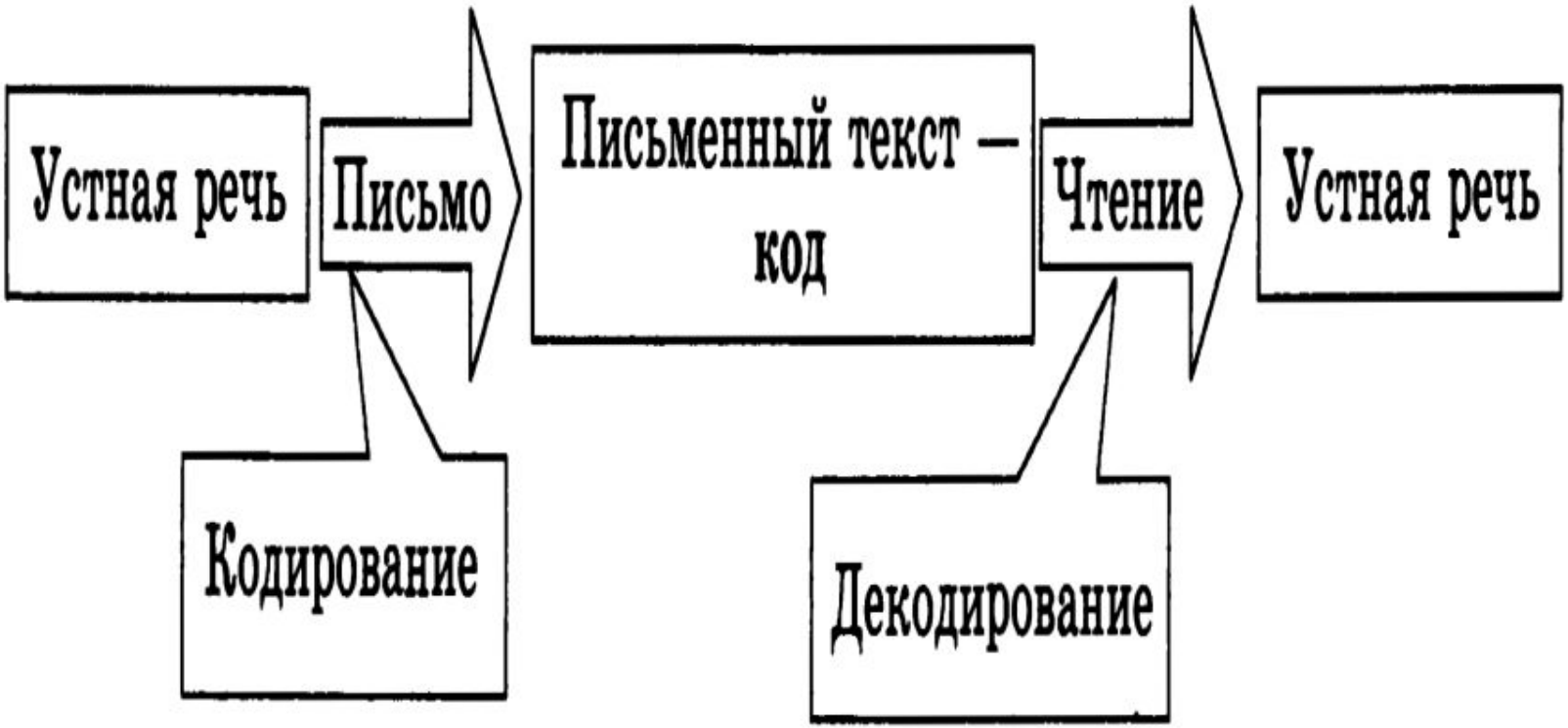
Представление информации, языки, кодирование

- Язык – это знаковая система для представления и передачи информации
- Люди сохраняют свои знания на различных носителях. Знания передаются не только в пространстве, но и во времени – от поколения к поколению.

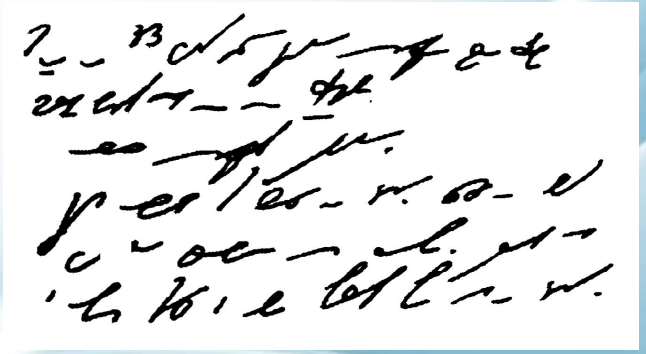
Кодирование -

процесс представления информации, удобный для ее хранения и / или передачи.


Устная речь
Письмо
Письменный текст – код
Чтение
Устная речь
Кодирование
Декодирование

Способы кодирования

- Алфавит национального языка (русского, английского)
- Стенография и другие знаковые системы



Выбор способа кодирования зависит от

- цели кодирования;
- условий;
- имеющихся средств;
- предполагаемого способа дальнейшей обработки информации.

Языки	
Естественные	Формальные
Тридцать пять умножить на сто двадцать семь	35*127

Переход от представления на естественном языке к представлению на формальном языке можно также рассматривать как кодирование

В информатике широко используются такие формальные языки как языки программирования.

Защита от несанкционированного доступа

Шифрование – процесс превращения открытого текста в зашифрованный.

Дешифрование – процесс обратного преобразования, при котором восстанавливается исходный текст.

Шифрование

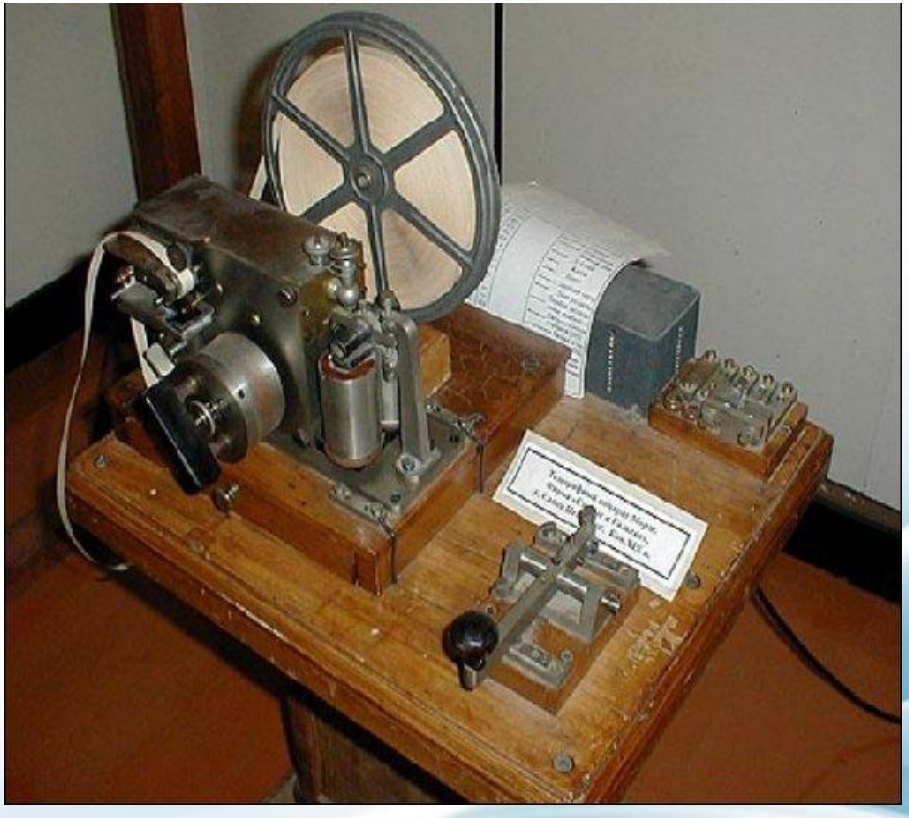
это тоже кодирование, но с засекреченным методом, известным только источнику и адресату.

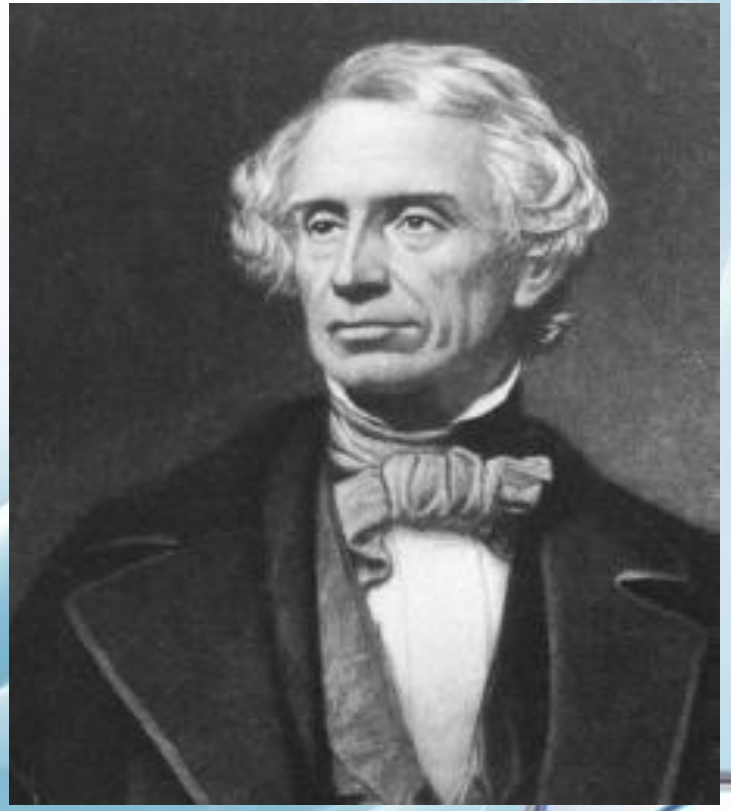
Методами шифрования занимается наука **криптография.**

11.9.14

История технических способов кодирования информации

Телеграф (1837 год)





Сэмюэл Финли Бриз Морзе (1791-1872, США)

Кодовая таблица азбуки 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 • • • •	

Равномерный телеграфный код

Оригинальный код Бодо

Управляющие символы		
o.	...	пробел, перейти к таблице букв
.o	...	пробел, перейти к таблице цифр
oo	...	удалить последний знак

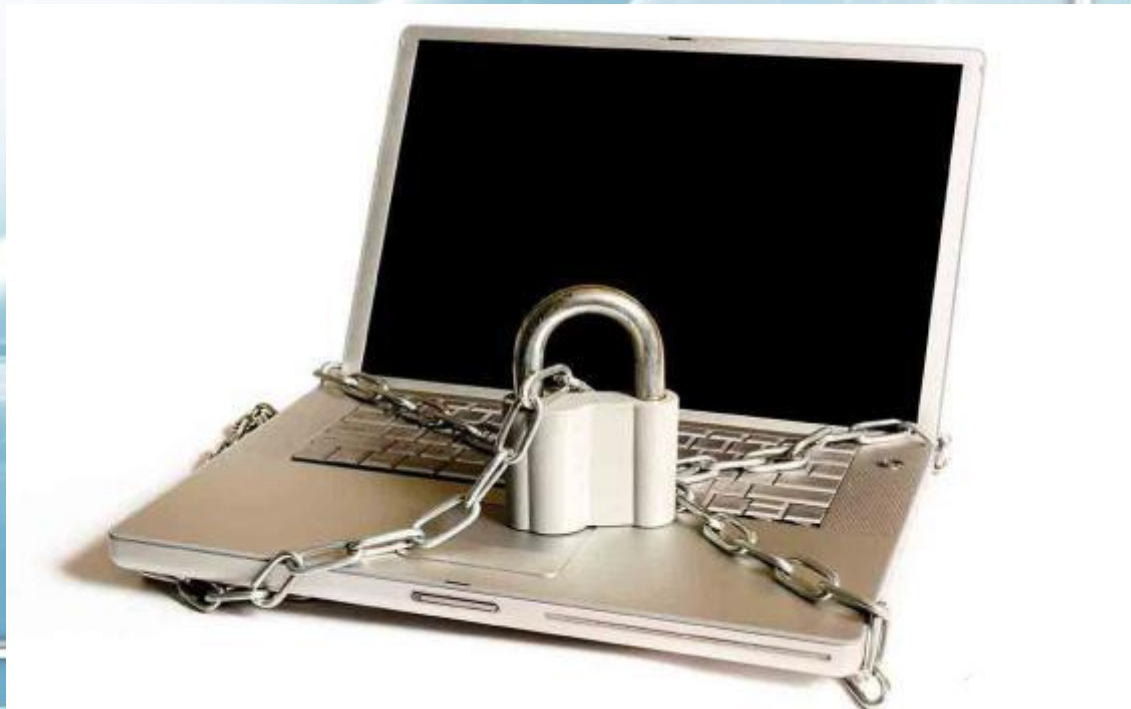
таблица букв						таблица цифр					
..	o..	A	oo	o..	K	..	o..	1	o.	o..	.
..	oo.	É	oo	oo.	L	..	.o.	2	o.	.o.	9/
..	.o.	E	oo	.o.	M	..	..o	3	o.	..o	7/
..	.oo	I	oo	.oo	N	..	o.o	4	o.	o.o	2/
..	ooo	O	oo	ooo	P	..	ooo	5	o.	ooo	'
..	o.o	U	oo	o.o	Q	..	oo.	1/	o.	oo.	:
..	..o	Y	oo	..o	R	..	.oo	3/	o.	.oo	?
.o	..o	B	o.	..o	S	.o	o..	6	oo	o..	(
.o	o.o	C	o.	o.o	T	.o	.o.	7	oo	.o.	)
.o	ooo	D	o.	ooo	V	.o	..o	8	oo	..o	-
.o	.oo	F	o.	.oo	W	.o	o.o	9	oo	o.o	/
.o	.o.	G	o.	.o.	X	.o	ooo	0	oo	ooo	+
.o	oo.	H	o.	oo.	Z	.o	oo.	4/	oo	oo.	=
.o	o..	J	o.	o..	—	.o	.oo	5/	oo	.oo	£

Жан Морис Эмиль Бодо (1845-1903), Франция

Представление информации					
Языки представления информации					
Естественные: русский, китайский, английский и др.			Формальные: язык математики, нотная грамота, языки программирования и др.		
Кодирование					
Цели кодирования					
Засекречивание информации	Быстрый способ записи	Передача по техническим каналам связи		Выполнение математических вычислений	
Шифрование	*Стенография*	*Телеграфный код*		*Системы счисления*	
Алгоритмы криптографии	Один знак — слово или сочетание букв	Код Морзе: неравномерный, троичный код	Код Бодо: равномерный, двоичный код	Для человека: десятичная с. с.	Для компьютера: двоичная с. с.

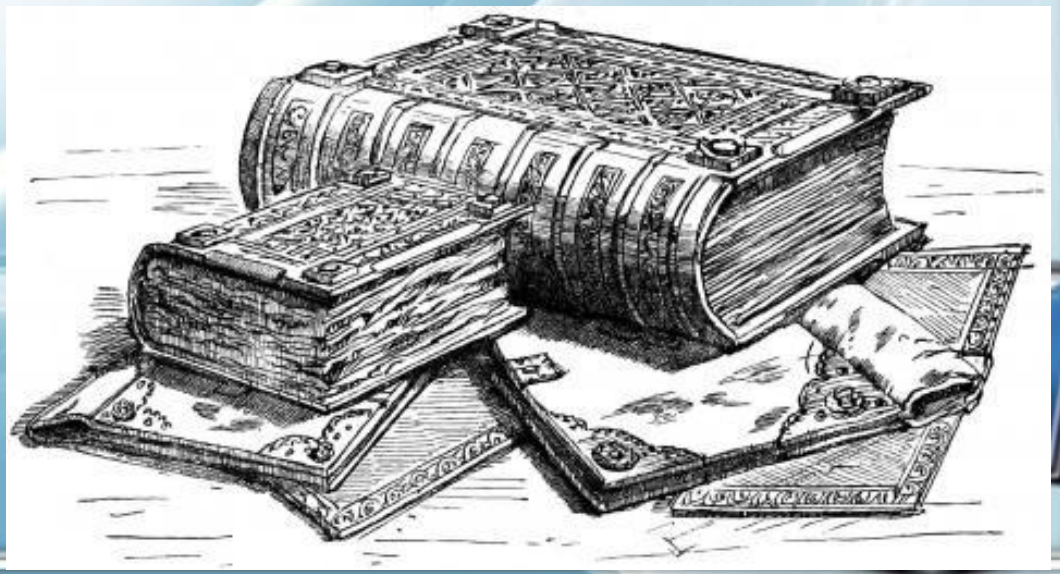
Криптография как инструмент для обеспечения конфиденциальности

Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.



История развития науки криптографии

Формально криптография (с греческого — «тайнопись») определяется как наука, обеспечивающая секретность сообщения.
История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования:

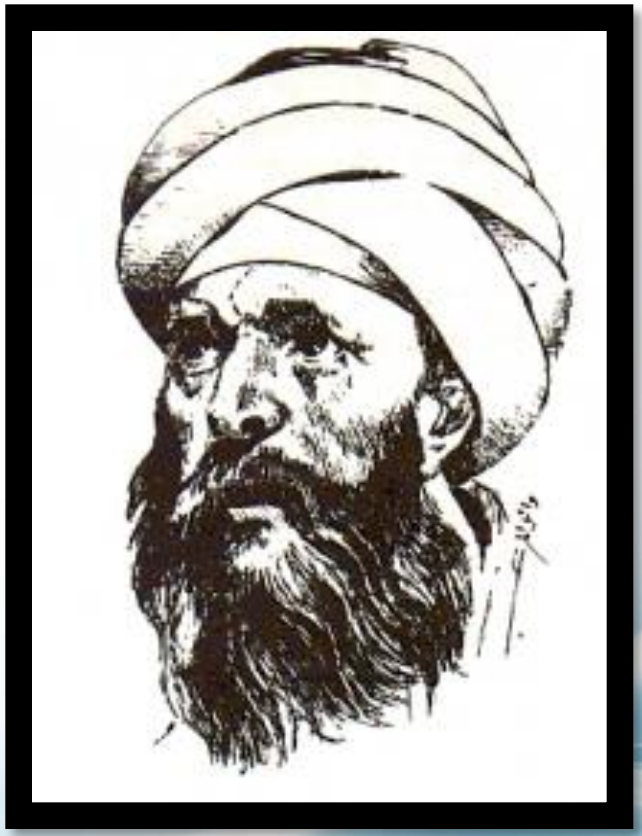


1.Первый период (*3 тыс. до н. э.*)

- моноалфавитные шифры

- основной принцип — **замена алфавита исходного текста другим алфавитом** через замену букв другими буквами или символами

2.Второй период (*IX век на Ближнем Востоке* (Ал-Кинди) и *XV век в Европе* (Леон Баттист Альберти) — *начало XX века*) **-полиалфавитные** шифры.



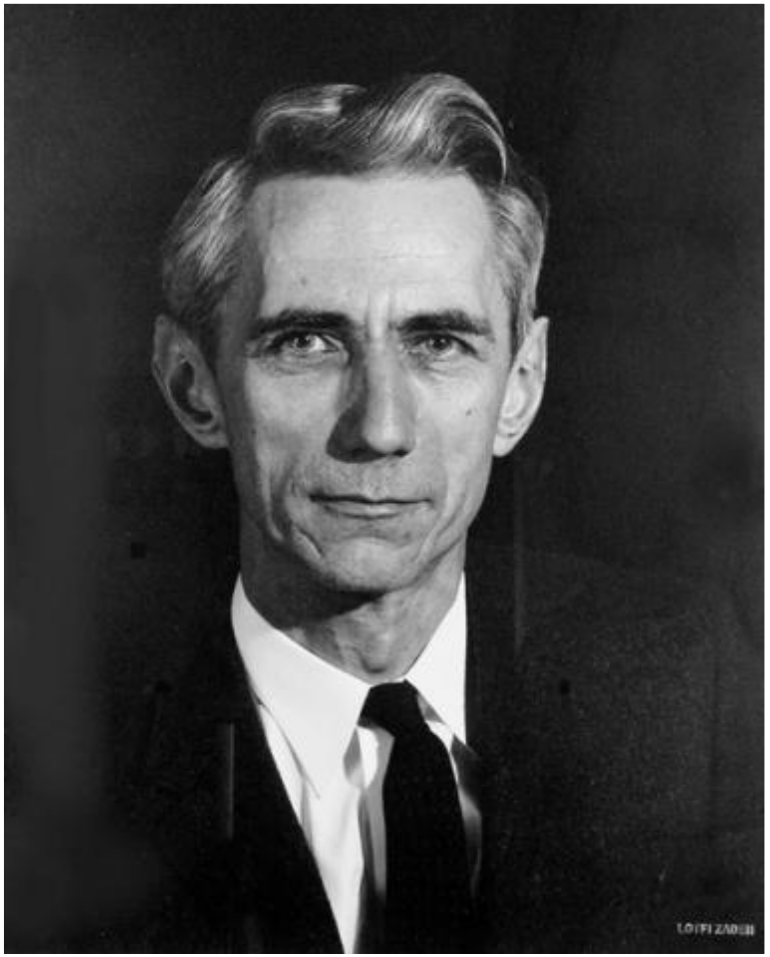
Ал-Кинди

Леон Баттист Альберти

3.Третий период (*с начала и до середины XX века*) - **внедрение электромеханических устройств в работу шифровальщиков**.

-продолжение использования **полиалфавитных** шифров.

4.Четвертый период *—с 50-х до 70-х годов XX века* — **переход к математической криптографии**. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования.



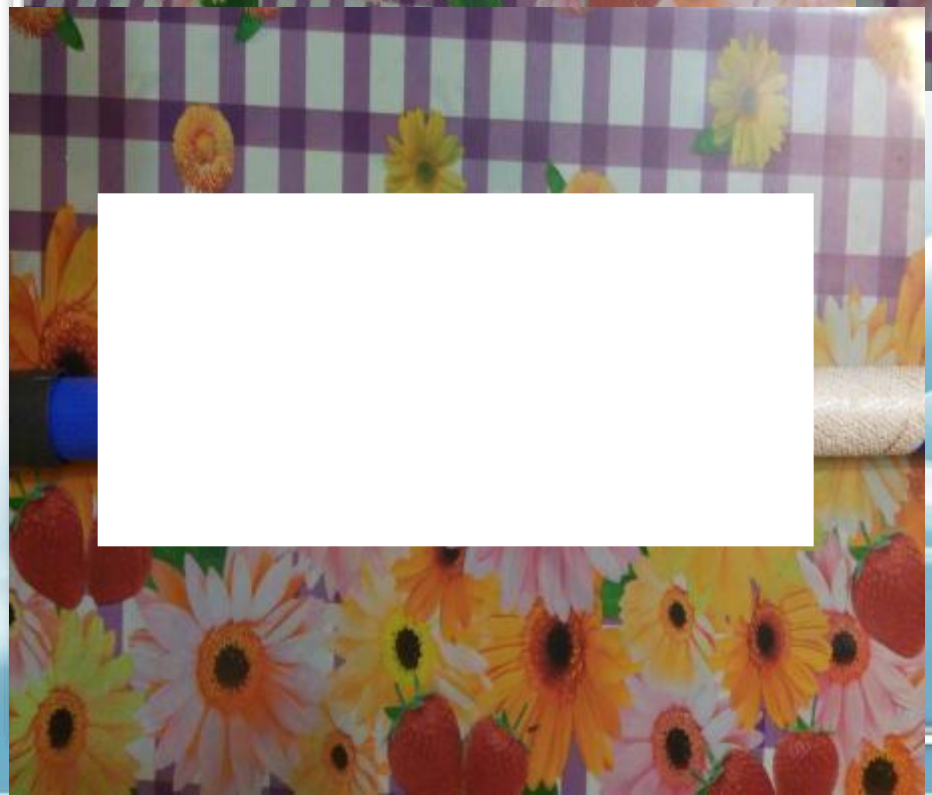
Клод Шеннон

5.Современный период (*с конца 1970-х годов по наше время*) зарождение и развитие нового направления — **криптография с открытым ключом**.

Также известна другая периодизация истории криптографии:

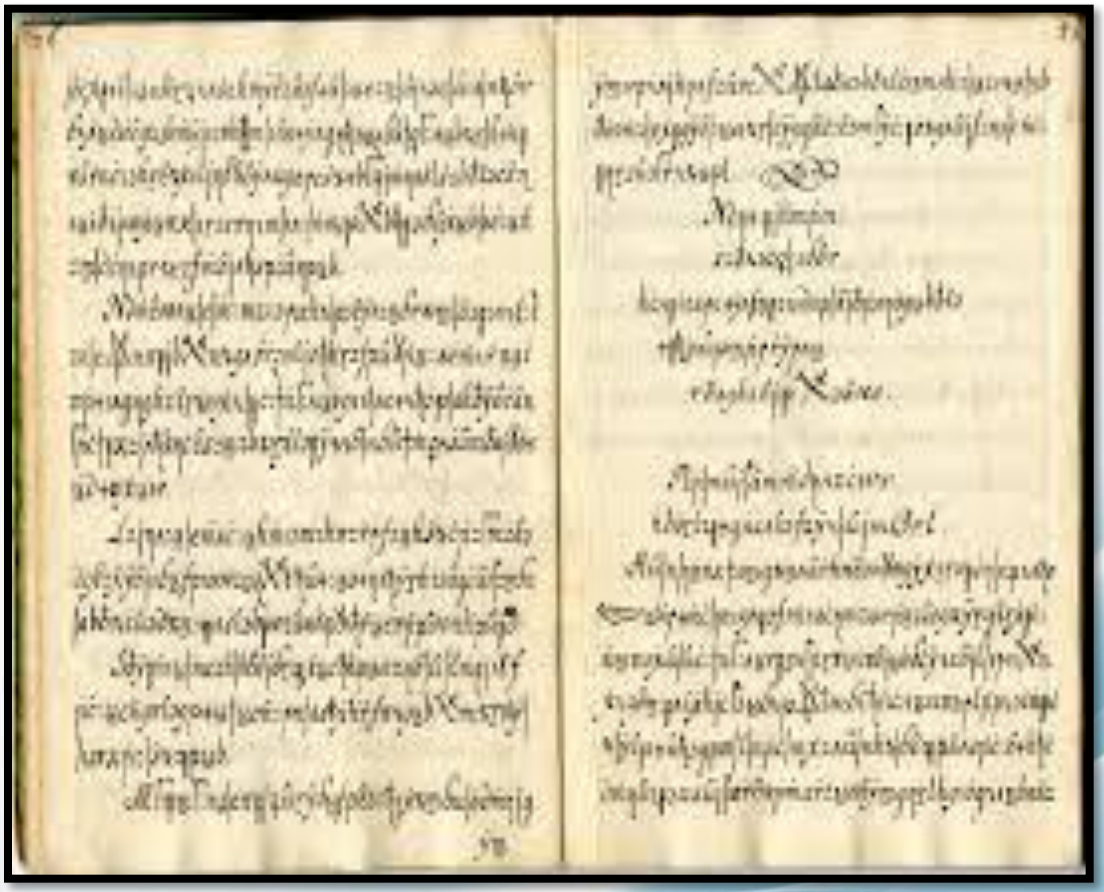
1.*Эней Тактик* написал ***первый научный труд о криптографии***.

Широко известен **шифр «Скитала» -** *Спартой против Афин в V веке до н. э.*



2. *Средние века*

-*Кодекс Copiale* — изящно оформленную рукопись с водяными знаками, не расшифрованную полностью до сих пор.

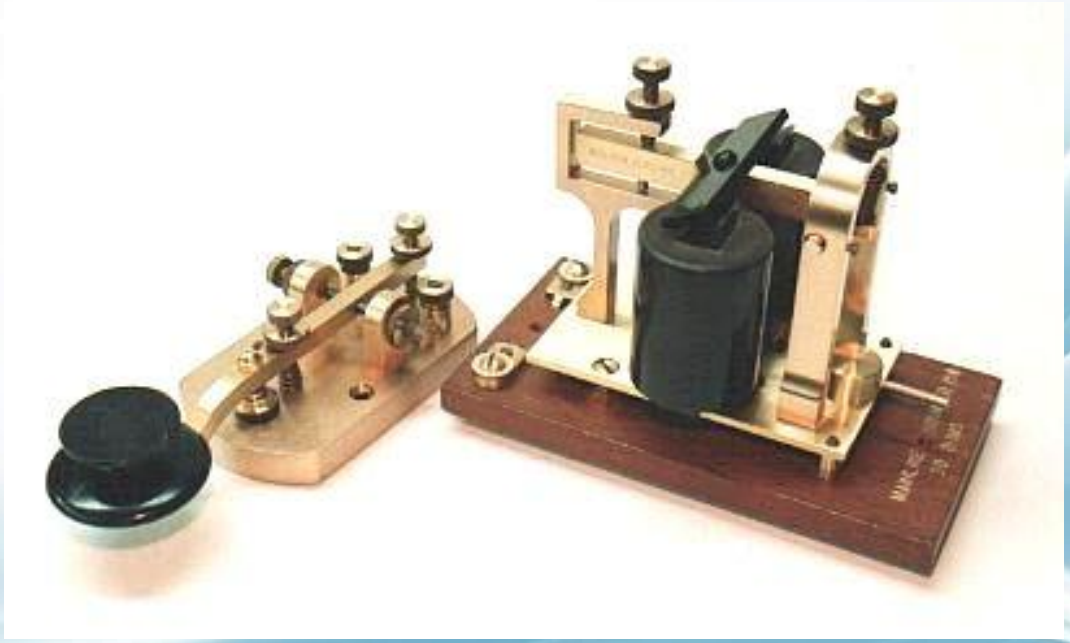


Кодекс Copiale

3.*Эпоха Возрождения - золотой век криптографии*: ее изучением занимался Фрэнсис Бэкон, предложивший двоичный способ шифрования.

Фрэнсис Бэкон

4.Появление телеграфа- факт передачи данных перестал быть секретным.



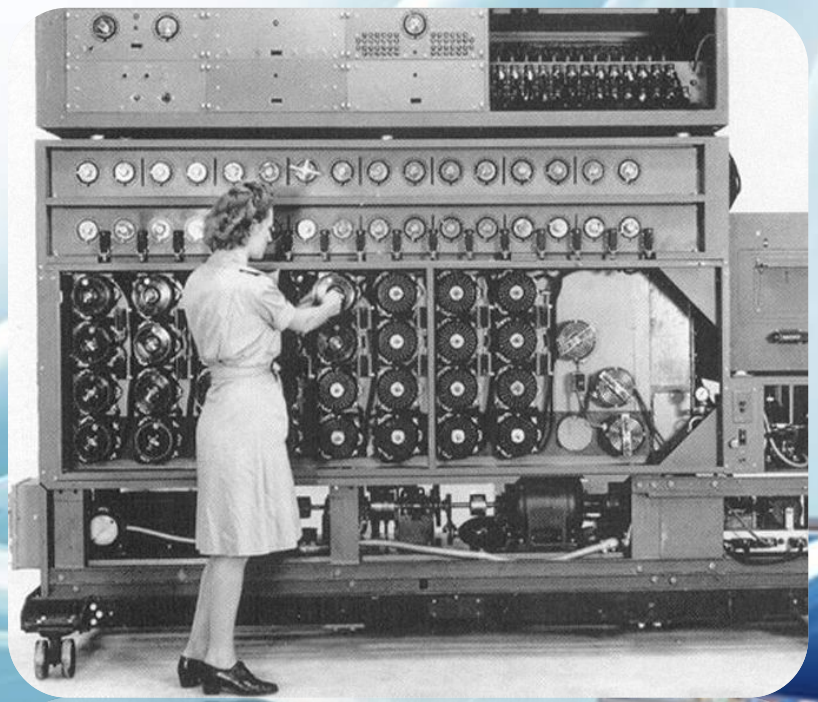
***5.Первая мировая война* - криптография** стала признанным **боевым инструментом**.

***6.Вторая мировая война* -развитие компьютерных систем**. Использованные шифровальные машины ясно показали жизненную важность информационного контроля.

Wehrmacht Enigma («Энигма»)- Шифровальная машина Третьего рейха.

Turing Bombe («Бомба Тьюринга»)

Разработанный под руководством Алана Тьюринга дешифратор.



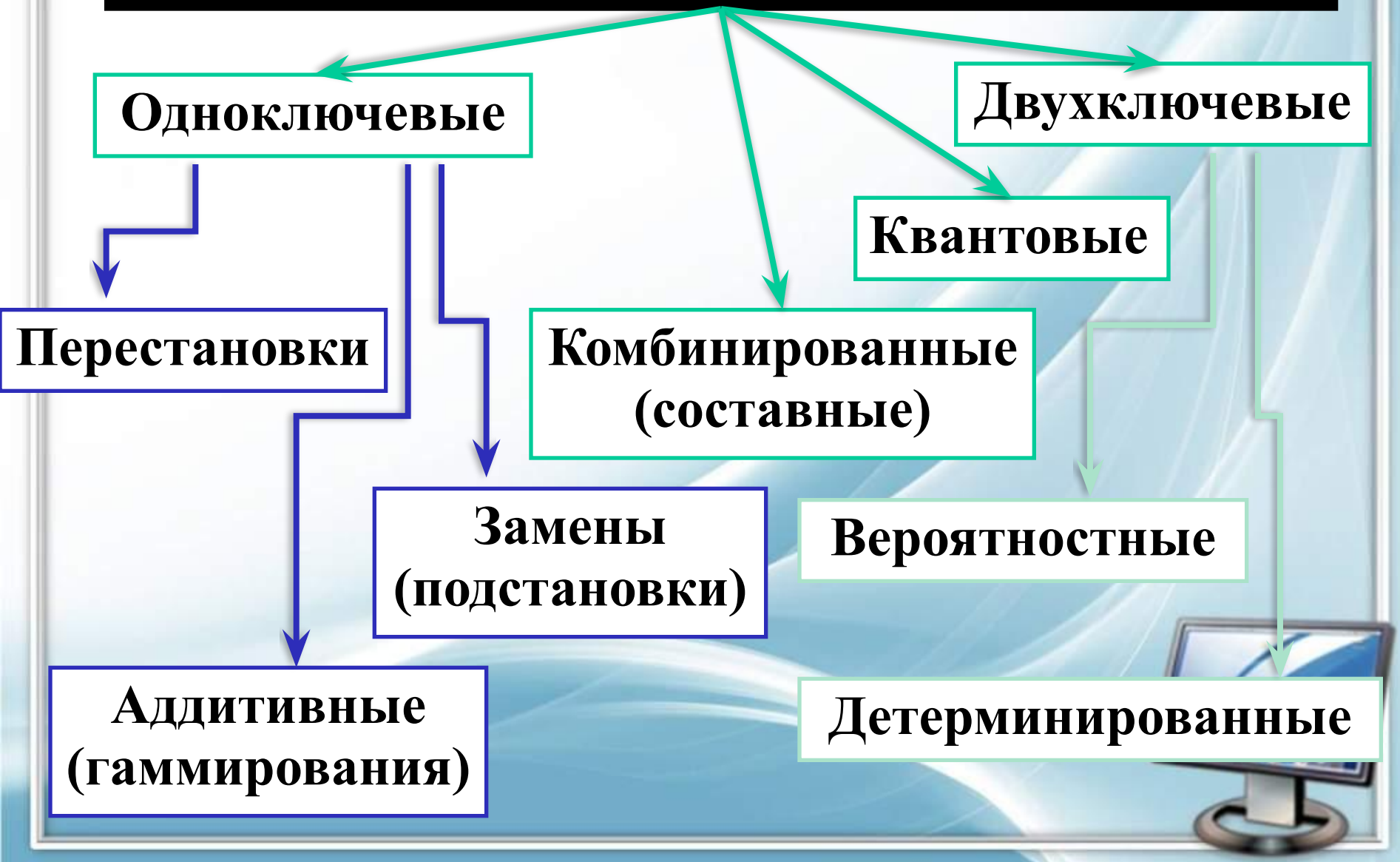
Классификация криптографических систем

1. По области применения

Криптосистемы **ограниченного использования**

Криптосистемы **общего использования**

2. По особенностям алгоритма шифрования



3. По количеству символов сообщения

Блочные

Потоковые

4. По стойкости шифра

- совершенные
- практически стойкие
- нестойкие

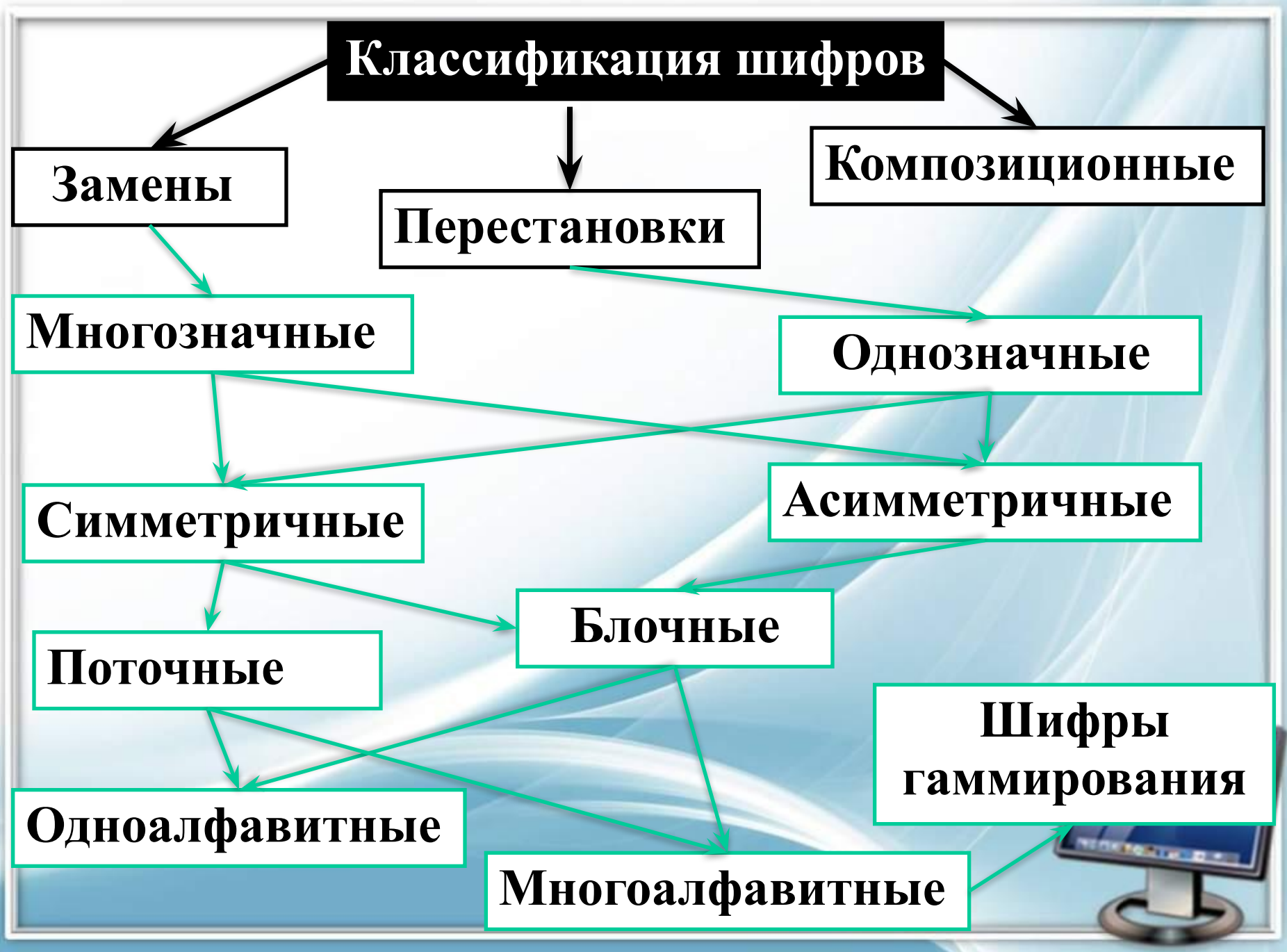
Основные требования, предъявляемые к криптосистемам

- Сложность и трудоёмкость процедур шифрования и дешифрования;
- Временные и стоимостные затраты на защиту информации;
- Процедуры шифрования и дешифрования;
- Количество всех возможных ключей шифра;

- Избыточность сообщений;
- Любой ключ из множества возможных ;
- Незначительное изменение ключа;
- Зашифрованное сообщение.

Шифры

Шифр (от фр. *chiffre* «цифра» от араб. صِفْر, *sifr* «ноль») — какая-либо система преобразования текста с секретом (ключом) для обеспечения секретности передаваемой информации.


Классификация шифров
Замены
Перестановки
Композиционные
Многозначные
Однозначные
Симметричные
Асимметричные
Блочные
Поточные
Шифры гаммирования
Одноалфавитные
Многоалфавитные

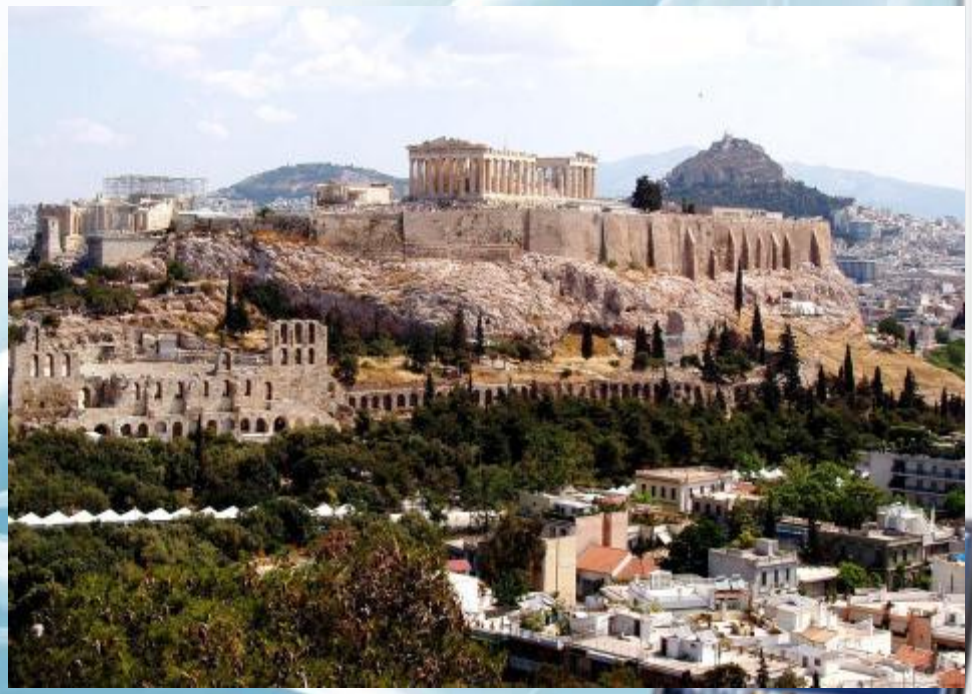
Аффинный шифр

Аффинный шифр - шифр простой замены, использующий в качестве ключа два числа. Линейная зависимость **аффинного шифра** может быть такой:

2*N+8

INFORMATION →

AKUMRIJVAMK

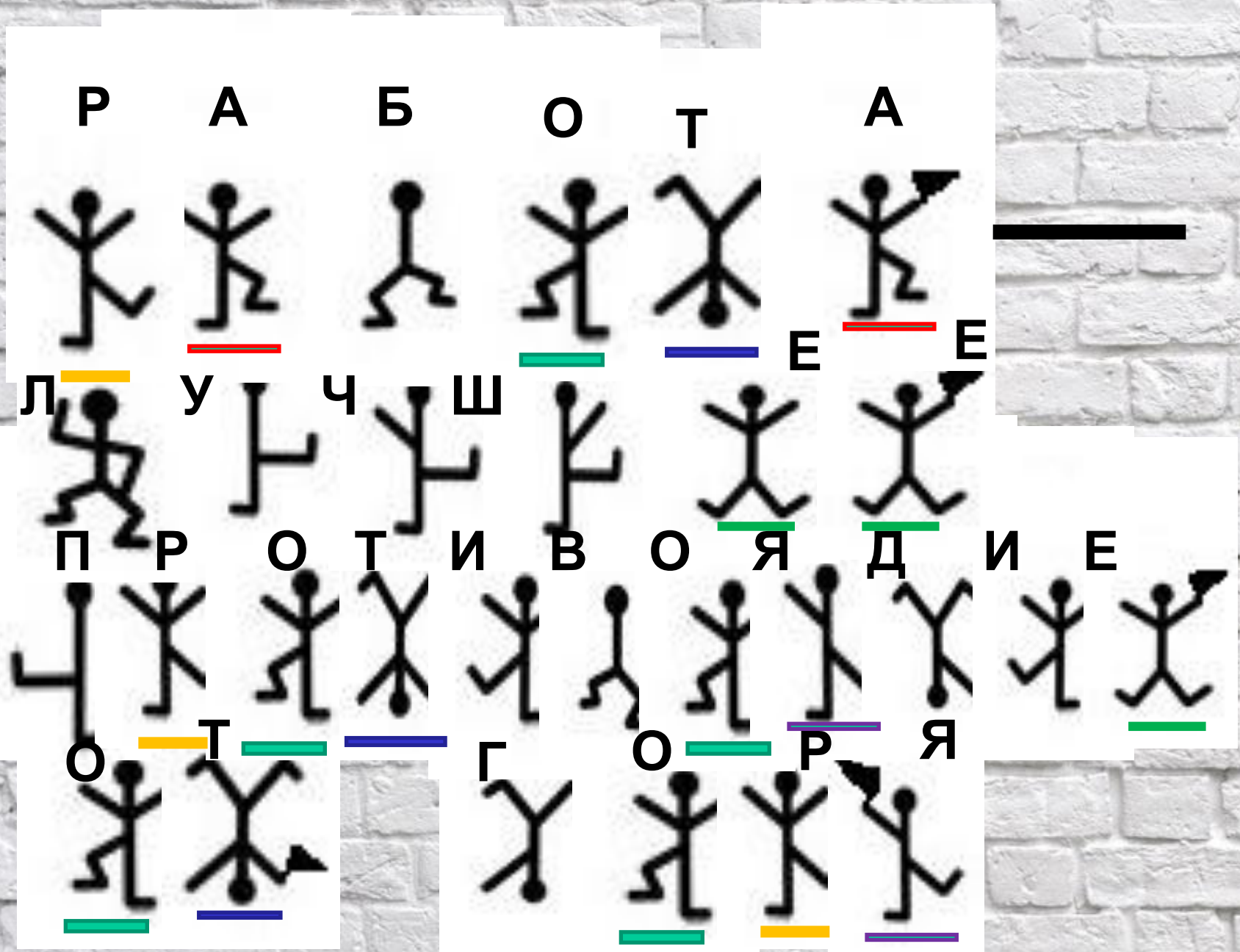


Шифр Цезаря

Замена символов открытого текста согласно *формуле,* например такой:
N-номер символа в алфавите
N+3
INFORMATION ⟶
LRISUQDWMDSR

Шифр пляшущих человечков

Преимущество - благодаря стенографическим свойствам *шифровки* может написан где угодно.
Недостаток - не обеспечивает ни достаточной конфиденциальности, ни аутентичности.


Р А Б О Т А
Е Е
Л У Ч Ш
П Р О Т И В О Я Д И Е
О Т Г О Р Я

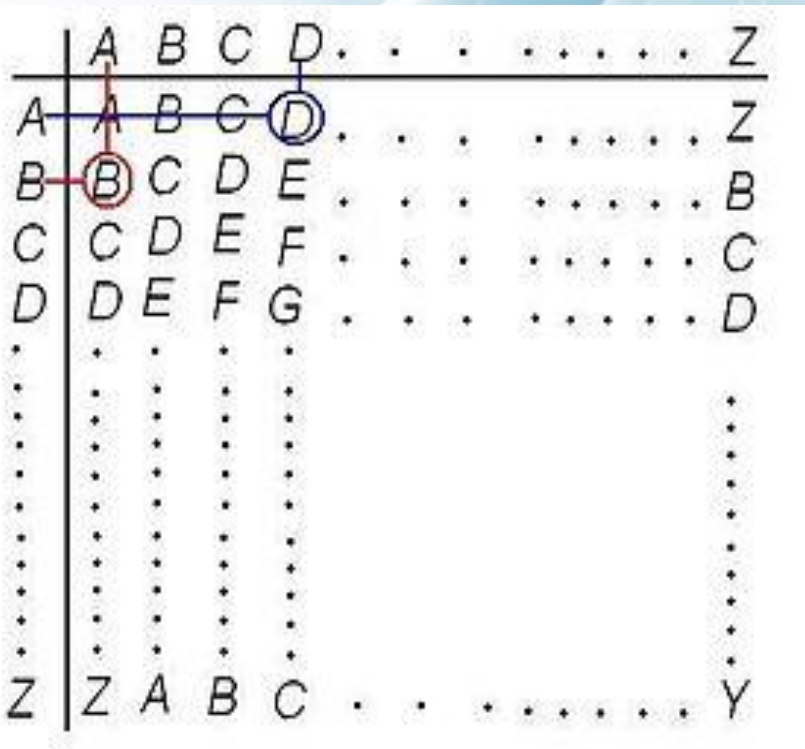
Шифр Виженера

За ключ шифра **Виженера** берут слово (фразу), удобное для запоминания, слово (кодовая фраза) повторяется до тех пор, пока не станет равным длине сообщения.

Таблица Виженера

Для зашифрования сообщения шифром **Виженера** при помощи таблицы **Виженера**, выберите столбец, начинающийся с первого символа открытого текста и строку, начинающуюся с первого символа ключа. На пересечении этих столбца и строки будет находиться первый символ шифровки.

ключ	A B C A B C
открытый текст	D A N C E
шифрованный текст	D B P C F



Штриховые коды

Линейный штрихкод

Штрихово́й код (штрихко́д) — графическая информация, наносимая на поверхность, маркировку или упаковку изделий, представляющая возможность считывания её техническими средствами — последовательность чёрных и белых полос либо других геометрических фигур.

Способы кодирования информации:

1.Линейные

2.Двухмерные

Сферы применения

- Увеличение скорости прохождения документооборота платежных систем;
- Минимизация ошибок считывания данных за счет автоматизации процесса;
- Идентификация сотрудников;
- Организация систем регистрации времени;
- Унификация бланков для сбора разного вида данных;
- Упрощение складской инвентаризации;
- Контроль за наличием и продвижением товаров в магазинах, обеспечение их сохранности.

QR-код

Основное достоинство QR-кода — это лёгкое распознавание сканирующим оборудованием.