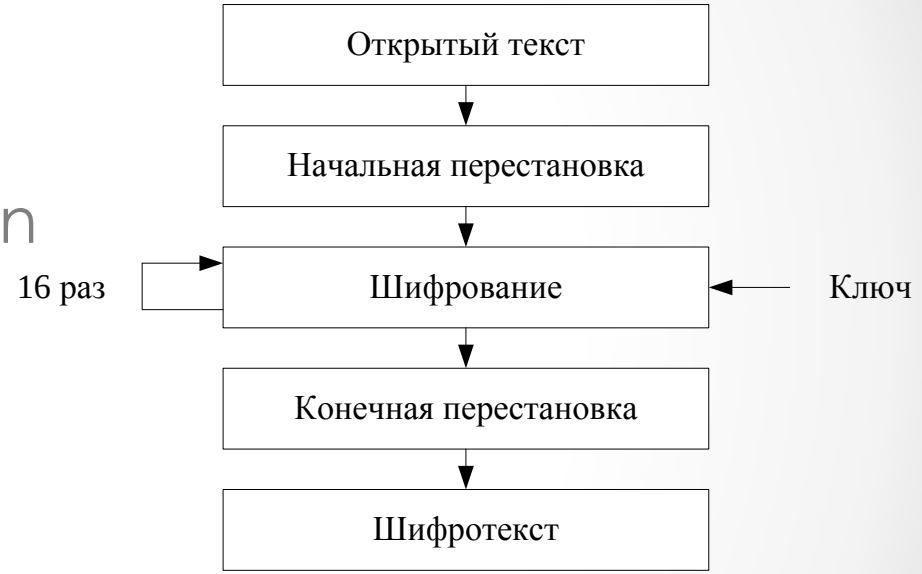
Диски Альберти, Джефферсона





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**).

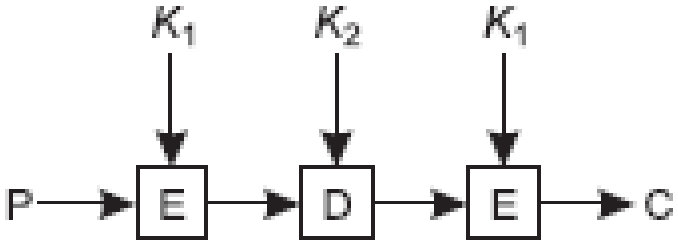
Triple DES

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**.

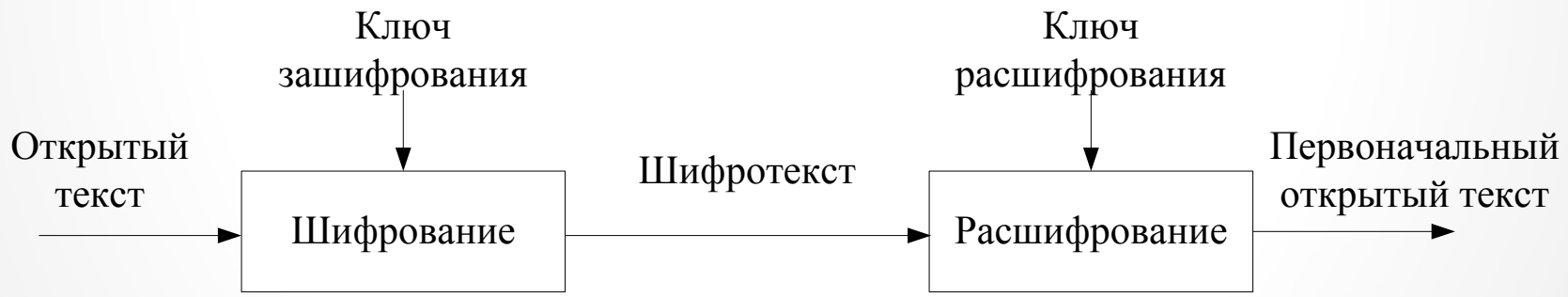
Симметричные криптосистемы

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

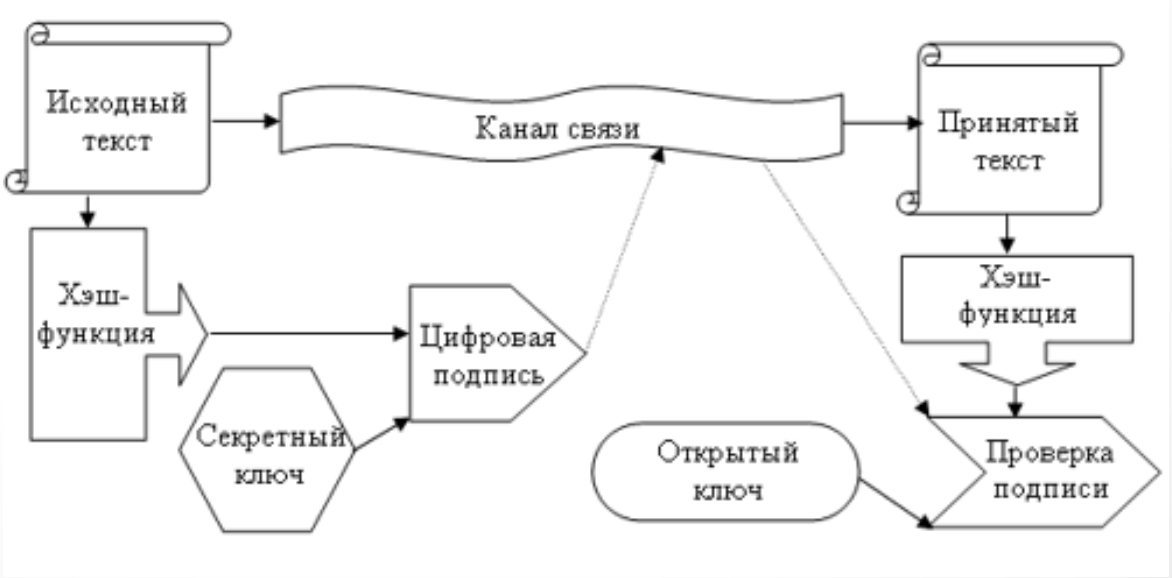
Современные асимметричные криптосистемы:

- RSA (1977);
- Эль-Гамаля (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.

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 цифровая подпись 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);
- **ренегатство** (отказ от авторства информации).

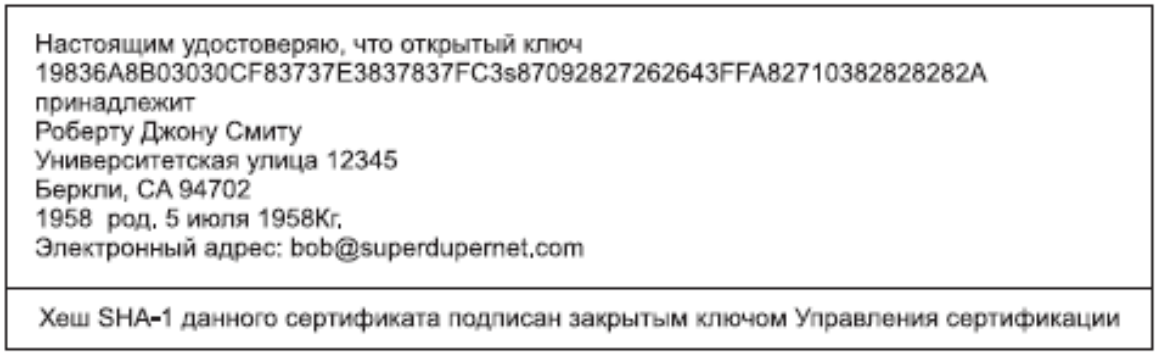
Электронная цифровая подпись

ЭЦП содержит следующую информацию:

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

Управление ключами

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



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.