Основы криптографической защиты информации

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

1. Основные понятия криптографии.

2. Исторические примеры шифрования.

3. Классификация методов криптографического закрытия информации.

ЛИТЕРАТУРА

Основная литература

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В.К. Новиков, С.Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : ЮНИТИ-ДАНА, 2019. – 287 с..

2. Основы информационной безопасности в органах внутренних дел : учеб. пособие / сост. А.Б. Сизоненко, С.Г. Клюев, В.Н. Цимбал. - Краснодар : Краснодарский университет МВД России, 2016. – 122 с..

ЛИТЕРАТУРА

Основная литература

3. Костюченко, К.Л. Основы информационной безопасности в органах внутренних дел : учеб. пособие / К. Л. Костюченко, С. В. Мухачев. – Екатеринбург: Уральский юридический институт МВД России, 2015.

1. Основные понятия криптографии.

Криптология **– наука, изучающая математические методы защиты информации *путем ее преобразования*.**

(kryptos - тайный, logos - наука)

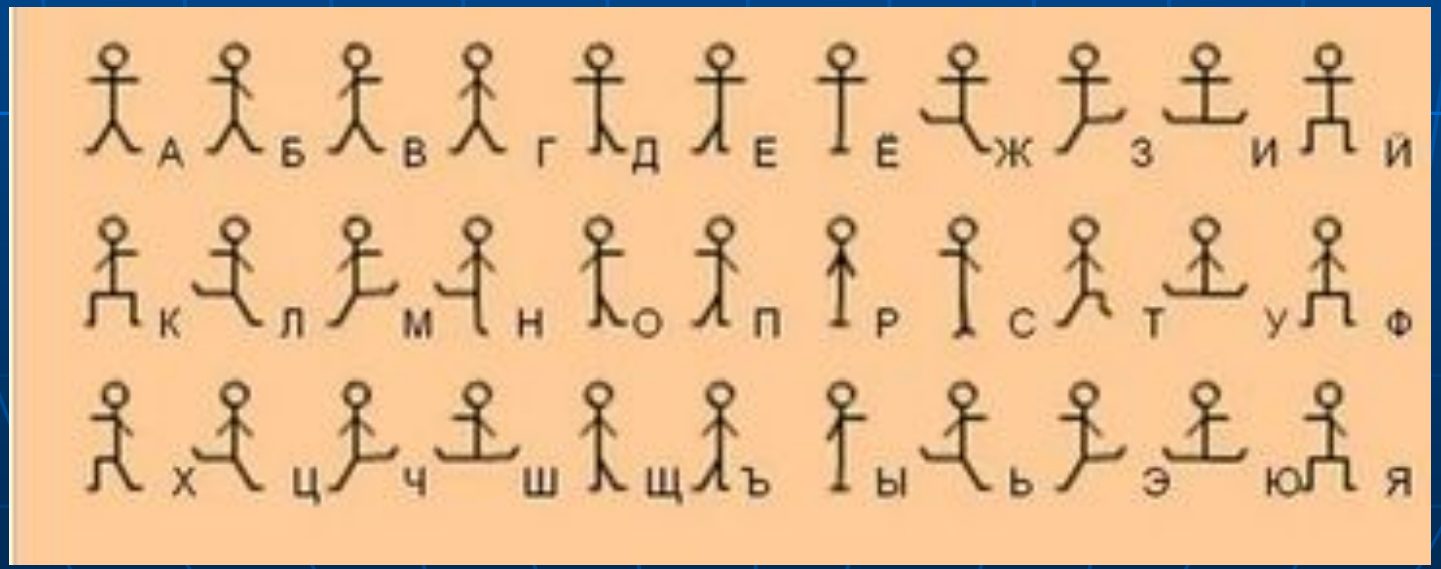
Криптология

Криптография

Криптоанализ

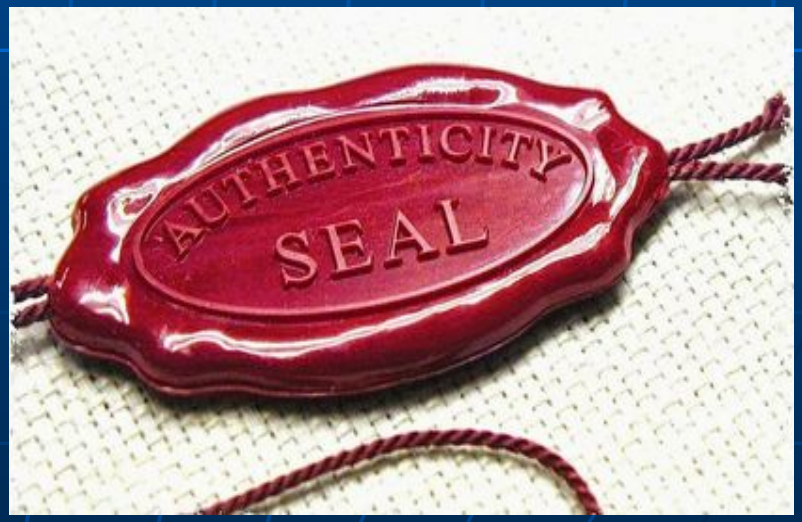
Криптография **– раздел криптологии, изучающий методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.**

(криптос – тайный, графейн – писать) – тайнопись



Конфиденциальность **(в криптологии) - невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).**

Аутентичность **(в криптологии) состоит в подлинности авторства и целостности.**



Алфавит **– конечное множество используемых для шифрования информации знаков.**

Текст **(*сообщение, послание*) – упорядоченный набор из элементов алфавита.**


Текст
(сообщение, послание)
зашифрование
Исходный текст
открытый текст, открытые данные
Шифртекст
закрытый текст, закрытые данные
расшифрование
дешифрование

***Зашифрование* (*шифрование*) – обратимое преобразование данных с помощью шифра, которое формирует шифртекст из открытого текста.**

***Расшифрование* (*шифрование*) – процесс преобразования зашифрованных данных в открытые данные при помощи шифра.**

***Дешифрование* - процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.**

Шифр **(криптографическая система) - совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.**

Шифр – криптографический метод, используемый для обеспечения конфиденциальности данных, включающий алгоритм зашифрования и алгоритм расшифрования.

Ключ – информация, необходимая для беспрепятственного зашифрования и дешифрования текстов.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма.

Ключ – изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

Уравнение зашифрования (расшифрования) **– соотношение, описывающее процесс образования зашифрованных (открытых) данных из открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования.**

Шифр Цезаря

$$y_i = (x_i + k) \bmod N$$

где x_i – i-й символ исходного текста
y_i - i-й символ шифротекста
k - константа (= 3)
N - количество символов алфавита

Метод ***полиномов***

$$y_i = \left(x_i^n + a_i \cdot x_i^{n-1} + \ldots + a_n \cdot x_i\right) \bmod p$$

где x_i – i-й элемент открытого текста,
y_i – i-й элемент шифротекста,
a_i – целые неотрицательные числа (ключ),
p – большое простое число.

Криптоанализ **– это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.**

Криптостойкость **- характеристика шифра, определяющая его стойкость к дешифрованию.**

Криптографическая защита **– это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки.**

Имитозащита **– защита от навязывания ложных данных.**

Имитовставка **– строка бит фиксированной длины, полученная применением симметричного криптографического метода к сообщению, добавляемая к сообщению для обеспечения его целостности и аутентификации источника данных.**

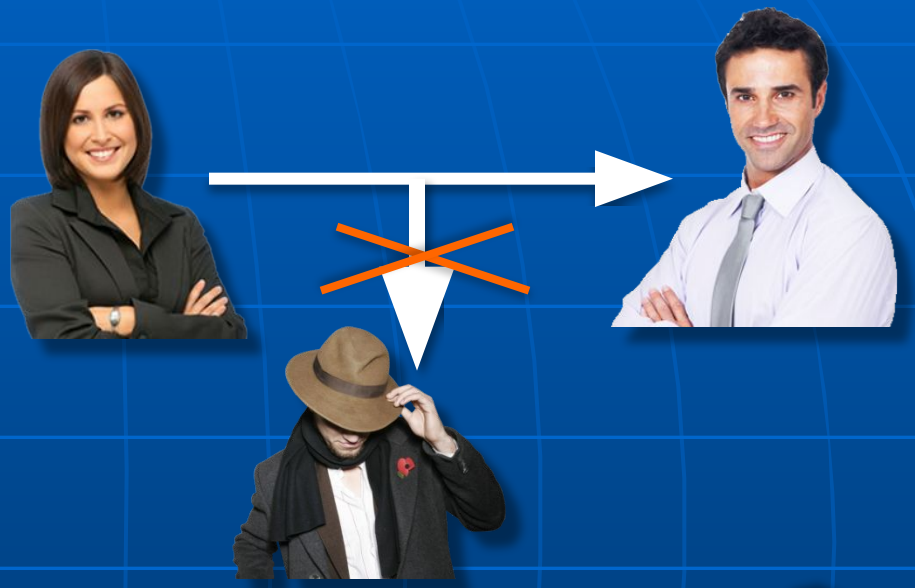
Федеральный закон от 06.04.2011 N 63-ФЗ

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

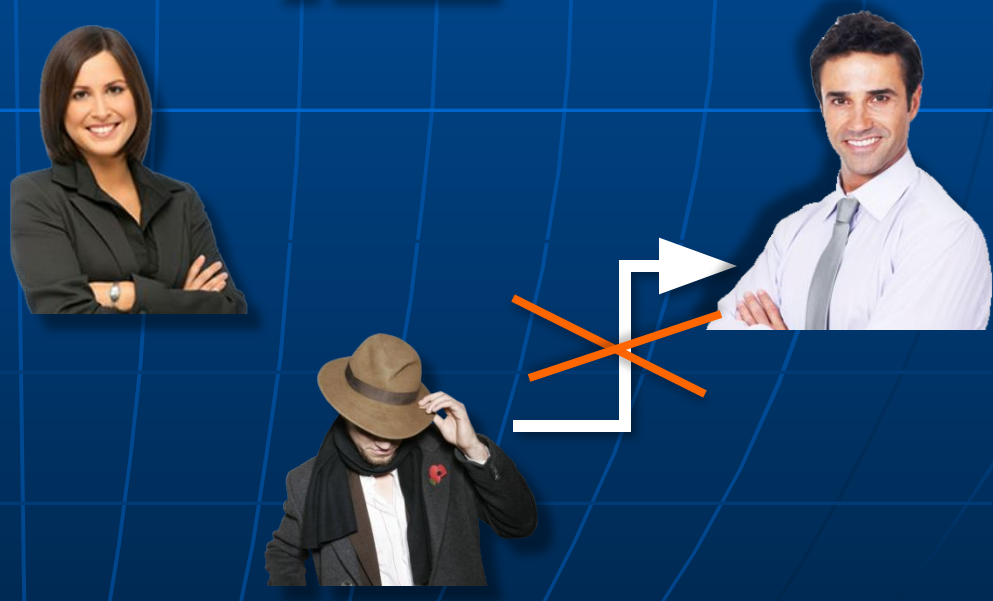
Электронная подпись - **присоединяемое к документу его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.**

Основные цели криптографии:

- Обеспечение конфиденциальности данных

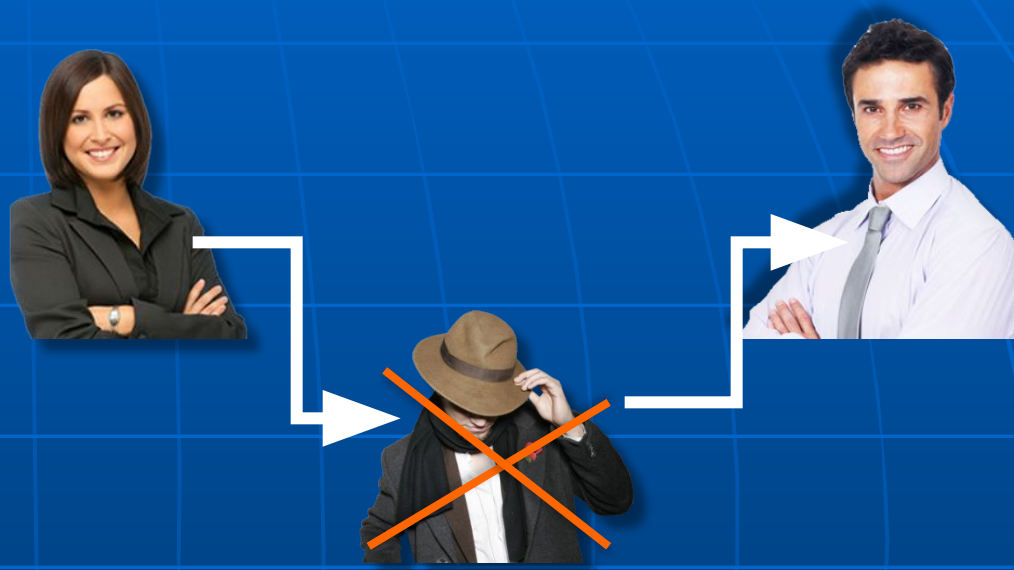


- Обеспечение аутентификации

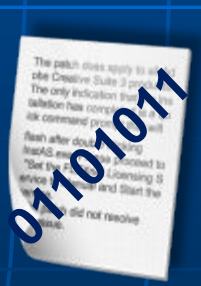


Основные цели криптографии:

- Обеспечение целостности данных



- Обеспечение невозможности отказа от авторства



Разделы современной криптографии:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- системы электронной подписи;
- управление ключами.

2. Исторические примеры шифрования.

Этапы развития криптографии:

1. Наивная криптография (до нач. XVI века).

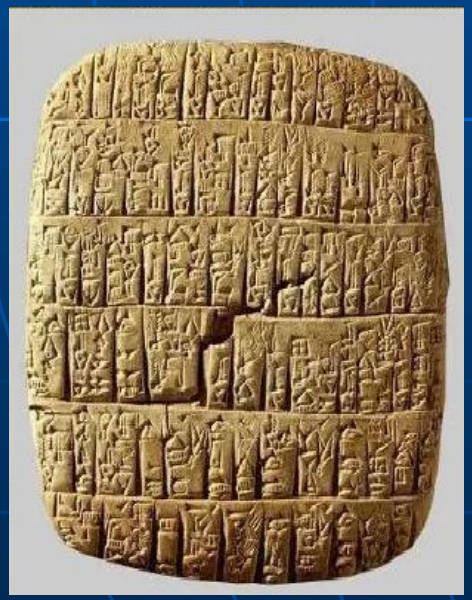
2. Формальная криптография (кон. XV века – нач. XX века).

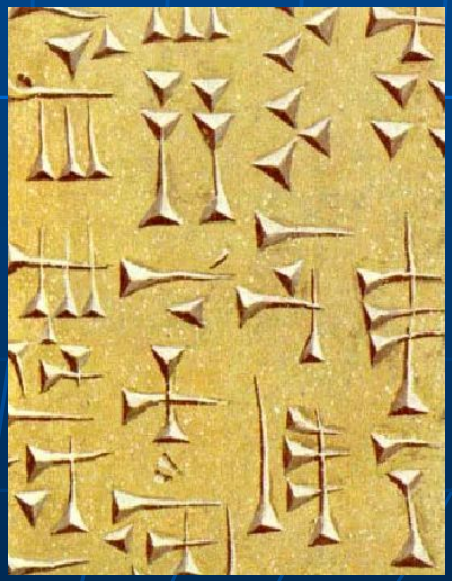
3. Научная криптография (30-е – 60-е годы XX века).

4. Компьютерная криптография (с 70-х годов XX века).

Наивная криптография

Старейший сохранившийся шифрованный текст – табличка с клинописью, содержащая рецепт изготовления глазури для гончарных изделий. Использовались редко употребляемые знаки, игнорировались некоторые символы, употреблялись цифры вместо имен.





Наивная криптография

Сцитала (IX в. до н. э.)

(сциталь, скиталь)

Наивная криптография

Шифр Цезаря (56 г. н. э.)

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

К У Р С А Н Т

Н Ц У Ф Г Р Х

Наивная криптография

Квадрат Полибия (3 в. до н. э.)

	1	2	3	4	5	6
I	А	Б	В	Г	Д	Е
II	Ж	З	И	К	Л	М
III	Н	О	П	Р	С	Т
IV	У	Ф	Х	Ц	Ч	Ш
V	Щ	Ы	Ь	Э	Ю	Я

Сообщение: П Р И К А З

Шифртекст: III3 III4 II3 II4 I1 II2

Формальная криптография

Шифровальный диск Альберти (XV в)

Формальная криптография

Шифр Вижинера (XVI в.)

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

Формальная криптография

Шифр Вижинера

Сообщение: КРИПТОГРАФИЯ

Ключ: ЗОНД

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

Шифртекст: СЭХУЩЫРФЗАХВ

Формальная криптография

Роторные криптосистемы

Позволили повысить криптостойкость и автоматизировать процесс шифрования

Механическая машина Томаса Джефферсона (1790 г.)

Enigma Артура Кирха (Шербиуса) (1918 г.)

Научная криптография: появление криптосистем со строгим математическим обоснованием криптостойкости, возникновение криптологии как науки

Компьютерная криптография – появление криптосистем, благодаря использованию ЭВМ обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры.

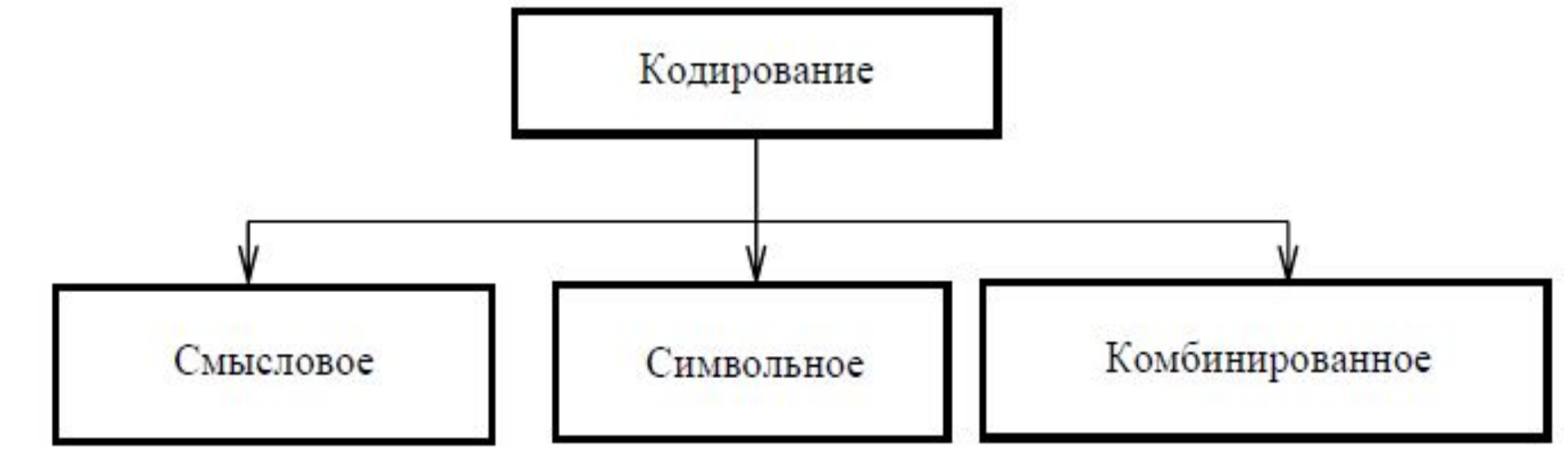
3. Классификация методов криптографического закрытия информации.

Виды криптографического закрытия информации

(по виду преобразования информации)

– шифрование;
– кодирование;
– рассечение-разнесение;
– сжатие;
– стеганография.

Кодирование – это процесс преобразования данных из одной формы, удобной для использования, в форму удобную для хранения, передачи и обработки.



Символьное кодирование: **каждый знак** алфавита открытого текста **заменяется** соответствующим **символом.**

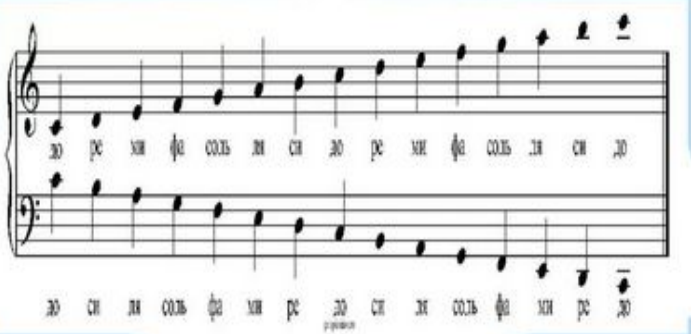
Азбука Морзе

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

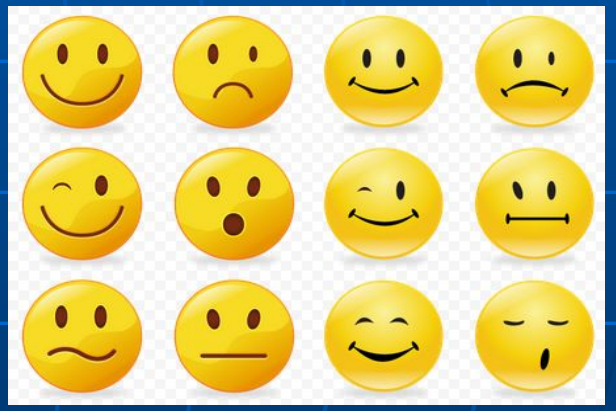
АЛФАВИТ БРАЙЛЯ

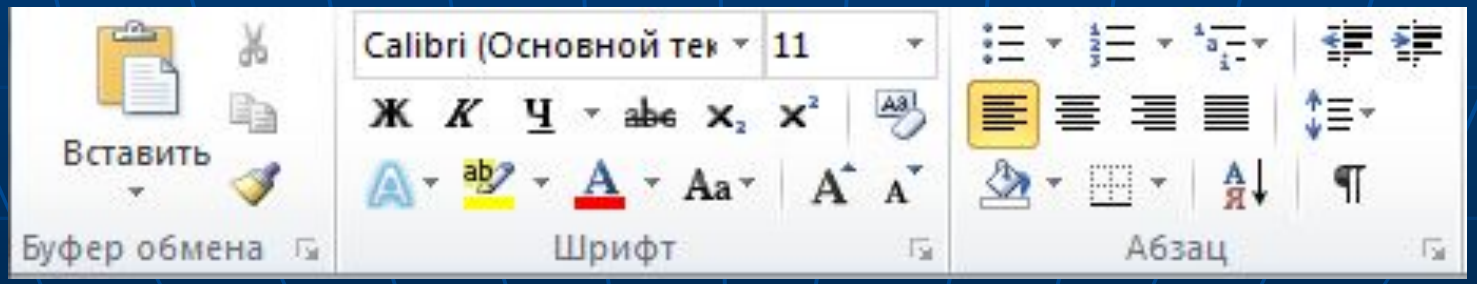
Символ	Двоичный код	Десятичный код	Символ	Двоичный код	Десятичный код
A	01000001	65	N	01001110	78
B	01000010	66	O	01001111	79
C	01000011	67	P	01010000	80
D	01000100	68	Q	01010001	81
E	01000101	69	R	01010010	82
F	01000110	70	S	01010011	83
G	01000111	71	T	01010100	84
H	01001000	72	U	01010101	85
I	01001001	73	V	01010110	86
J	01001010	74	W	01010111	87
K	01001011	75	X	01011000	88
L	01001100	76	Y	01011001	89
M	01001101	77	Z	01011010	90

Современная нотная запись



Смысловое кодирование – это **кодирование, в котором в качестве исходного алфавита используются** не только отдельные символы (буквы), но и **слова и** даже наиболее часто встречающиеся **фразы.**





Метод рассечения (разнесения) информации заключается в **разделении защищаемой информации** на такие **элементы, каждый из которых в отдельности не позволяет раскрыть содержание** защищаемой информации.

Пример: содержимое одного файла разбивается на блоки, которые разносятся по нескольким файлам.

Метод сжатия информации заключается в замене повторяющихся последовательностей символов в сообщении на меньшую по размерам последовательность.

Стеганография – способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения).

Стеганография – наука о методах преобразования информации в вид, при котором сам факт её существования становится секретом.

Виды стеганографии:

- **классическая;**
- **компьютерная;**
- **цифровая.**

Классическая стеганография:

Примеры:

- татуировки;

- восковые таблички;

Классическая стеганография:

Примеры:

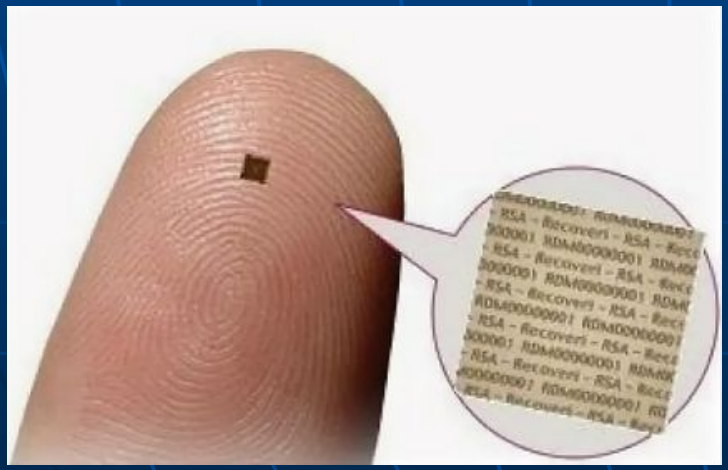
- **симпатические чернила**;

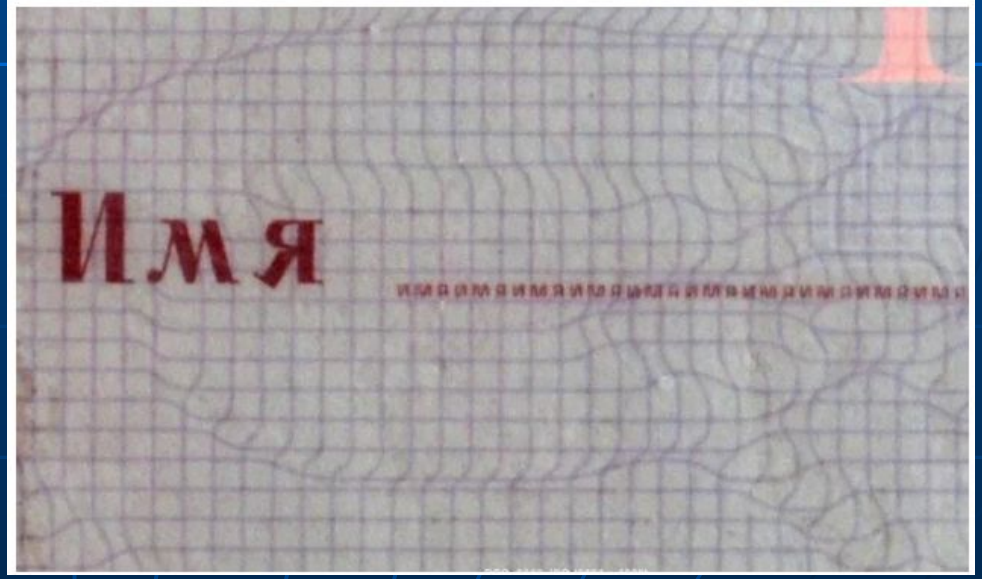
Чернила	Проявитель
Лимонная кислота (пищевая)	Бензилоранж
Воск	$CaCO_3$ или зубной порошок
Яблочный сок	Нагрев
Молоко	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев
Пирамидон (в спиртовом растворе)	Нагрев
Вяжущие средства для дезинфекции рта и глотки	Нагрев
Квасцы	Нагрев
Слюна	Очень слабый водный раствор чернил
Фенолфталеин	Разбавленная щелочь
Стиральный порошок	Свет лампы ультрафиолета
Крахмал	Йодная настойка
Аспирин	Соли железа

Классическая стеганография:

Примеры:

-микронадписи;





Классическая стеганография:

Примеры:
-микроточки;

Не просто игра

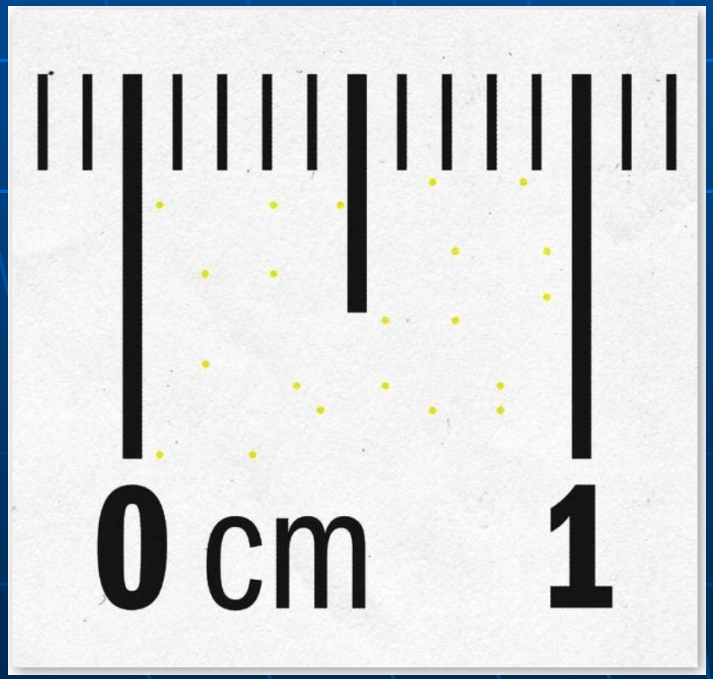
Е́сли какую-то игру и можно назвать царицей игр, то этого титула, не́сомненно, заслуживают шахматы. В них случайность ника́к не влияет на ход игры́, а определяющее значе́ние имеют чиста́я стратегия и память: число возможных ходов в партии имеет порядок 10^{123} — это невообразимая величина. Однажды чемпионом мира по шахматам стал профессиональный математик Эмануэль Ласкер (1868–1941). Сейчас мы говорим о стандартных шахматах на доске из 64 клеток, но еще в далекую викторианскую эпоху математик Артур Кэли (1821–1895) уже рассмотрел трехмерные шахматы, в которые сегодня играют персонажи сериала «Звездный путь».

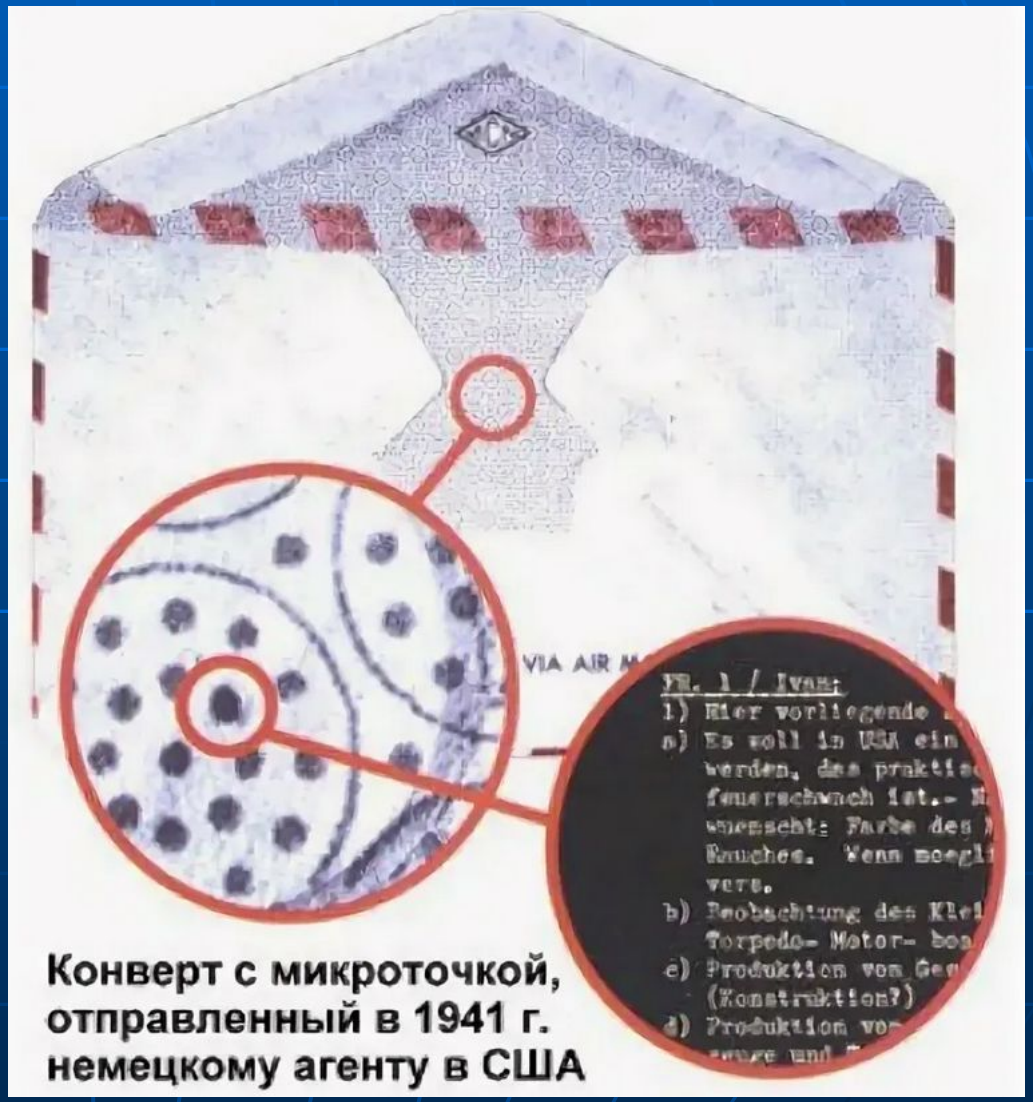
Классическая стеганография:

Примеры:

-микроточки;

желтые точки





Конверт с микроточкой, отправленный в 1941 г. немецкому агенту в США

Классическая стеганография:

Примеры:

-пустышечный шифр;

Компания «Люцифер» использует едкий натр, тяжелые грузила, острогу трехзубую, обветшалый ватник.

Классическая стеганография:

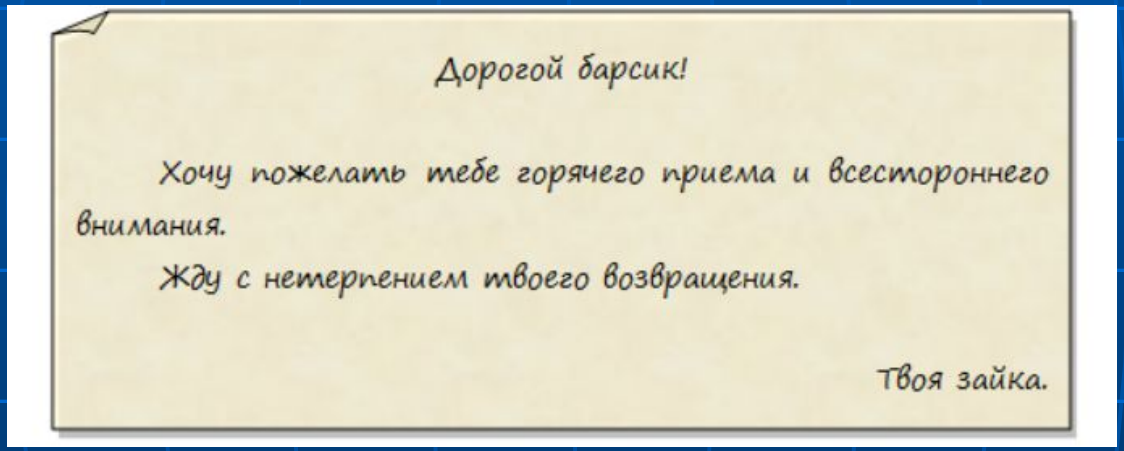
Примеры:
-актостих;

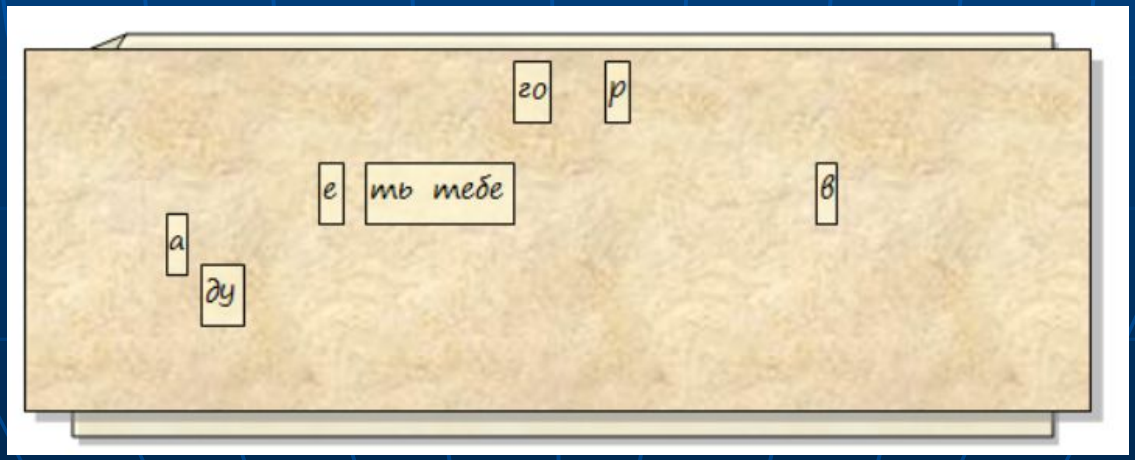
Рязанские задумчивые клены,
О, вашу грусть вовек мне не забыть...
Судьба, ко мне ты все же благосклонна,
Смогла решить — мне быть и только быть,
И благодарный возрожденья чуду,
Я кленов грусти все же не забуду...

Классическая стеганография:

Примеры:

-решетка Кардано;





Компьютерная стеганография — направление стеганографии, основанное на особенностях компьютерной платформы.

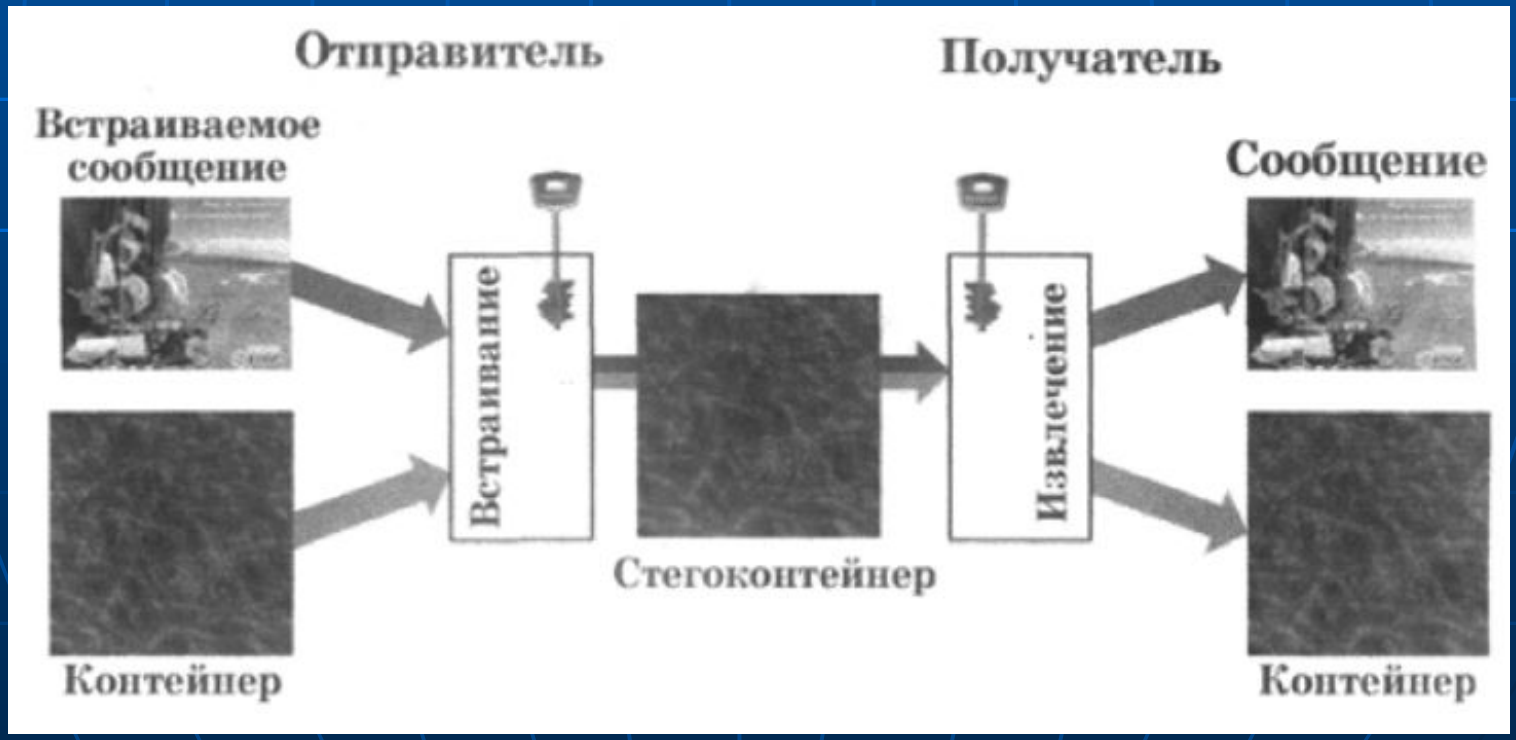
Примеры:

-скрытие данных в неиспользуемых областях форматов файлов;

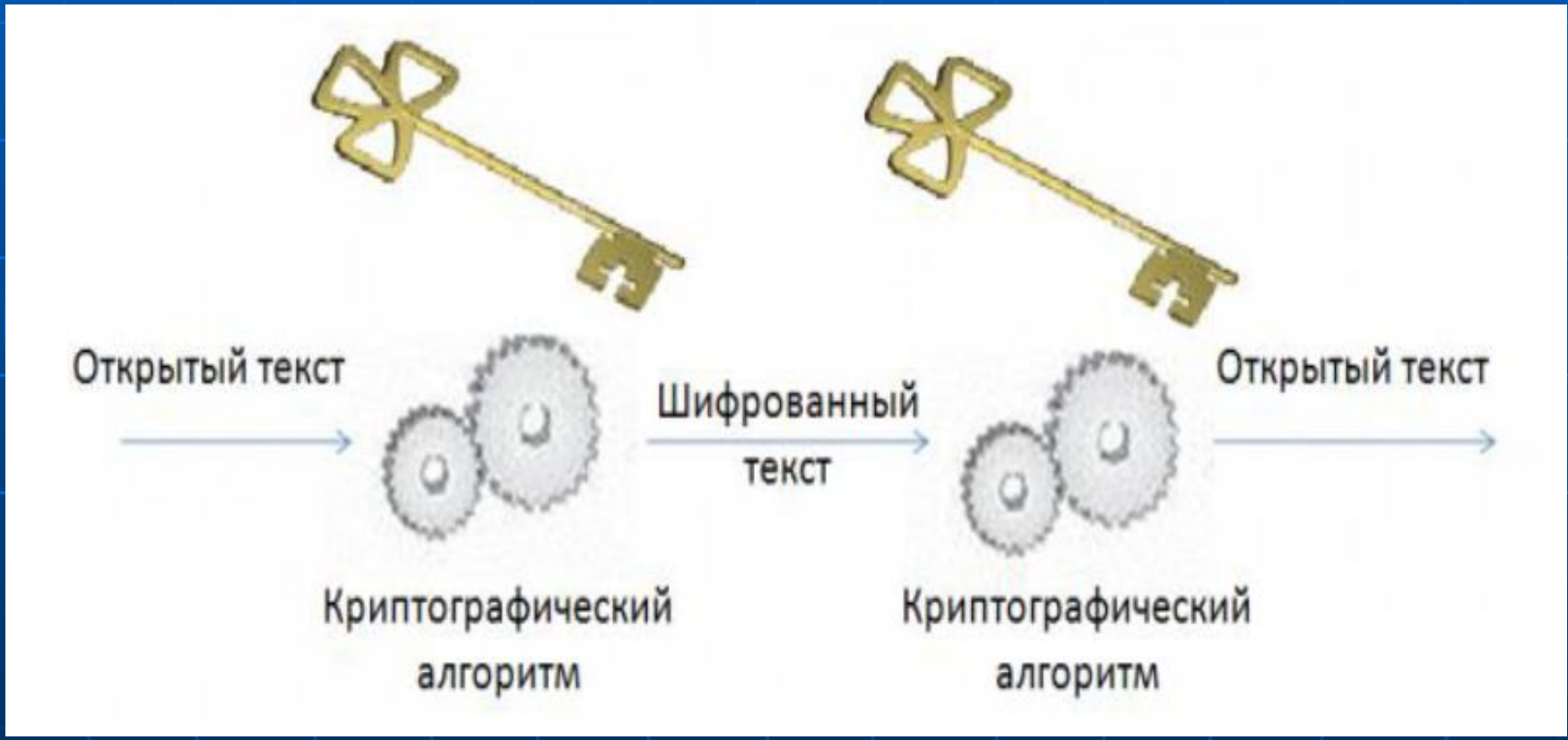
-подмена символов в названиях файлов;

- текстовая стеганография и т. д.

Цифровая стеганография - направление стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.



Общий принцип шифрования



Методы шифрования

(по типу ключей)

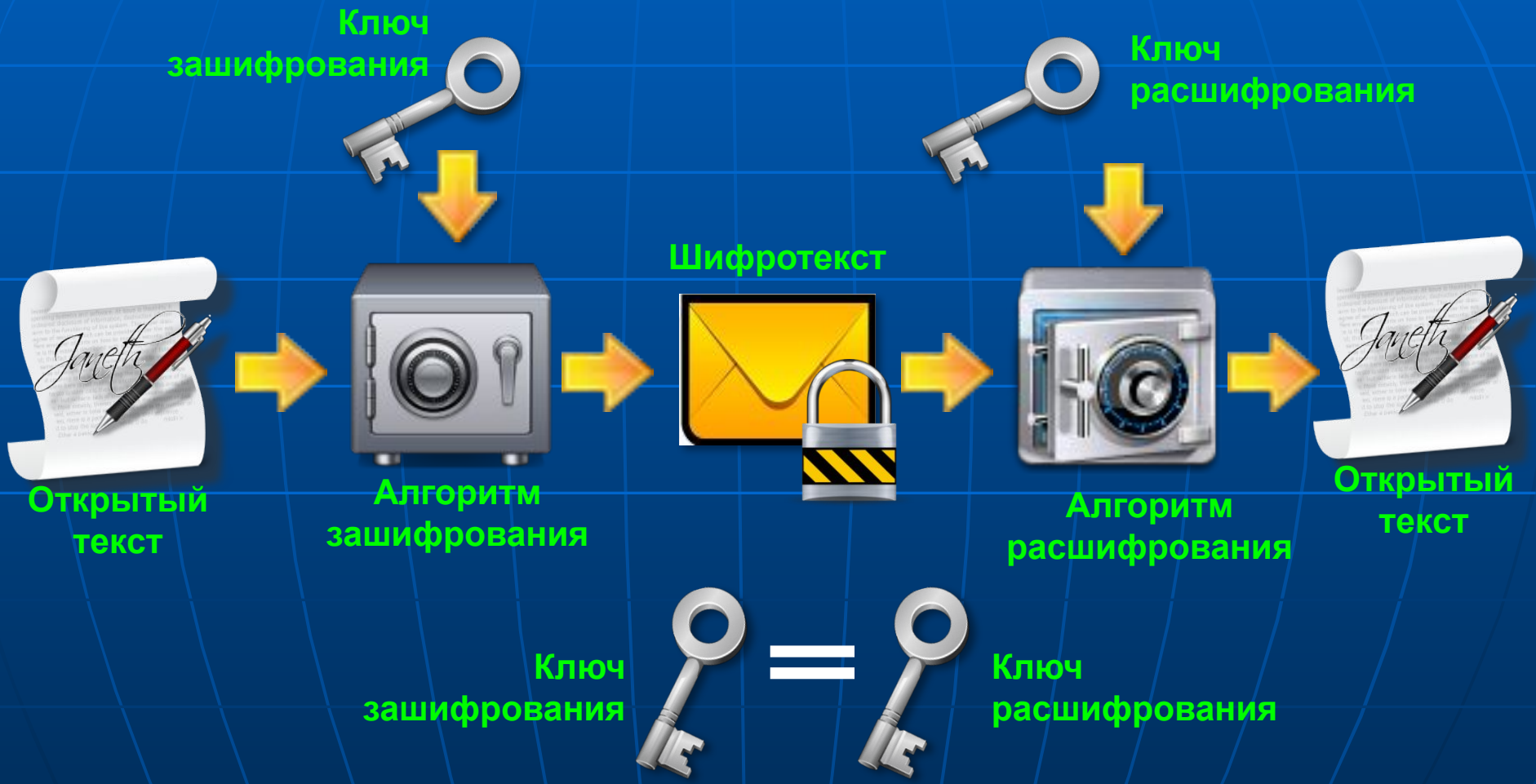
симметричные

(одноключевые, с секретным ключом)

асимметричные

(несимметричные, двухключевые, с открытым ключом)

Симметричное шифрование



Симметричное шифрование

Преимущества:

-большая скорость;

-простота в реализации;

-меньшая требуемая длина ключа для сопоставимой стойкости.

Недостатки:

-сложность обмена ключами;

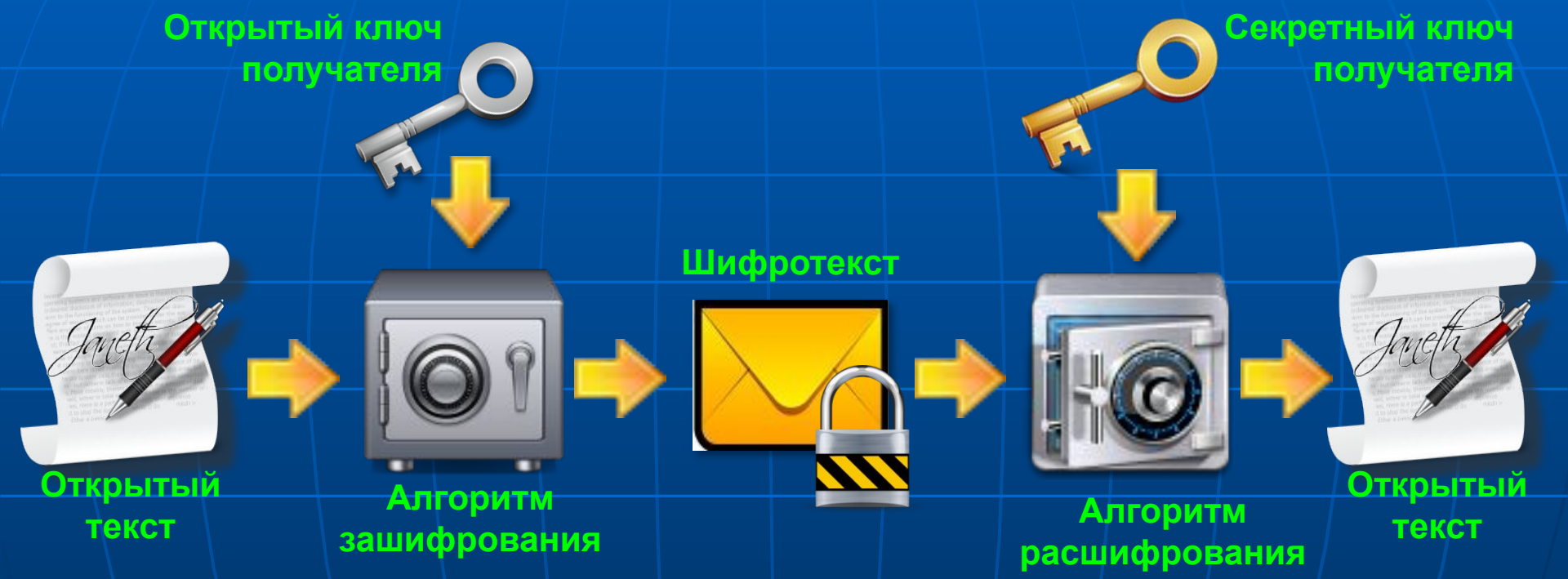
-сложность управления ключами в большой сети (означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети.)

Симметричное шифрование

Примеры криптоалгоритмов:

- **AES** (англ. Advanced Encryption Standard) - американский стандарт шифрования;
- **ГОСТ 28147-89** (отечественный стандарт шифрования данных);
- **DES** (англ. Data Encryption Standard) - стандарт шифрования данных в США до AES;
- **IDEA** (англ. International Data Encryption Algorithm);
- **RC6** (Шифр Ривеста).

Асимметричное шифрование



Асимметричное шифрование

Преимущества:

-в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной;

-отсутствии необходимости предварительной передачи секретного ключа по надёжному каналу.

Недостатки:

-низкая скорость выполнения операций зашифровки и расшифровки;

-используются более длинные ключи;

-трудно внести изменения.

Асимметричное шифрование

Преимущества:

-в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной;

-отсутствии необходимости предварительной передачи секретного ключа по надёжному каналу.

Недостатки:

-низкая скорость выполнения операций зашифровки и расшифровки;

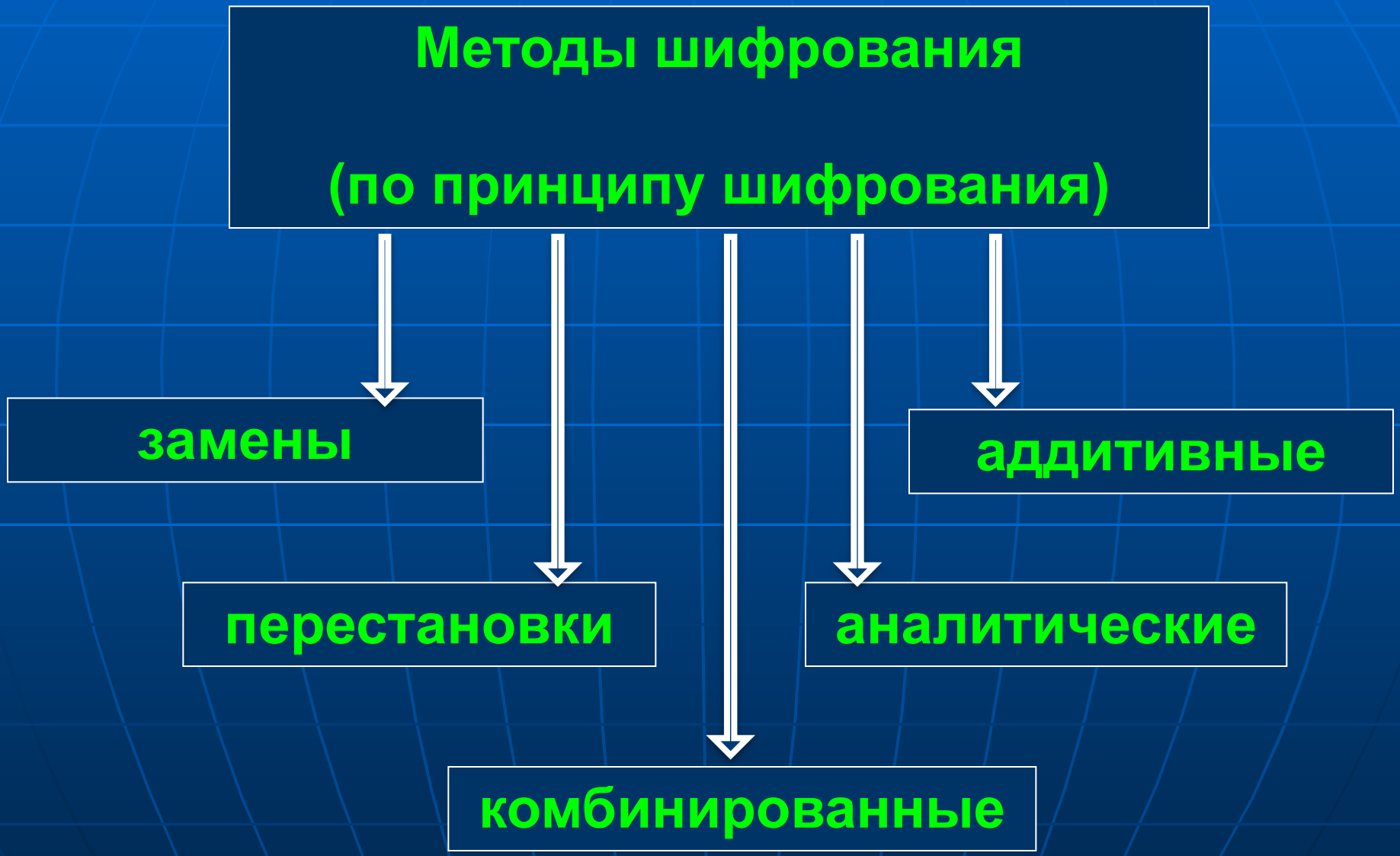
-используются более длинные ключи;

-трудно внести изменения.

Асимметричное шифрование

Примеры криптоалгоритмов:

- **RSA** (Rivest-Shamir-Adleman, Ривест — Шамир — Адлеман);
- **Elgamal** (Шифросистема Эль-Гамаля);
- **ГОСТ 34.10-2001**;
- **Williams System** (Криптосистема Уильямса);
- **RSA** (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman).


Методы шифрования
(по принципу шифрования)
замены
перестановки
комбинированные
аналитические
аддитивные

Метод замены (подстановки) - **символы шифруемого текста заменяются другими символами**, взятыми из одного алфавита (одноалфавитная замена) или нескольких алфавитов (многоалфавитная замена).

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

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
Q	W	E	R	T	Y	U	I	O	P	[	]	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	<	>	@	%

Примеры:

- шифр Цезаря, квадрат Полибия, метод сдвига (одноалфавитная замена);

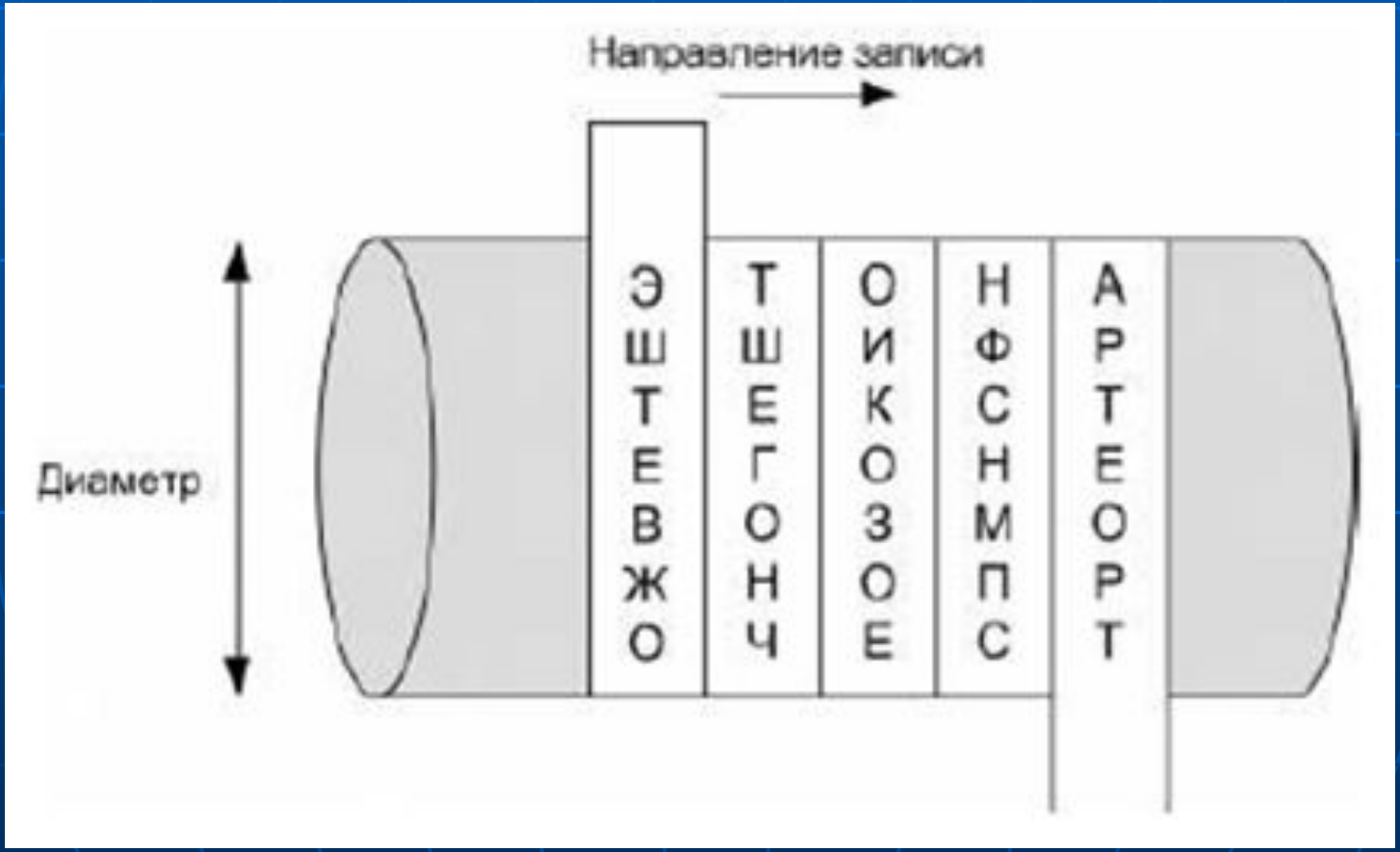
- шифр Вижинера, диск Альберти.

Метод перестановки – несложный метод криптографического преобразования, **заключающийся в перестановке местами символов исходного текста по некоторому правилу**.

Примеры:
Простая перестановка

Ключ: 1-3-2
Исходный текст: ПРО СТА Я_П ЕРЕ СТА НОВ КА
Шифротекст: ПОР САТ ЯП_ ЕЕР САТ НВО КА

Перестановка по таблице
Пример:
Сцитала



Перестановка по таблице:

Пример: шифр вертикальной перестановки

Открытый текст:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Размер блока: 7x6

Ключ: 5,4,1,7,2,6,3

5	1	4	7	2	6	3
В	О	Т	П	Р	И	М
Е	Р	Ш	И	Ф	Р	А
В	Е	Р	Т	И	К	А
Л	Ь	Н	О	Й	П	Е
Р	Е	С	Т	А	Н	О
В	К	И	-	-	-	-

Шифртекст:

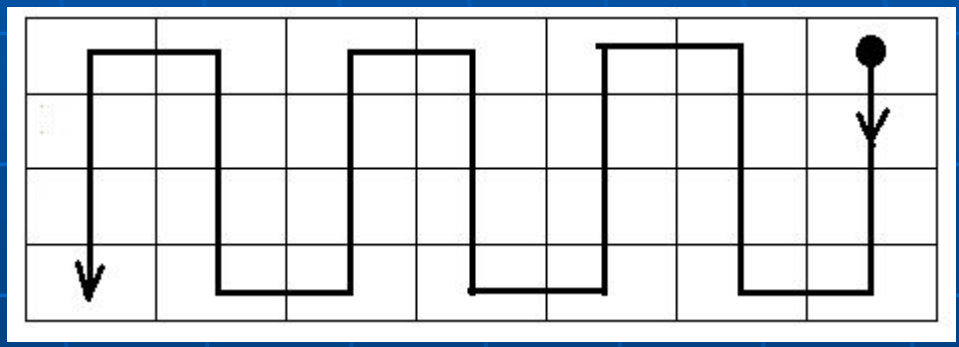
ОРЕЬЕКРФИЙА-МААЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ-

Маршрутная перестановка

Открытый текст:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

Размер блока: 7х4



Ключ:

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Шифртекст:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Аддитивные методы состоят в наложении по определенному, закону гаммы шифра на открытые данные (гаммирование).

Гамма шифр - это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных.

Процесс зашифрования заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом, например с использованием операции сложения по модулю.

Аналитические методы состоят в том, что шифруемый **текст преобразуется по** некоторому **аналитическому правилу** (формуле) и **основаны на понятии односторонней функции.**

Функция является односторонней, если она за сравнительно небольшое число операций преобразует элемент открытого текста X в элемент шифротекста, а обратная операция является вычислительно трудоемкой.

Примеры односторонней функции :

- умножение матриц;
- решение задачи об укладке ранца;
- вычисление значения полинома по модулю;
- экспоненциальные преобразования и др.

Комбинированные методы предполагают использование нескольких различных способов шифрования, т.е. **последовательное шифрование исходного текста с помощью двух или более методов**.

Распространенные комбинации:

- подстановка + гаммирование
- замена + гаммирование
- гаммирование + гаммирование
- замена + перестановка

Пример:

- стандарт шифрования данных DES;
- ГОСТ 28147-89.

Методы шифрования (по размеру блока информации)

- **блочные**
- **потоковые (поточные)**

Поточные шифры – это те, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста.

Блочные шифры Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами.

Требования к криптографическим системам:

– стойкость шифра противостоять криптоанализу должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи полного перебора ключей;

– криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа;

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

Требования к криптографическим системам:

– шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных;

– незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;

– структурные элементы алгоритма шифрования должны быть неизменными;

Требования к криптографическим системам:

– шифртекст не должен существенно превосходить по объему исходную информацию;

– ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

– структурные элементы алгоритма шифрования должны быть неизменными;

Требования к криптографическим системам:

– любой ключ из множества возможных должен обеспечивать равную криптостойкость;

– время шифрования не должно быть большим;

– стоимость шифрования должна быть согласована со стоимостью закрываемой информации.