

# ШИФРЫ И ИХ ОСНОВНЫЕ ТРЕБОВАНИЯ



# Криптография

Криптография - это область знаний, относящаяся к средствам и методам преобразования сообщений в непонятную для посторонних форму, а также к средствам и методам проверки подлинности сообщений.

Цель криптографии:

сделать понятное (т.е. "открытое") сообщение всецело непонятным (т.е. "закрытым") для непосвященного. Подобный трюк осуществляется при помощи кодирования и шифрования, а то, что получается в итоге - зовется криптограммой.



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

Шифр - разновидность кодирования секретной информации для безопасной передачи по открытым каналам, в целях исключения нежелательного ее получения или изменения третьими лицами. В состав шифра входят алгоритмы шифрования и дешифрования.

Все шифры различают, прежде всего, на шифры замены, шифры перестановки и композиционные шифры.

## Классификация шифров:

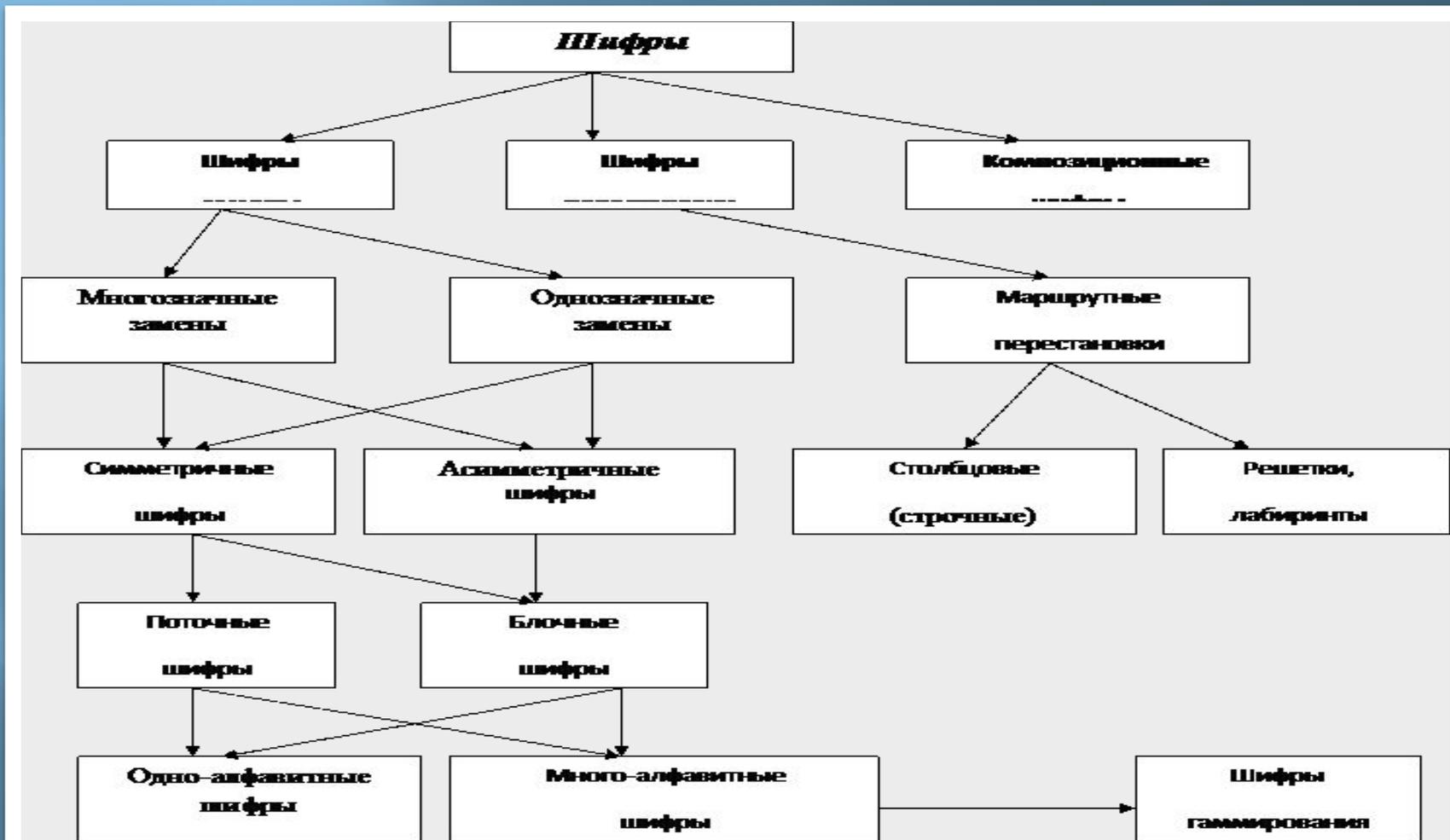


Рисунок 1 – Классификация шифров

Шифр замены – это шифр, в котором фрагменты открытого текста заменяются некоторыми их эквивалентами в шифротексте.

Если ключ шифрования совпадает с ключом расшифровывания, то такие шифры называют симметричными, если же ключи различны, то такие шифры называют асимметричными.

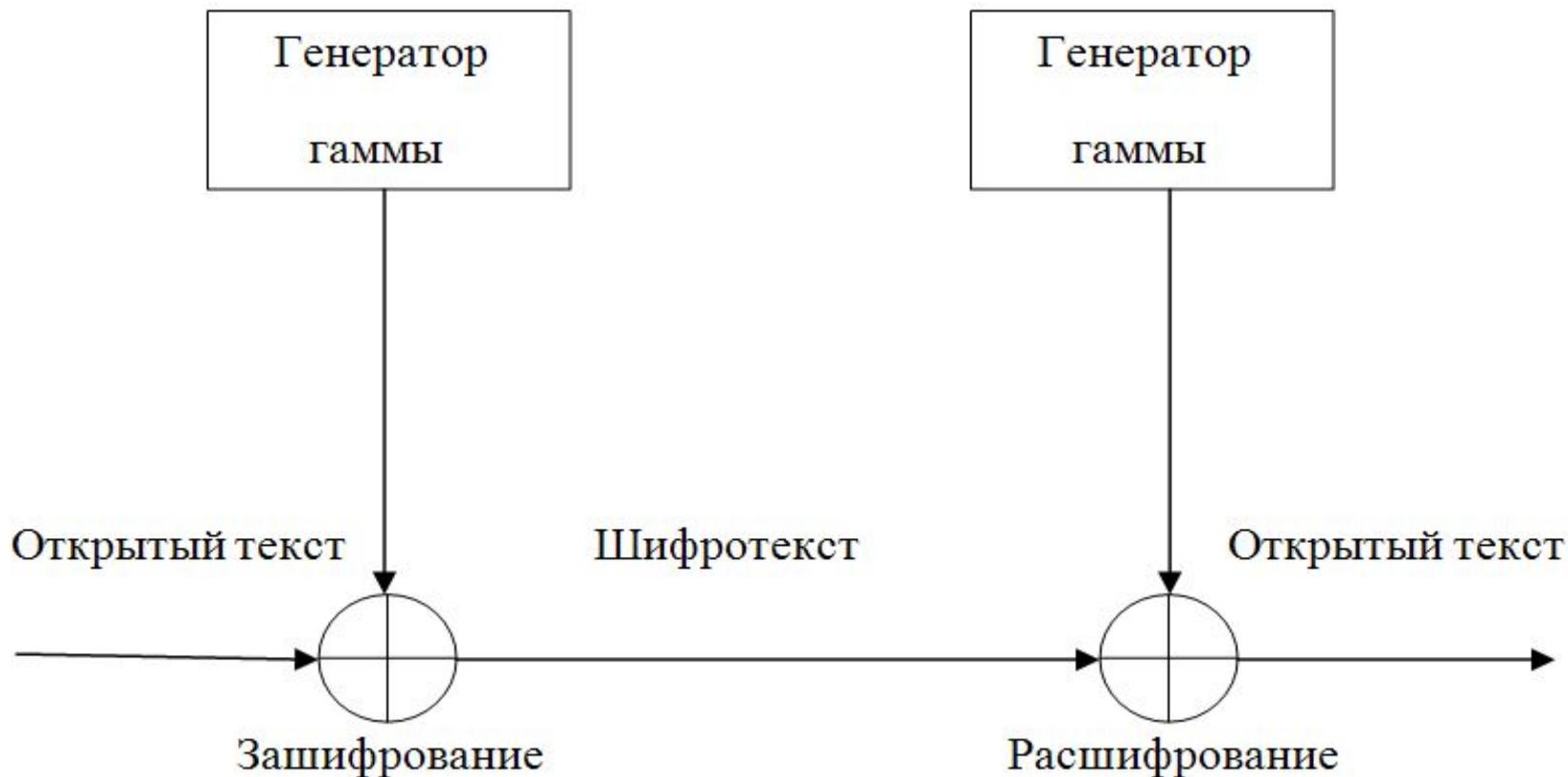
<b>A</b>	<b>B</b>	<b>C</b>
<b>D</b>	<b>E</b>	<b>F</b>
<b>G</b>	<b>H</b>	<b>I</b>

<b>J</b>	<b>K</b>	<b>L</b>
<b>M</b>	<b>N</b>	<b>O</b>
<b>P</b>	<b>Q</b>	<b>R</b>

	<b>S</b>	
<b>T</b>		<b>U</b>
	<b>V</b>	

	<b>W</b>	
<b>X</b>		<b>Y</b>
	<b>Z</b>	

Метод шифрования  
масонов



Шифр гаммирования - пример шифра однозначной замены со случайной равновероятной гаммой (гаммой принято называть последовательность чисел  $k_1 \dots k_n$ , складываемую по модулю с шифруемым сообщением).

Шифр перестановки – это шифр преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих (буквы открытого текста при шифровании лишь меняются местами друг с другом). Ключом шифра является перестановка номеров букв открытого текста.

П	Р	О	И	З
В	Е	Д	Е	Н
	З	А	П	У
С	К		С	П
У	Т	Н	И	К
А				
↓	↓	↓	↓	↓

Шифр перестановки  
"скитала"

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

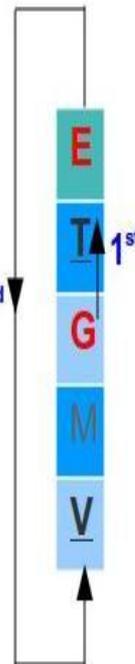


O → B



OQ → BN

2<sup>nd</sup>



G → T

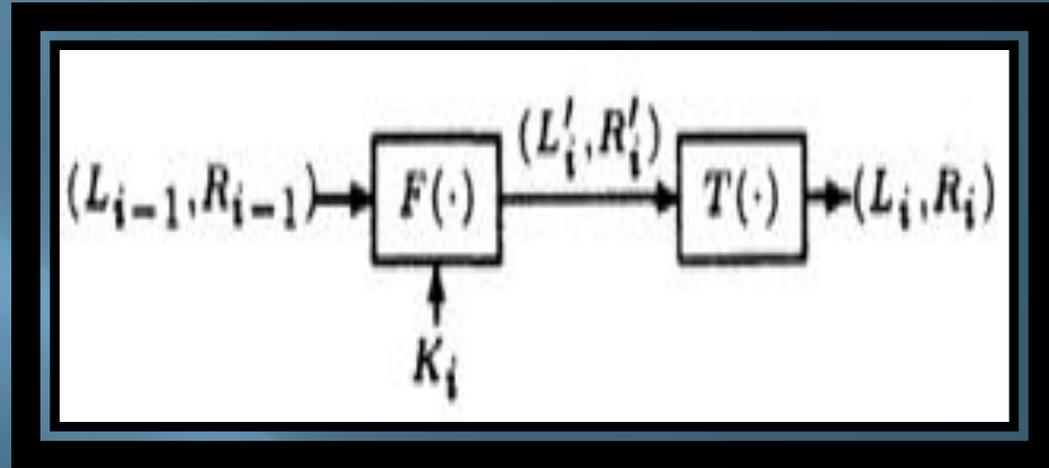


GE → TV

### Шифр Плейфера

Одной из разновидностей шифров простой замены являются *блочные шифры*. Простейший блочный шифр оперирует с биграммными шифровеличинами. Одним из первых таких шифров был биграммный шифр Порта и Плейфера.

Композиционный шифр — это всевозможные композиции различных шифров. То есть, с целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра.



# Основные требования к криптографическим системам

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений)
- знание алгоритма шифрования не должно влиять на надежность защиты
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при шифровании одного и того же исходного текста
- незначительное изменение исходного текста должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа
- структурные элементы алгоритма шифрования должны быть неизменными
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте
- длина шифрованного текста должна быть равной длине исходного текста
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования
- любой ключ из множества возможных должен обеспечивать надежную защиту информации
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования

# Заключение

Широкое применение компьютерных технологий и постоянное увеличение объема информационных потоков вызывает постоянный рост интереса к криптографии. Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.



The image shows a circular inset of a chalkboard filled with mathematical equations. In the center of the board is a large black padlock. The equations are written in white chalk and include:

$$(y f(2x) + 20(x^2)y_1 + e_2(x)y_2 + e_3(x)y_3)$$
$$(x+1) = \left(\frac{x(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right)$$
$$= \left(\frac{(x-1)(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right)$$
$$f(x,y)$$
$$(y+6x+3)^4 - (y^2+8x^2+8x)^2 + (y+9x+6)^4 (x+1)$$
$$1)(x+6)^4 (x+9)^4 \quad x(x+1)(x+2)^4$$
$$-9b + \sqrt{3} \sqrt{4a^3 + 27b^2} \sqrt{y^2 + 6x^2} (y+10x+8)^2 x+1$$
$$2^{1/3} 3^{2/3} \quad x(x+6)^2 \quad (y+9x+)$$
$$(y+8x)^2$$
$$(1-i\sqrt{3})(-9b + \sqrt{3} \sqrt{4a^3 + 27b^2})^{1/3} (y+8x+)$$
$$1/3 + \quad 2^{1/3} 3^{2/3} x+9$$
$$(y+8x)^2 (y+7x+4)^4 (y+)$$