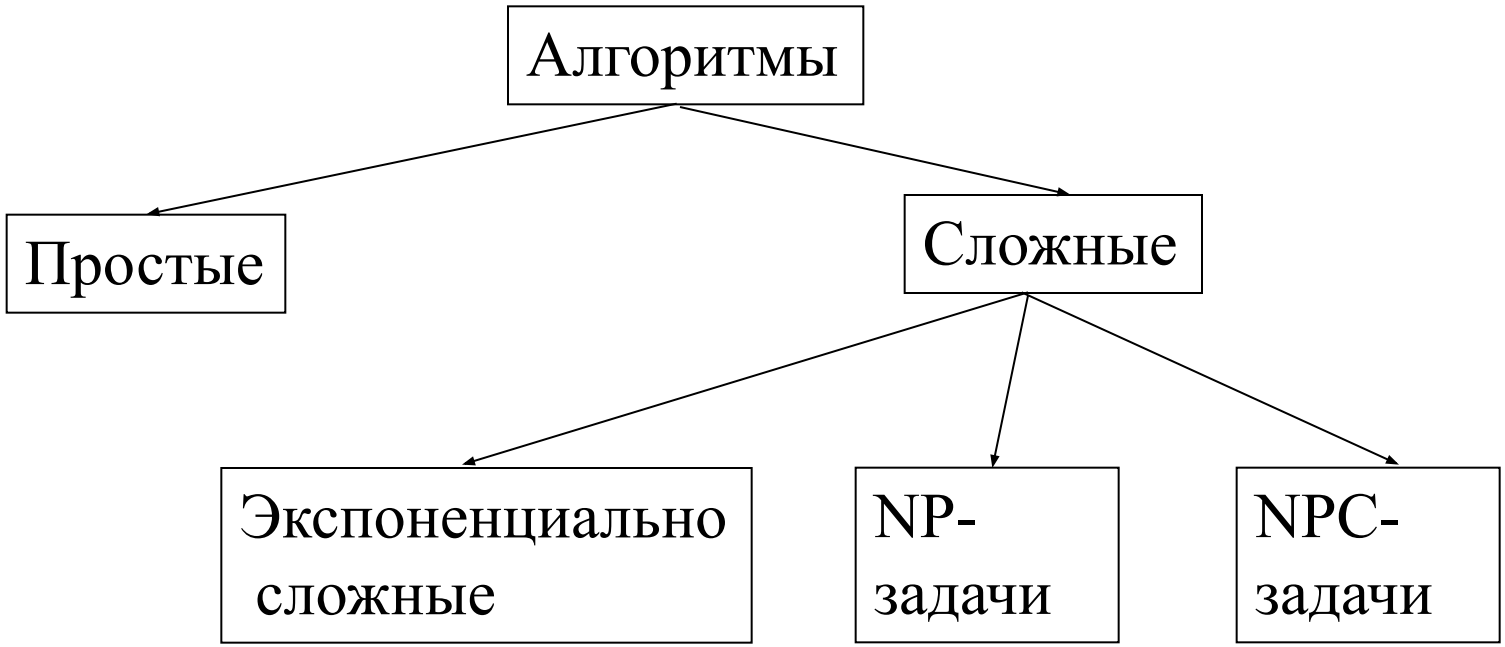
Лекция 3
Вычислительно стойкие системы шифрования
Способы шифрования и их анализ

Вычислительно стойкие системы шифрования

Система шифрования называется **вычислительно стойкой** (ВССШ), если вскрытие такой системы возможно, но даже наилучший алгоритм вскрытия требует необозримо большого времени или необозримо большой памяти устройств, с помощью которых проводится криптоанализ

Время криптоанализа определяется:
-Сложностью алгоритма дешифрования;
-Быстродействием вычислительных устройств, осуществляющих дешифрование

Элементы теории сложности алгоритмов



Простые алгоритмы – это задачи полиномиальной сложности

$N_{опер}$=polynom(n), $N=k_1n^d+k_2n^{d-1}+k_1n^{d-2}….n$

Простые алгоритмы – это задачи полиномиальной сложности

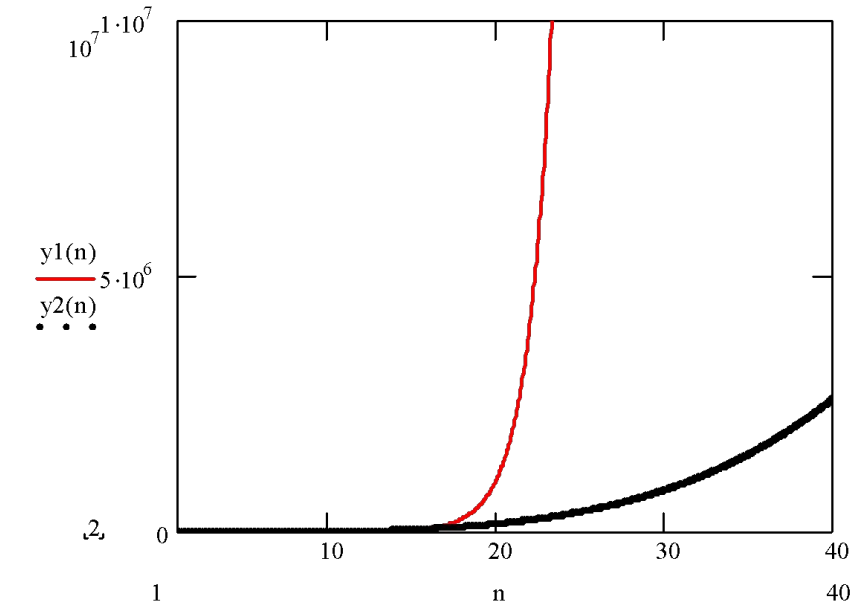
$N_{опер}$=polynom(n), $N=k_1n^d+k_2n^{d-1}+k_1n^{d-2}….n$

Сложные алгоритмы- это задачи экспоненциальной сложности

$N_{опер}=a^{kn}$, a,k>0

NP-задачи (недетерминистско полиномиальные) это такие задачи для которых пока не известны алгоритмы решения с полиномиальной сложностью, однако если решение найдено, то проверка его правильности – задача полиномиальной сложности

Пример оценки сложности решения полиномиальной и экспоненциальной задач



$$y1(n) := 2^n$$

$$y2(n) := n^4 + n^3 + n$$

Сложность алгоритмов криптоанализа должна соответствовать
сложности решения сложной задачи

Сложность алгоритмов криптоанализа должна соответствовать
сложности решения сложной задачи

Основные подходы к криптоанализу:

1. Тотальный перебор ключей
2. Анализ статистических особенностей криптограмм
3. Линейный криптоанализ
4. Дифференциальный криптоанализ
5. Другие

Быстродействие вычислительных устройств 10^{10}- 10^{12} операций/с

Быстродействие ЭВМ увеличивается в 4 раза каждые 3 года

Оценка времени тотального перебора ключей

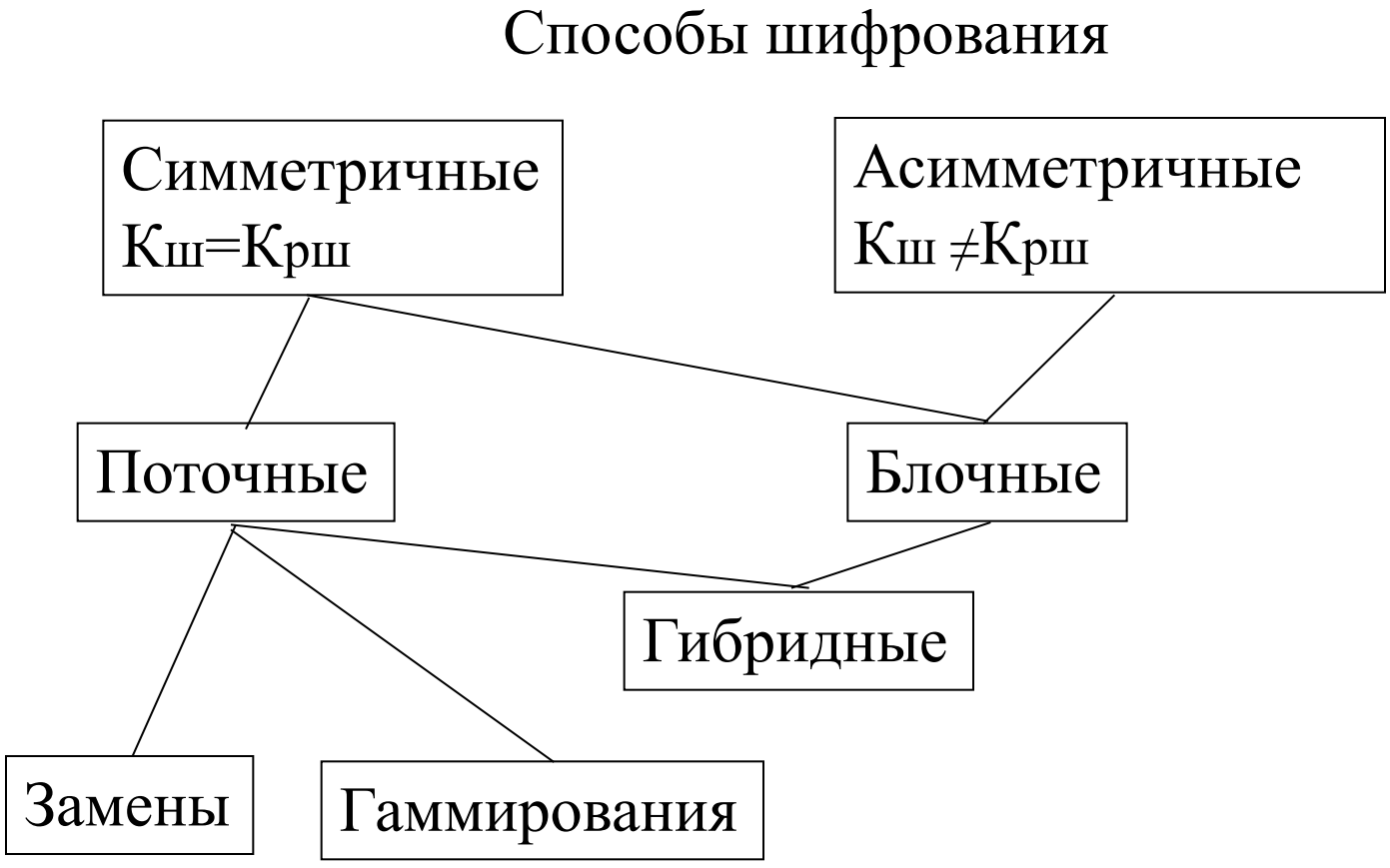
- Симметричные ключи N=64-256 ,бит
- Асимметричные ключи N=1024 бит

При N=256 бит $S_k = 2^{256} = 1.18*10^{77}$
Время полного перебора $Tп=S_k/V$,
Если $V=10^9$ ключей в секунду, то $Tп =10^{68}$ сек =
$=3.3*10^{60}$ лет!

В году $3.1536*10^7$ секунд

Способы шифрования и их анализ

Классификация способов шифрования



Шифр гаммирования

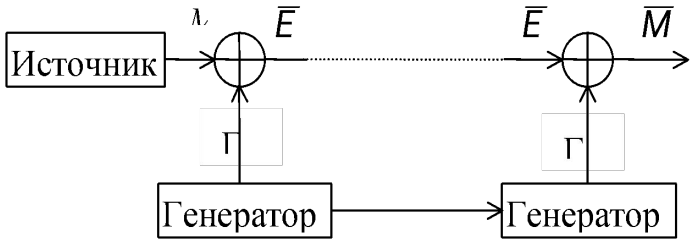
ШИФР ГАММИРОВАНИЯ:
(модуль *m*)

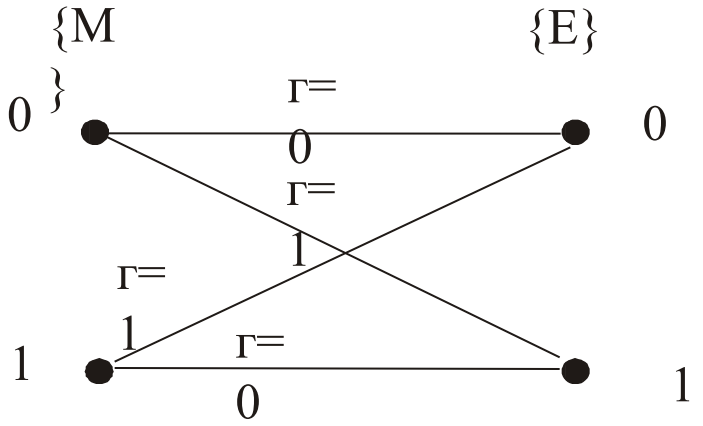
$$E = M + \Gamma (\mathrm{mod}\, m)$$
$$M = E - \Gamma (\mathrm{mod}\, m).$$

ШИФР ГАММИРОВАНИЯ:
(модуль *2*)

$$E = M \oplus \Gamma$$
$$M = E \oplus \Gamma.$$

0+0=0
0+1=1
1+0=1
1+1=0





Нумерация символов русского алфавита

Пробел	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь, Ъ	Ы	Э	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Примеры шифрования гаммированием

- Исходный текст: ***файл*** → 21 1 10 12
- Гамма: → + 25 3 27 6
- Криптограмма: ***нгдс*** ← 14 4 5 18
- Гамма → - 25 3 27 6

- -11 1 -22 12
- Расшифров. текст: ***файл*** ← 21 1 10 12

+

Свойства шифра гаммирования

1. **Если все элементы гаммы равновероятны и взаимонезависимы, то система шифрования, использующая этот способ, будет абсолютно стойкой.**
2. **Операции зашифрования, расшифрования просты в реализации.**
3. **При шифровании информации способом гаммирования не происходит размножение ошибок при расшифровании криптограммы, из-за помех возникающих в канале связи.**
4. **Использование одного и того же отрезка гаммы для шифрования различных сообщений, называемое в криптографии *перекрытием шифра*, приводит к возможности простого дешифрования сообщений без знания ключа.**
5. **Способ требует синхронизации гамм на передаче и приеме.**

Повторное использование гаммы не допустимо

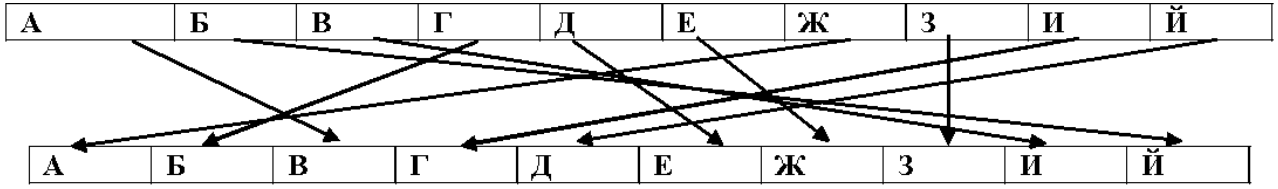
Пусть E_1^n **и** E_2^n **две криптограммы, следующего вида**

$$E_1^n = M_1^n \oplus \Gamma\,, \quad E_2^n = M_2^m \oplus \Gamma\,.$$

Сложим их поэлементно по модулю два

$$E_1^n \oplus E_2^n = M_1^n \oplus \Gamma \oplus M_2^m \oplus \Gamma = M_1^n \oplus M_2^n\,.$$

Шифр замены



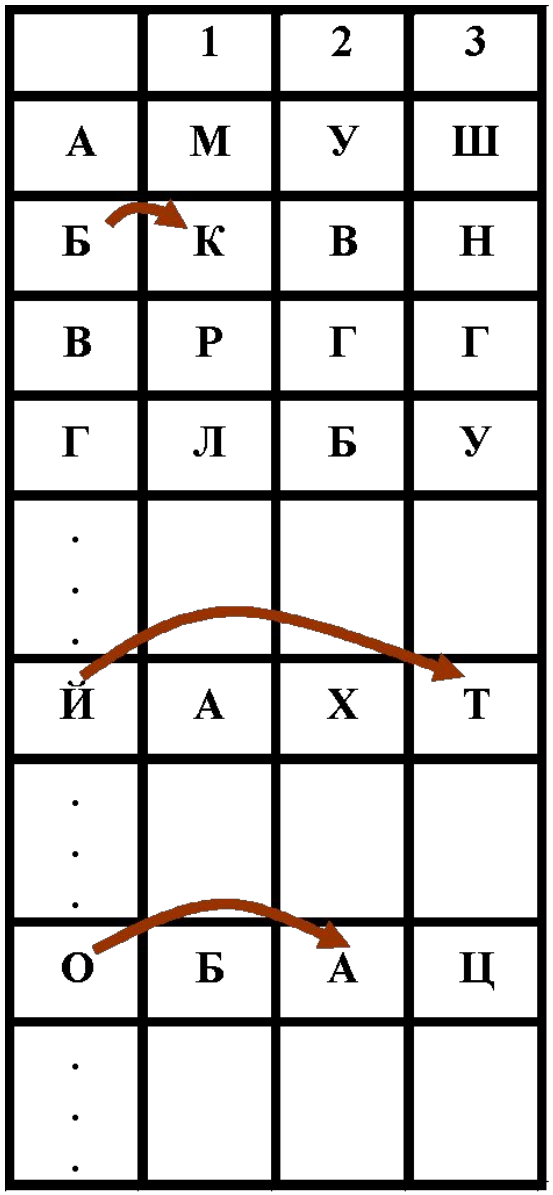
ДАВАЙ ⟶ **ЕВИВД**

Число возможных замен $S_k=m(m-1)(m-2)\cdots 1=m!$

$$S_k=32!=2{,}63\ 10^{35}$$

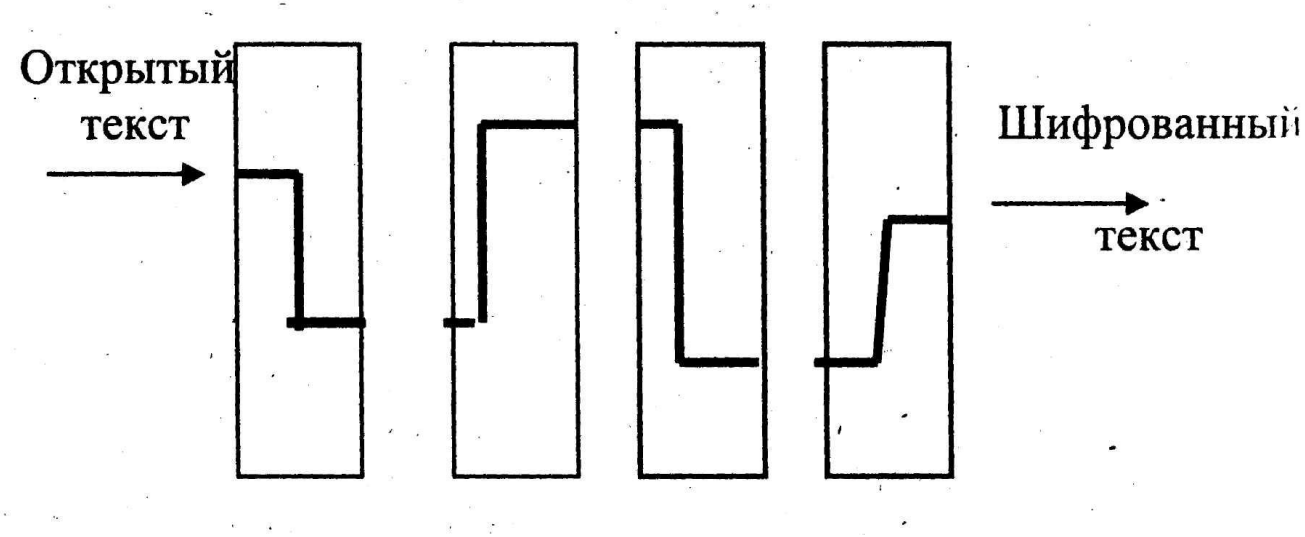
Если каждую секунде перебирать 10^6 ключей, то для перебора всех ключей понадобится $8{,}3\cdot 10^{21}$ лет.

Шифр колонной замены

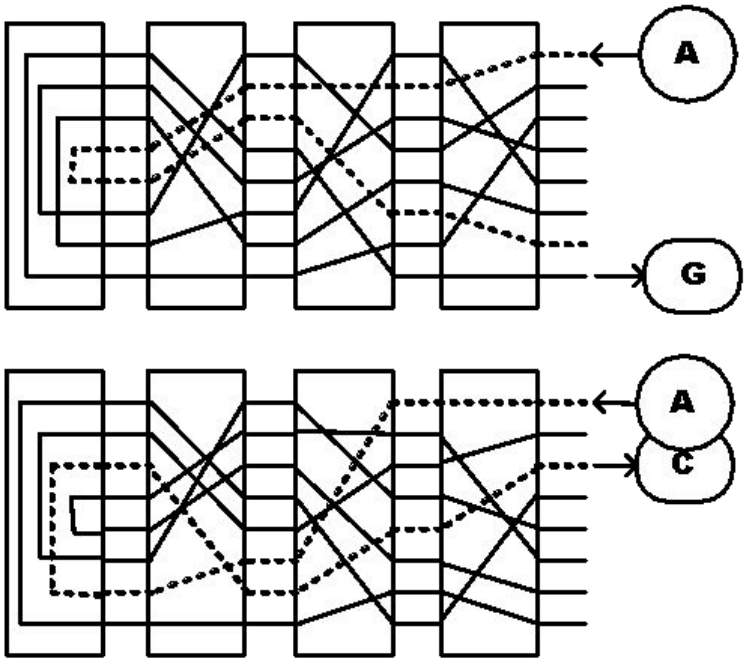


Б О Й → К А Т

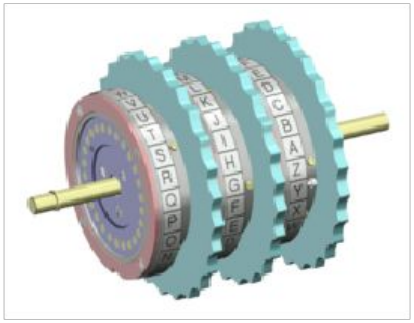
Реализация шифра замены

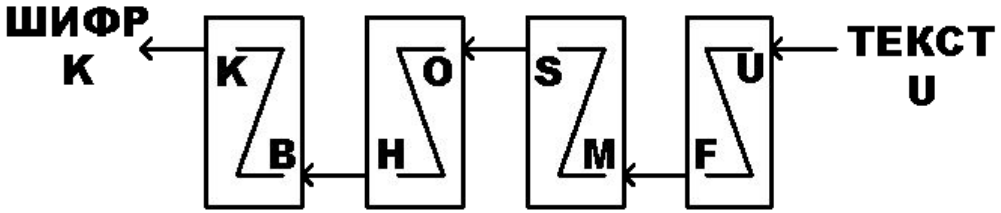


ПРИНЦИП РАБОТЫ ШИФРОВАЛЬНОЙ МАШИНЫ ЭНИГМА



Энигма вначале представляла собой четыре вращающихся на одной оси барабана, что обеспечивало более миллиона вариантов шифра простой замены, которые определялись текущим положением барабанов. На каждой стороне барабана по окружности располагались 25 электрических контактов (сколько букв в алфавите). Контакты с обеих сторон барабана соединялись попарно случайным образом 25 проводами, формировавшими замену символов. Колеса складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет колес. Перед началом работы барабаны поворачивались так, чтобы устанавливалось заданное кодовое слово - ключ. При нажатии клавиши и кодировании очередного символа правый барабан поворачивался на один шаг. После того, как барабан делал полный оборот, на один шаг поворачивался следующий барабан (как в счетчике электроэнергии). Таким образом получался ключ заведомо гораздо более длинный, чем текст сообщения.





Свойства шифра замены

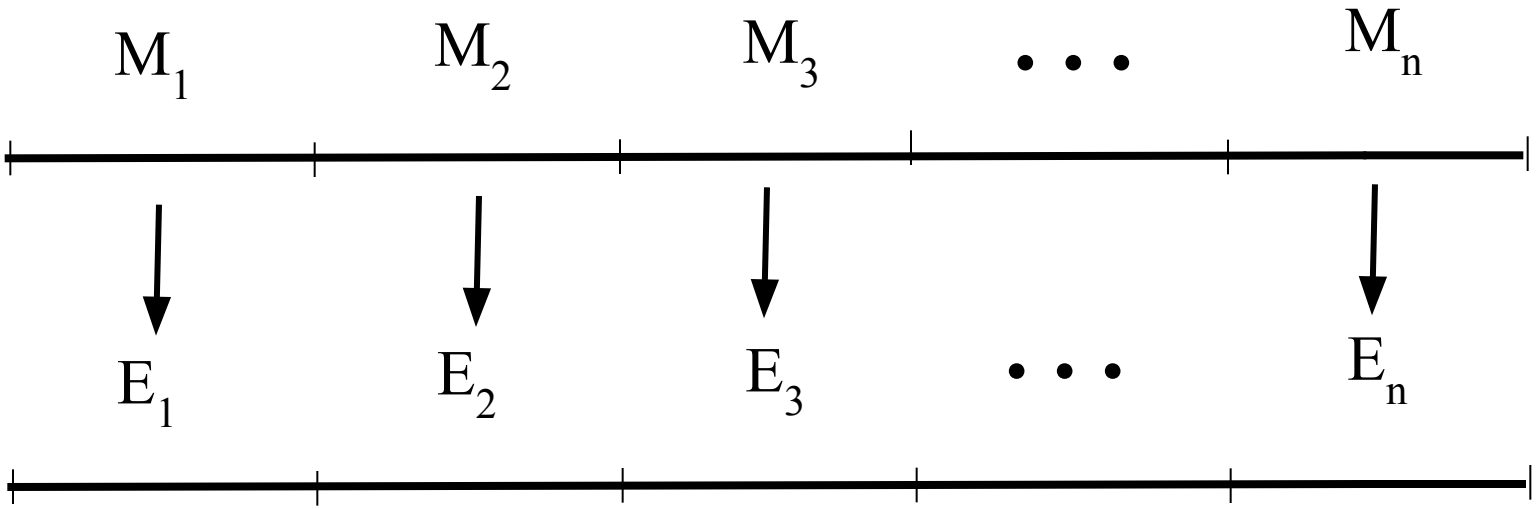
1. **Если все замены в таблице замен равновероятны и взаимонезависимы, то система шифрования, использующая данный способ, будет абсолютно стойкой.**

2. В отличие от способа гаммирования, реализация данного способа шифрования более сложна, что определяется необходимостью построения управляемого узла перестановки с m выходами.

3. При шифровании методом замены не происходит размножение ошибок, возникающих в канале связи из-за помех.

4. Перекрытие шифра, т е. шифрование одной и той же таблицей разных сообщений, не приводит к простому и однозначному дешифрованию, как в способе гаммирования. Однако стойкость способа снижается, т. к. повторяющиеся замены дают возможность проведения криптоанализа на основе частот повторения букв криптограммы.

Принцип блочного шифрования



Блочные шифры: схема Фейстеля

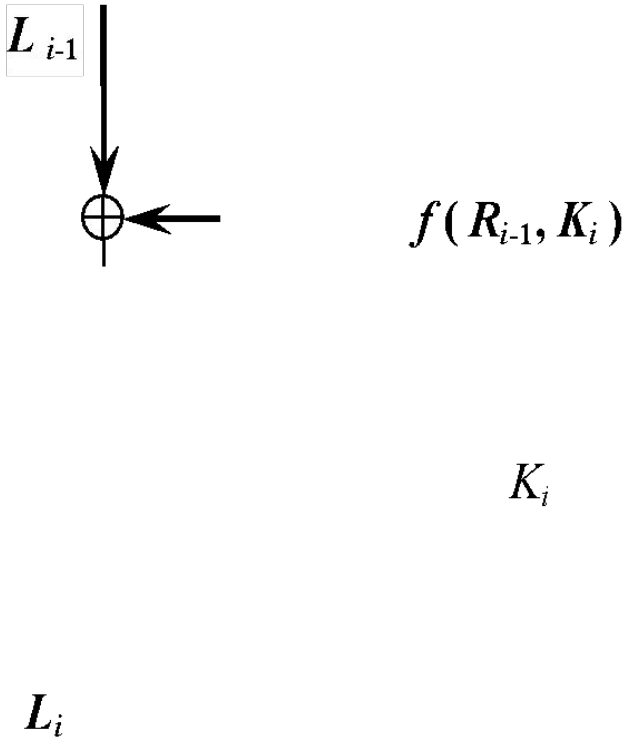


Схема одной итерации шифрования блочного шифра

Блочные шифры: схема Фейстеля

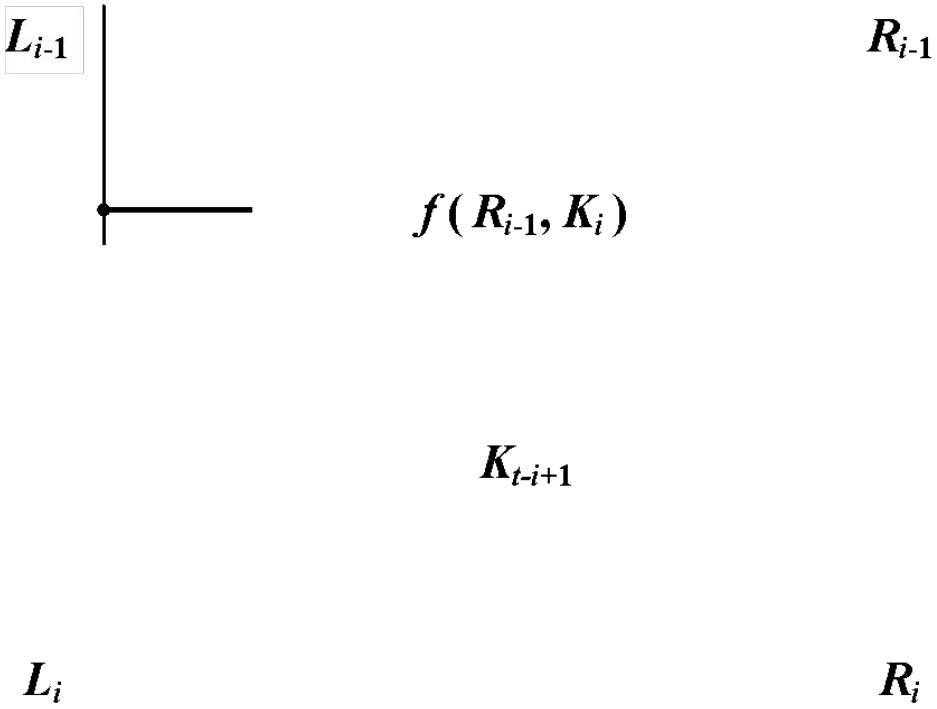


Схема одной итерации расшифрования

Свойства блочного шифра

- **1. Абсолютная стойкость шифрования недостижима, т.к. на одном ключе шифруется несколько блоков, при этом необходимые и достаточные условия АССШ не выполняются.**
- **2. Реализация блочных шифров на современном уровне развития элементной базы и вычислительной техники не представляет больших трудностей и может быть осуществлена как программным, так и аппаратным путем.**
- **3. Характерное свойство блочных шифров - размножение ошибок, возникающих в канале связи, что является следствием нелинейности используемого преобразования и влиянием каждого символа криптограмм на все символы блока сообщения**
- **4. Перекрытие шифра имеет место, однако криптоанализ затруднен ввиду большой длины блока. Статистические связи между блоками практически отсутствуют, что не позволяет эффективно использовать криптоанализ на основе частот повторения блоков.**
- **5. Нет необходимости в передаче специальной синхро-последовательности для синхронизации шифраторов. Для синхронизации достаточна лишь цикловая синхронизация передаваемых блоков.**

Статистика букв русского языка

пробел **0.175**	**О** **0.090**	**Е,Ё** **0.072**	**А** **0.062**
И **0.062**	**Т** **0.053**	**Н** **0.053**	**С** **0.045**
Р **0.040**	**В** **0.038**	**Л** **0.035**	**К** **0.028**
М **0.026**	**Д** **0.025**	**П** **0.023**	**У** **0.021**
Я **0.018**	**Ы** **0.016**	**З** **0.016**	**Ь,Ъ** **0.014**
Б **0.014**	**Г** **0.013**	**Ч** **0.012**	**Й** **0.010**
Х **0.009**	**Ж** **0.007**	**Ю** **0.006**	**Ш** **0.006**
Ц **0.004**	**Щ** **0.003**	**Э** **0.003**	**Ф** **0.002**

Блочные шифры

Наименование шифра	Год	Длина ключа	Схема
DES	1975	56	F
FEAL	1978	64	F
ГОСТ 28147-89	1989	256	F
IDEA	1991	128	
BLOWFISH	1993	32-448	F
RC5 (RC6)	1994	255	
AES	2000	128-256	