МЕТОДЫ ШИФРОВАНИЯ.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ МЕТОДОВ ШИФРОВАНИЯ

Метод шифрования характеризуется показателями ***надежности*** и ***трудоемкости***.

Важнейшим показателем надежности криптографического закрытия информации является его ***стойкость*** - тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст.

Трудоемкость метода шифрования определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

КЛАССИФИКАЦИЯ ОСНОВНЫХ МЕТОДОВ ШИФРОВАНИЯ

- Замена (подстановка)
  - Простая (одноалфавитная)
  - Многоалфавитная одноконтурная обыкновенная.
  - Монофоническая замена.
  - Многоалфавитная многоконтурная
- Перестановка
  - Простая
  - Ключевая
  - Усложненная по таблицам
  - Усложненная по маршрутам
- Аналитическое преобразование
- Гаммирование

ШИФРЫ ЗАМЕНЫ

- *Шифрами замены* называются такие шифры, преобразования в которых приводят к замене каждого символа открытого сообщения на другие символы - *шифробозначения*, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения.
- Стойкость метода равна 20 - 30

РАССМОТРИМ ШИФР ПРОСТОЙ ЗАМЕНЫ, СООТВЕТСТВУЮЩИЙ ТАБЛИЦЕ:

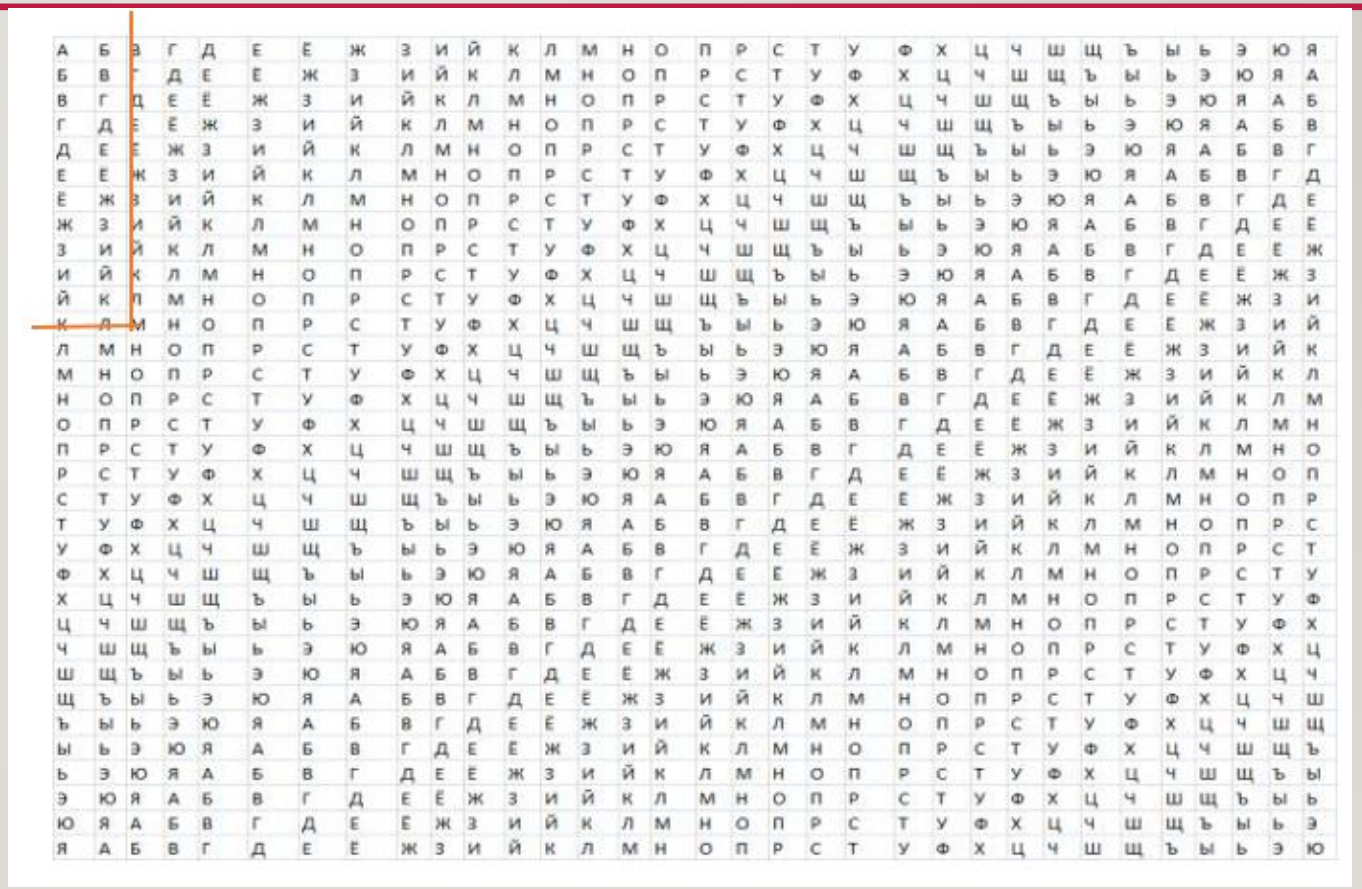
А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
11	98	33	42	19	13	87	54	43	49	48	50	69	32	73	18	81	29	76	74	22	31	90	59	67	77	91	12	52	45

В этом случае, например слово «ПОБЕДА» перейдет в

73 32 98 13 19 11

ПОЛИАЛФАВИТНАЯ ОДНОКОНТУРНАЯ, ОБЫКНОВЕННАЯ ПОДСТАНОВКА (ТАБЛИЦА ВИЖИНЕРА)

Ключ – ключ
Исходный текст – Вижинер
Зашифрованный текст – Мфеашро



Стойкость полиалфавитной подстановки оценивается величиной 20*n, где n - число различных алфавитов, используемых для замены.

ПРИМЕР ШИФРОВАНИЯ МЕТОДОМ КЛЮЧЕВОЙ ПЕРЕСТАНОВКИ

Зашифруем текст In this book the reader will …

блоком размером 4*8 и ключом 5-8-1-3-7-4-6-2.

В таблице пробелы заменены на символы подчеркивания.

Таблица простой перестановки

5	8	1	3	7	4	6	2
I	n	_	t	h	i	s	_
b	o	o	k	_	t	h	e
_	r	e	a	d	e	r	_
w	i	l	l	.	.	.	_

Зашифрованный текст будет иметь вид: _oel_e__tkalite.Ib_wshr.h_d.nori

ШИФР МАРШРУТНОЙ ПЕРЕСТАНОВКИ

Зашифруем, например, фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

используя прямоугольник размера 4×7:

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**

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

ШИФР ТАБЛИЧНОЙ ПЕРЕСТАНОВКИ

Зашифруем, например, фразу:

ПРИМЕР ТАБЛИЧНОЙ ПЕРЕСТАНОВКИ

используя прямоугольник размера 5×7:

П	Р	И	М	А	Е	Р
О	Т	А	Б	Л	Е	И
Ч	Н	О	С	Й	П	Е
Р	П	Е	С	Т	А	К
Н	О	В	О	К	А	И

Зашифрованная фраза выглядит так:

ПОЧРНРТНПОИАОЕВМБССОАЛЙТКЕЕПААРИЕКИ

ШИФРОВАНИЕ МЕТОДОМ ГАММИРОВАНИЯ

$$t_ш = t_0 \text{ XOR } t_г,$$

где $t_ш$, t_0, $t_г$ - ASCII коды соответственно зашифрованного символа, исходного символа и гаммы. XOR - побитовая операция "исключающее или". Расшифровка текста проводится по той же формуле:

$$t_0 = t_ш \text{XOR } t_г$$

СТОЙКОСТЬ ГАММИРОВАНИЯ

- все символы гаммы полностью случайны и появляются в гамме с равными вероятностями;
- длина гаммы равна длине открытого текста или превышает ее;
- каждый ключ (гамма) используется для шифрования только одного текста, а потом уничтожается.

ШИФРОВАНИЕ С ПОМОЩЬЮ АНАЛИТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В качестве односторонней функции можно использовать следующие преобразования:

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

МЕТОД УМНОЖЕНИЯ МАТРИЦ ИСПОЛЬЗУЕТ ПРЕОБРАЗОВАНИЕ ВИДА:

- Открытый текст: "ПРИКАЗ" ("17 18 10 12 01 09" согласно таблице алфавита).

Матрица С: $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 17 \\ 18 \\ 10 \end{pmatrix} = \begin{pmatrix} 91 \\ 102 \\ 97 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 12 \\ 01 \\ 09 \end{pmatrix} = \begin{pmatrix} 33 \\ 70 \\ 47 \end{pmatrix}$$

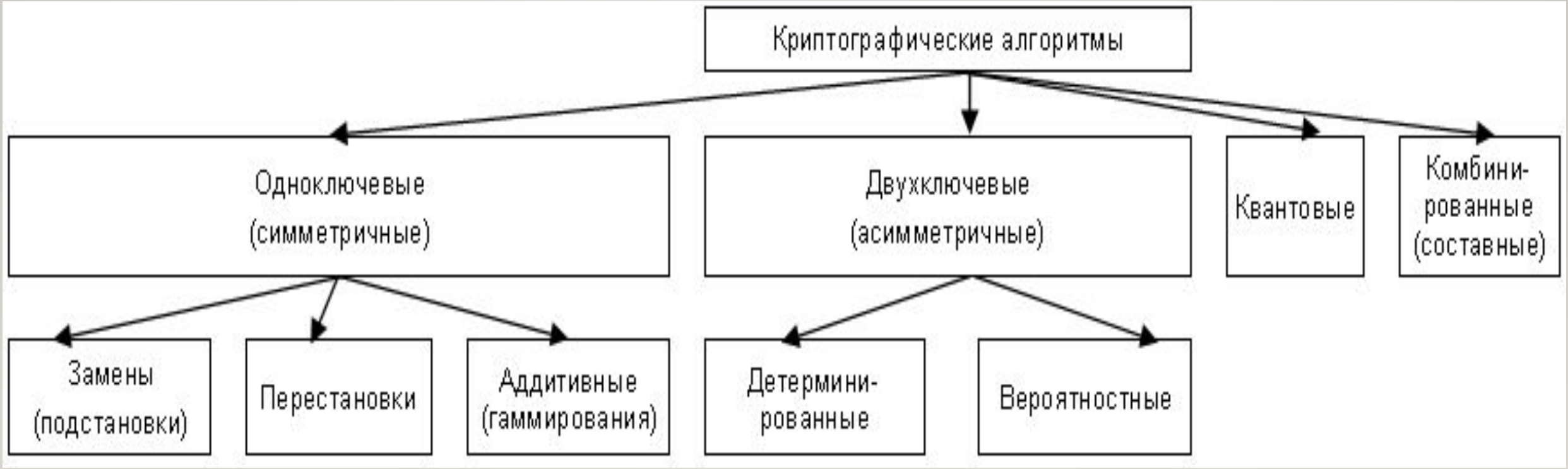
Шифтекст: «чвэягм».

КОМБИНИРОВАННЫЕ МЕТОДЫ ШИФРОВАНИЯ

Стойкость комбинированного шифрования S не ниже произведения стойкостей используемых способов $S >= S_1*S_2*...*S_k$

$R > R_1+R_2+ ... +R_k$, где R_i - **трудоемкость** i-го способа, используемого при комбинированном шифровании, R - трудоемкость того способа, который обеспечивает стойкость не ниже S.

- Подстановка + гаммирование
- Перестановка + гаммирование
- Гаммирование + гаммирование
- Подстановка + перестановка


Криптографические алгоритмы
Одноключевые (симметричные)
Двухключевые (асимметричные)
Квантовые
Комбини-рованные (составные)
Замены (подстановки)
Перестановки
Аддитивные (гаммирования)
Детермини-рованные
Вероятностные

КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ПО ОБЛАСТИ ПРИМЕНЕНИЯ:

- Криптосистемы ограниченного использования.
- Криптосистемы общего использования.

Стойкость **криптосистемы ограниченного использования** основывается на сохранении в секрете самого характера алгоритмов шифрования и дешифрования (безключевые системы).

Стойкость **криптосистемы общего использования** основывается на секретности ключа и сложности его подбора потенциальным противником.

КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ПО СТОЙКОСТИ ШИФРА:

- совершенные (абсолютно стойкие, теоретически стойкие) шифры – заведомо неподдающиеся к вскрытию (при правильном использовании). Шифры, для которых вскрытие шифрограммы приводит к нескольким осмысленным равновероятным открытым сообщениям;
- практически (вычислительно) стойкие шифры – допускающие вскрытие за приемлемое для противника время лишь при наличии вычислительных возможностей, которыми он не обладает на текущий момент или будет обладать в обозримом будущем. Практическая стойкость таких систем базируется на теории сложности и оценивается исключительно на какой-то определенный момент времени с двух позиций:

вычислительная сложность полного перебора;

известные на данный момент слабости (уязвимости) и их влияние на вычислительную сложность;

- нестойкие шифры.

ОСНОВНЫЕ ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К КРИПТОСИСТЕМАМ

- сложность и трудоёмкость процедур шифрования и дешифрования зависят от требуемого уровня защиты информации;
- временные и стоимостные затраты на защиту информации должны быть приемлемыми при заданном уровне ее секретности ;
- процедуры шифрования и дешифрования не должны зависеть от длины сообщения;
- количество всех возможных ключей шифра должно быть таковым, чтобы их полный перебор был невозможен за приемлемое для противника время;
- любой ключ из множества возможных, должен обеспечивать надежную защиту информации;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;
- избыточность сообщений должна быть как можно меньшей;
- зашифрованное сообщение должно поддаваться чтению только при наличии ключа.