Криптографические средства защиты объектов информатизации

Часть 1 Симметричные системы шифрования

Основные особенности функционирования систем обработки информации в корпоративных сетях

- Территориальная распределенность систем
- Непосредственный доступ к вычислительным и информационным ресурсам большого числа различных категорий пользователей
- Наличие большого числа каналов взаимодействия со сторонними организациями
- Непрерывность функционирования систем, высокая интенсивность информационных потоков
- Наличие ярко выраженных функциональных подсистем с различными требованиями по уровням защищенности

В связи с этим необходимо внедрение следующих технологий:

- аутентификация пользователей
- обеспечение конфиденциальности информации
- подтверждение авторства и целостности электронных документов
- обеспечение невозможности отказа от совершенных действий
- защита от повторов
- обеспечение юридической значимости электронных документов

Применение криптографических методов обеспечивает:

- Конфиденциальность - информация должна быть защищена от несанкционированного прочтения как при хранении, так и при передаче.
- Контроль доступа - информация должна быть доступна только для того, для кого она предназначена.
- Аутентификация - возможность однозначно идентифицировать отправителя.
- Целостность - информация должна быть защищена от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость - отправитель не может отказаться от совершенного действия.

Достоинства и недостатки криптографических методов

Достоинство:

- **высокая гарантированная стойкость защиты**

Недостатки:

- **значительные затраты ресурсов**
- **трудности совместного использования зашифрованной (подписанной) информации**
- **требования к сохранности секретных ключей и защиты открытых ключей от подмены**

Немного из истории развития криптографии

- I-Эра донаучной криптографии
- II- 1949 г. основан на работе американского ученого Клода Шеннона «Теория связи в секретных системах»
- III-1976 г. Связан с появлением работы У.Диффи и М. Хеллмана «Новые направления в криптографии»

Шифр перестановки
Скиталь (V век до н.э.)

Шифры простой замены. Шифр сдвига Цезаря (56г. н.э.)

, _ А Б В Г Д Е Ж … Э Ю Я
Б В Г Д Е Ж … , _ А

Небо синее, трава зеленая.

Ридсвфлриив хугег киоиргав

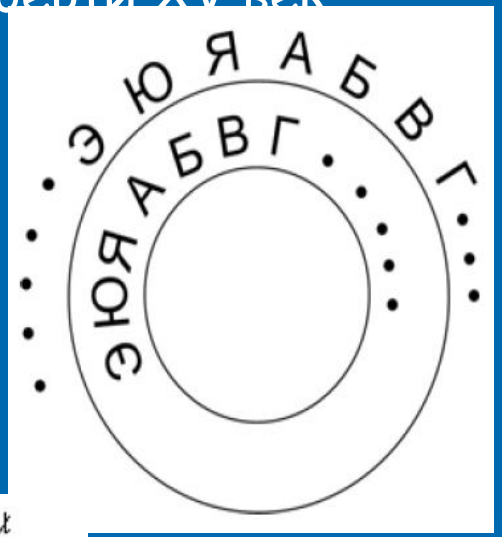
Шифр сдвига: количество возможных вариантов равно длине алфавита - n
Шифр простой замены: n!

Другие разновидности шифров замены и перестановки

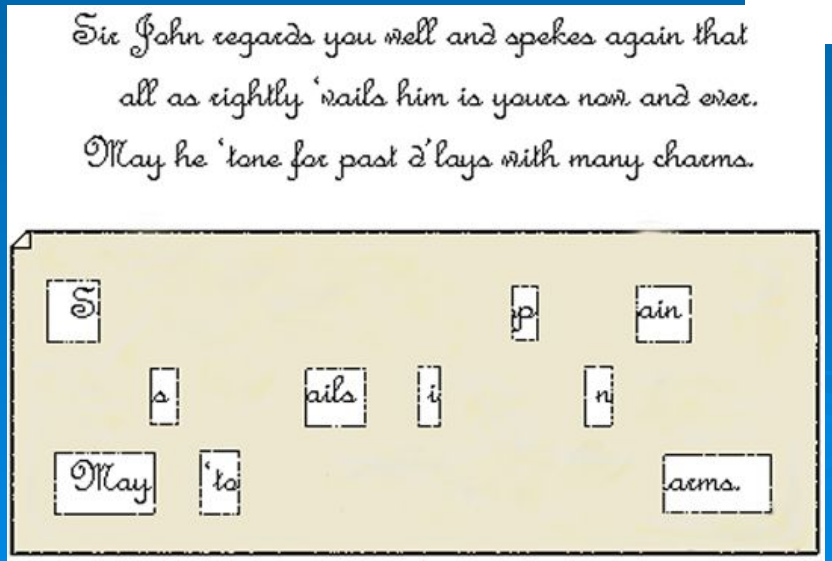
Квадрат Полибия

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	J	K
3	L	M	N	O	P
4	*Q*	*R*	*S*	*T*	*U*
5	*V*	*W*	*X*	*Y*	*Z*

Альберти XV век



Решетка Кордано



Шифр сдвига и теория чисел

	,		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Mi	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Mi	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Шифруемый текст:	Н	Е	Б	О		С	И	Н	Е	Е
Mi	15	7	3	16	1	19	10	15	7	7
Ключ:	Б	Б	Б	Б	Б	Б	Б	Б	Б	Б
Ki	3	3	3	3	3	3	3	3	3	3
Ei=(Mi+Ki) mod 34	18	10	6	19	4	22	13	18	10	10
Зашифрованный текст:	Р	И	Д	С	В	Ф	Л	Р	И	И

Расшифрование

Зашифрованный текст:	Р	И	Д	С	В	Ф	Л	Р	И	И
Ei	18	10	6	19	4	22	13	18	10	10
Ключ:	Б	Б	Б	Б	Б	Б	Б	Б	Б	Б
Ki	3	3	3	3	3	3	3	3	3	3
Mi=(Ei-Ki) mod 34	15	7	3	16	1	19	10	15	7	7
Расшифрованный текст:	Н	Е	Б	О		С	И	Н	Е	Е

Взлом шифра сдвига

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
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
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
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

ЕМКЕКАДЖ - ?

Среднестатистические частоты употребления русских букв

Буква	Процентное содержание	Буква	Процентное содержание	Буква	Процентное содержание
а	6,2	л	3,5	ц	0,4
б	1,4	м	2,6	ч	1,2
в	3,8	н	5,3	ш	0,6
г	1,3	о	9,0	щ	0,3
д	2,5	п	2,3	ы	1,6
е,ё	7,2	р	4,0	ъ,ь	1,4
ж	0,7	с	4,5	э	0,3
з	1,6	т	5,3	ю	0,6
и	6,2	у	2,1	я	1,8
й	1,0	ф	0,2		
к	2,8	х	0,2		

Шифр Вижинера- многоалфавитный

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

Шифрование

Шифруемый текст:	Н	Е	Б	О		С	И	Н	Е	Е
Ключ:	М	О	Р	Е	М	О	Р	Е	М	О
Зашифрованный текст:	Ы	Х	У	Х	Н		Ъ	Ф	У	Х

Шифр Вижинера - математическая модификация

	,		А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Mi	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Mi	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Шифруемый текст:	Н	Е	Б	О		С	И	Н	Е	Е
Mi	15	7	3	16	1	19	10	15	7	7
Ключ:	М	О	Р	Е	М	О	Р	Е	М	О
Ki	14	16	18	7	14	16	18	7	14	16
Ei=(Mi+Ki) mod 34	29	23	21	23	15	1	28	22	21	23
Зашифрованный текст:	Ы	Х	У	Х	Н		Ъ	Ф	У	Х

Расшифрование

Шифруемый текст:	Ы	Х	У	Х	Н		Ъ	Ф	У	Х
Ei	29	23	21	23	15	1	28	22	21	23
Ключ:	М	О	Р	Е	М	О	Р	Е	М	О
Ki	14	16	18	7	14	16	18	7	14	16
Mi=(Ei-Ki) mod 34	15	7	3	16	1	19	10	15	7	7
Зашифрованный текст:	Н	Е	Б	О		С	И	Н	Е	Е

Шифр перестановок

- Представить шифр в числовой форме
- Разбить на t блоков
- Каждый блок переставить с помощью матрицы перестановок $e=P*m$
- $m=P^{-1}e \quad (P*P^{-1}=E)$

Пример шифра перестановок

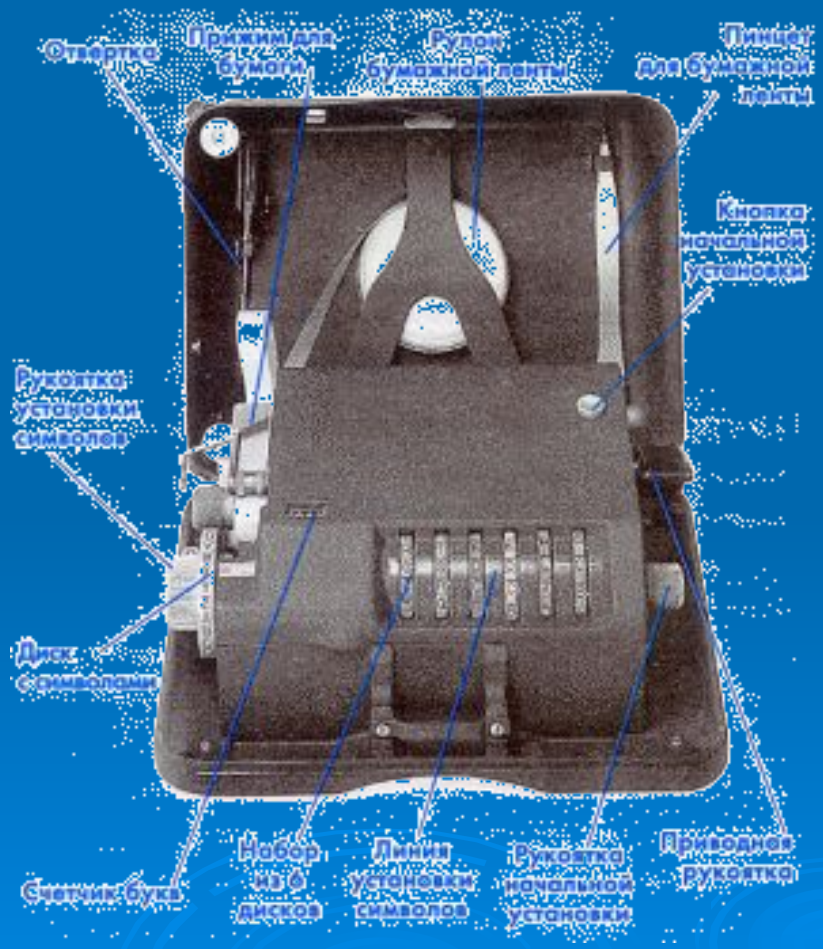
НЕБО СИНЕЕ 15 7 3 16 1 | 19 10 15 7 7

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 15 \\ 7 \\ 3 \\ 16 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \\ 7 \\ 1 \\ 16 \end{pmatrix} \rightarrow БНЕ\_О$$

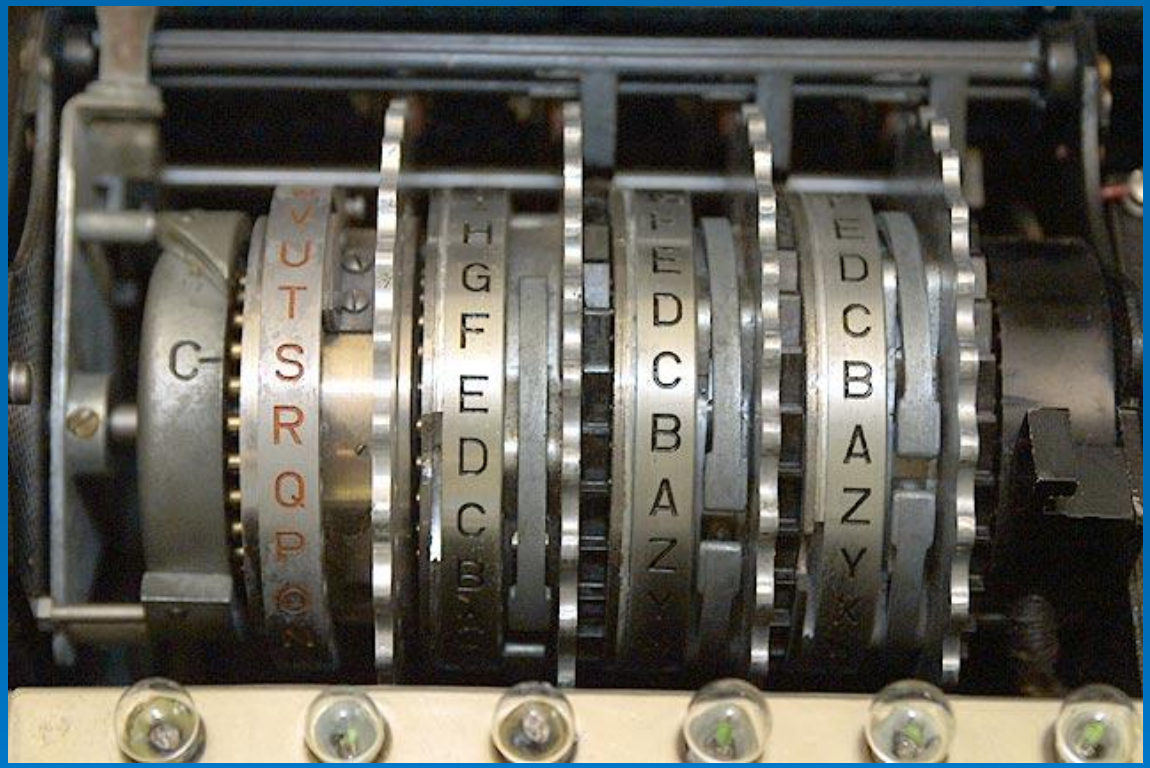
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 19 \\ 10 \\ 15 \\ 7 \\ 7 \end{pmatrix} = \begin{pmatrix} 15 \\ 19 \\ 10 \\ 7 \\ 7 \end{pmatrix} \rightarrow НСИЕЕ$$

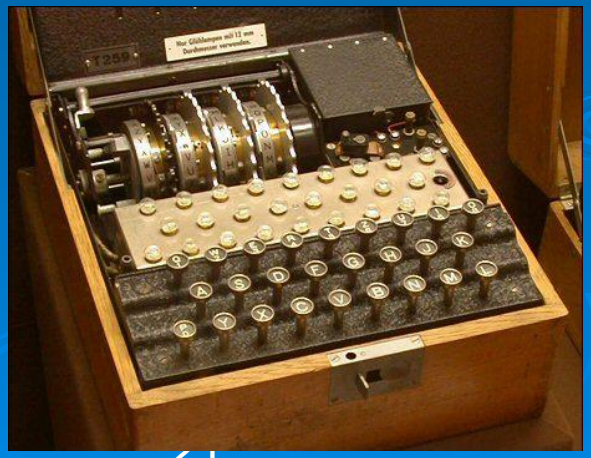
НЕБО СИНЕЕ БНЕ ОНСИЕЕ

Машина Хагелина



Роторные машины и «Энигма» (1920г.)





Одноразовый шифр-блокнот - шифр Вернама

- Текст представляется в двоичной форме mi
- Ключ ki состоит из того же количества двоичных знаков что и текст
- Каждый бит шифруемой строки mi складывается по модулю 2 (xor) с соответствующим знаком ключа ki.

$$Ci = mi \oplus ki$$

Гаммирование

- В качестве ключа используется случайная (псевдослучайная) последовательность, в которой отсутствует закономерность и очень большая длина.
- Ключевая последовательность накладывается на шифруемую информацию сложением по модулю, равному длине алфавита

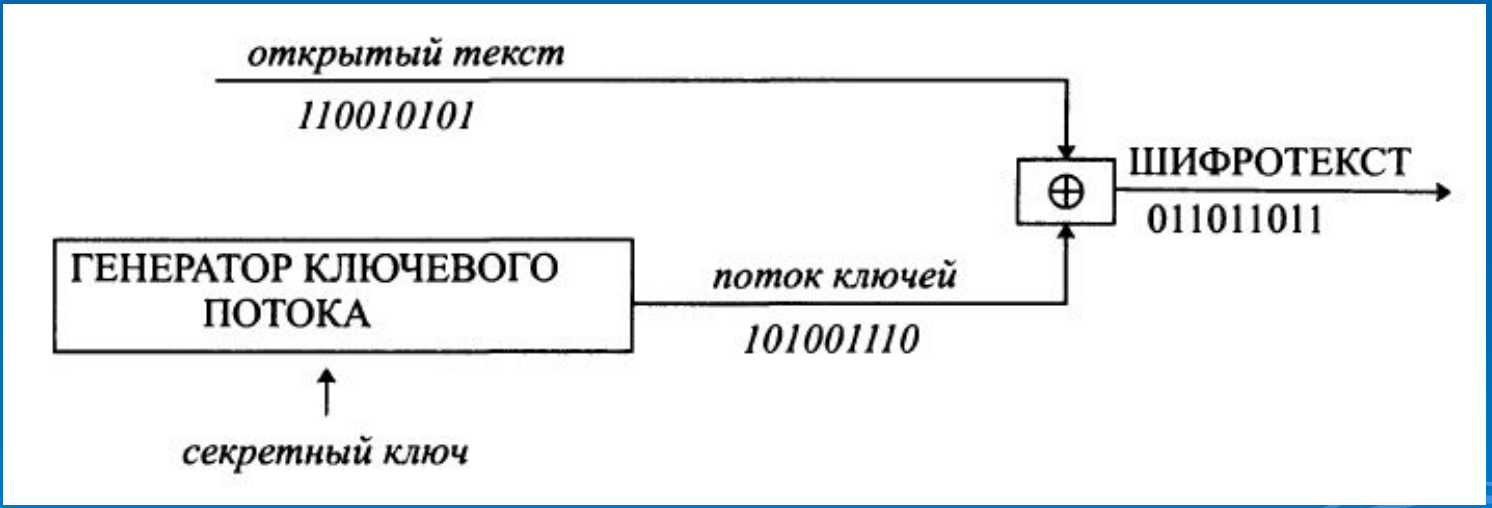
Гаммирование

- $L=m+\gamma \bmod p$
- m-вектор бит шифруемой информации
- γ – ключевая последовательность-гамма
- L – зашифрованная информация

Современные алгоритмы шифрования

Поточные системы шифрования

- Поточные системы – открытый текст разбивается на буквы или биты mi, каждый знак зашифровывается соответствующим ключевым символом ki



$$mi = Ci \oplus ki \qquad Ci = mi \oplus ki$$

$\oplus$ - Побитовое сложение по модулю 2

Поточные шифры

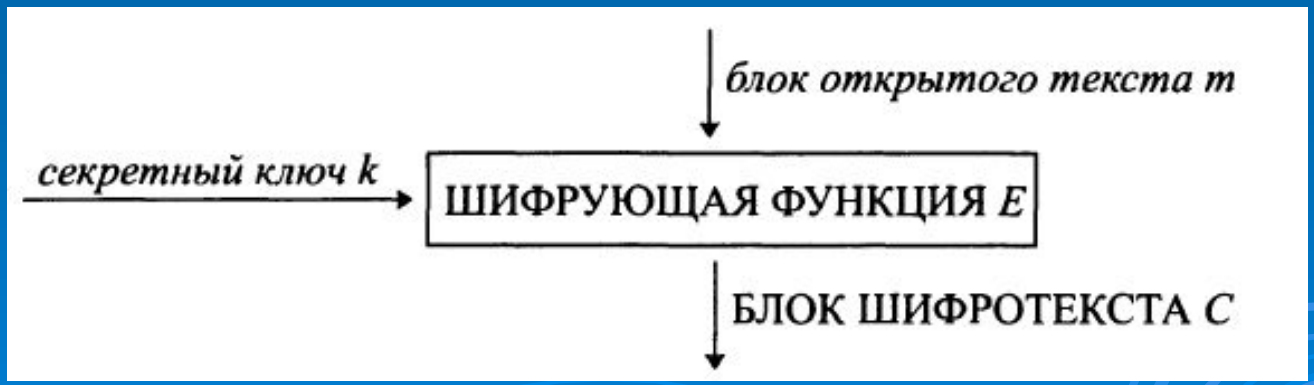
- РСЛОС (регистр сдвига с линейной обратной связью)
- SEAL
- RC4 (Ron’s Cipher)
- A5
- ORIX
- PIKE
- CHAMELEON
- И др.

аналог RC4

- Для генерации ключа используется S блок размером 8x8 – S_0, S_1.. S_{255}.
- Элементы S – перестановка чисел от 0 до 255
- 1) S-блок заполняется по правилу: $S_0 = 0$, $S_1 = 1$, …, $S_{255} = 255$.
- 2) ключ записывается в массив: K_0, K_1, …, K_{255}.
- 3) при начальном значении j = 0 в цикле выполняются:
- Для i = 0 до 255 выполнить j =(j+S[i]+K[i]) mod 256
- 4) Поменять местами S[i] и S[j].
- 5) Для генерации случайного байта выполняются следующие вычисления:
  - 5.1 i = (i + 1) mod 256
  - 5.2 j = (j + S[i]) mod 256
  - 5.3 Поменять местами S[i] и S[j]
  - 5.4 t = (S[i] + S[j]) mod 256
  - 5.5 K[i] = S[t]
- 6) C[i]:=(m[i] + k[i]) mod 2

Блочные системы шифрования

- информация разбивается на блоки фиксированной длины m, каждый блок шифруется отдельно обратимой функцией E_k (k - ключ), $D_k=E_k^{-1}$

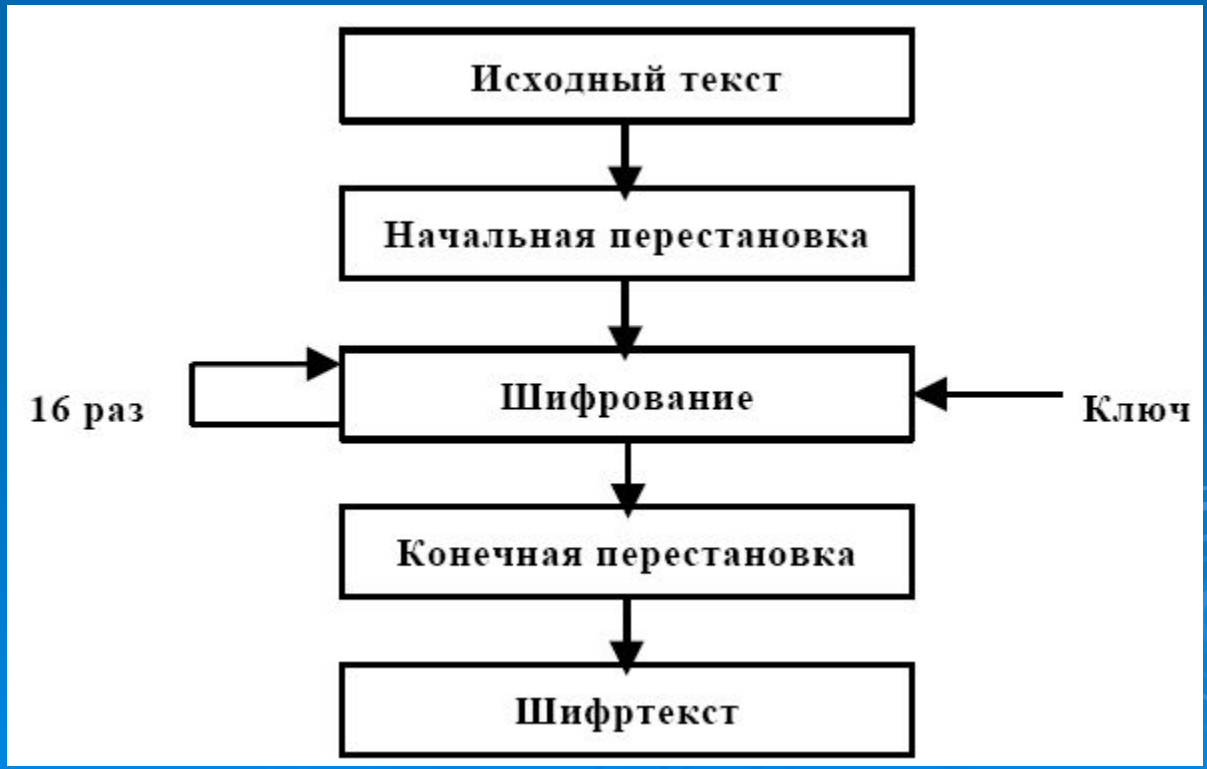


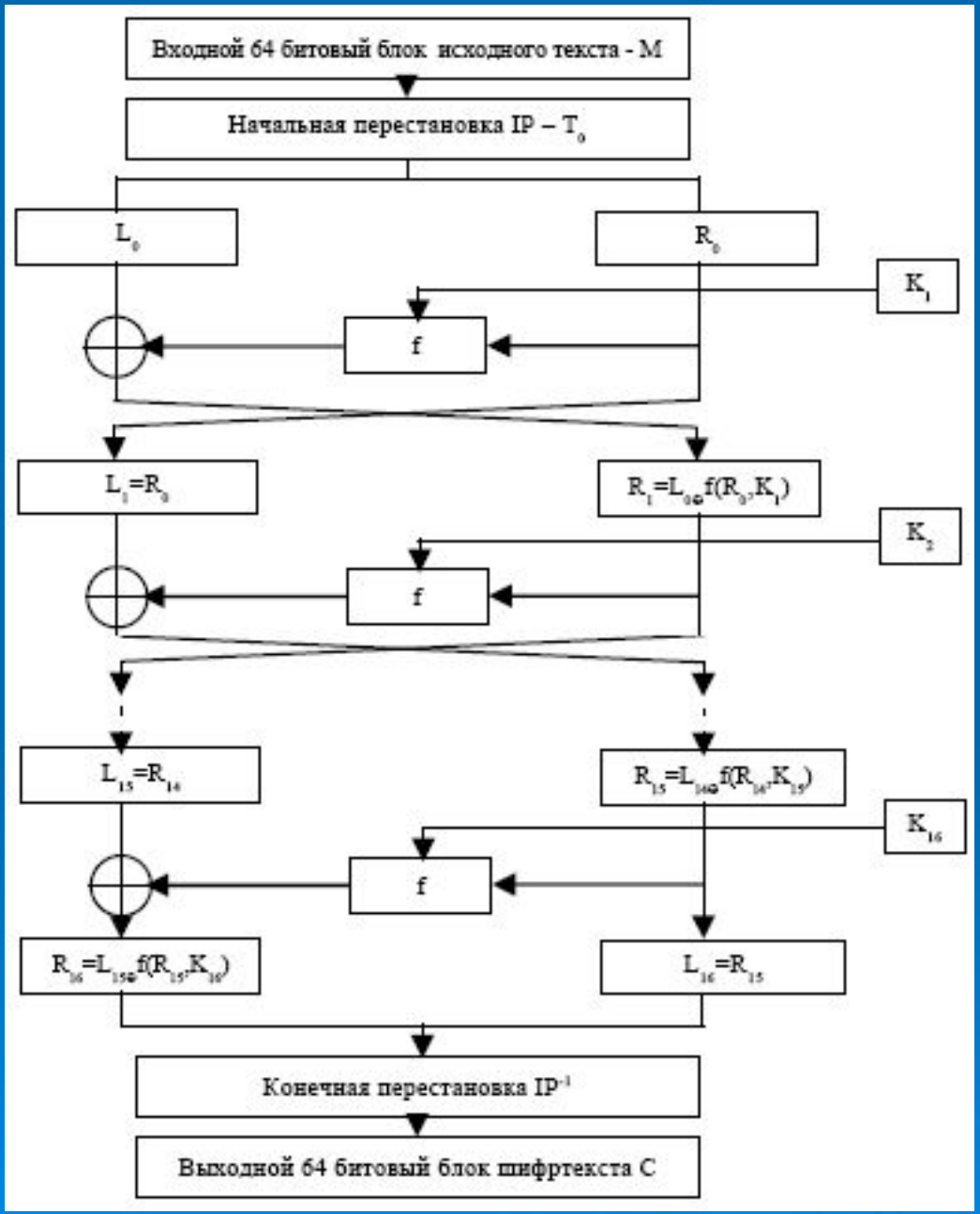
$$C = E_k(m) \qquad m = D_k(C)$$

Симметричное блочное шифрование

Система шифрования DES (Data Encryption Standard)

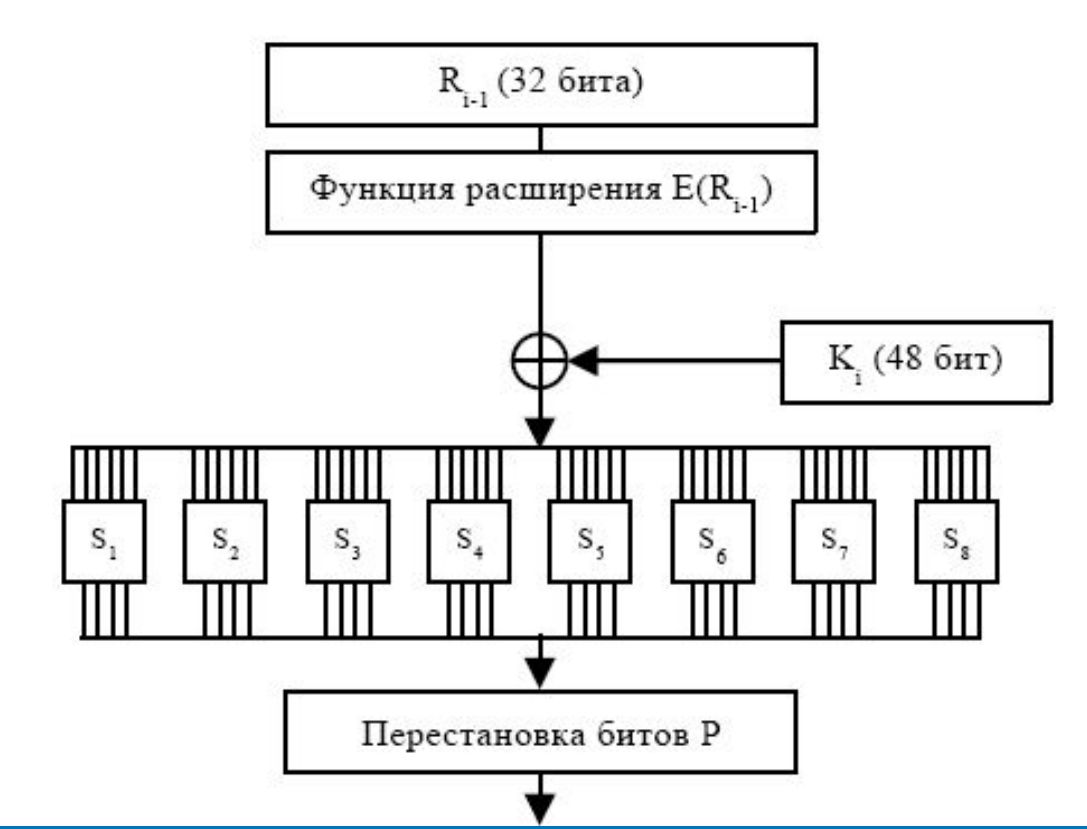
Оперирует 64-битными двоичными блоками.
Размерность ключа 64 бит.





Li и Ri – левый и правый 32-битовые блоки исходного 64 битового блока текста
Ki – 48 битовый ключ
f – функция шифрования
IP – начальная перестановка

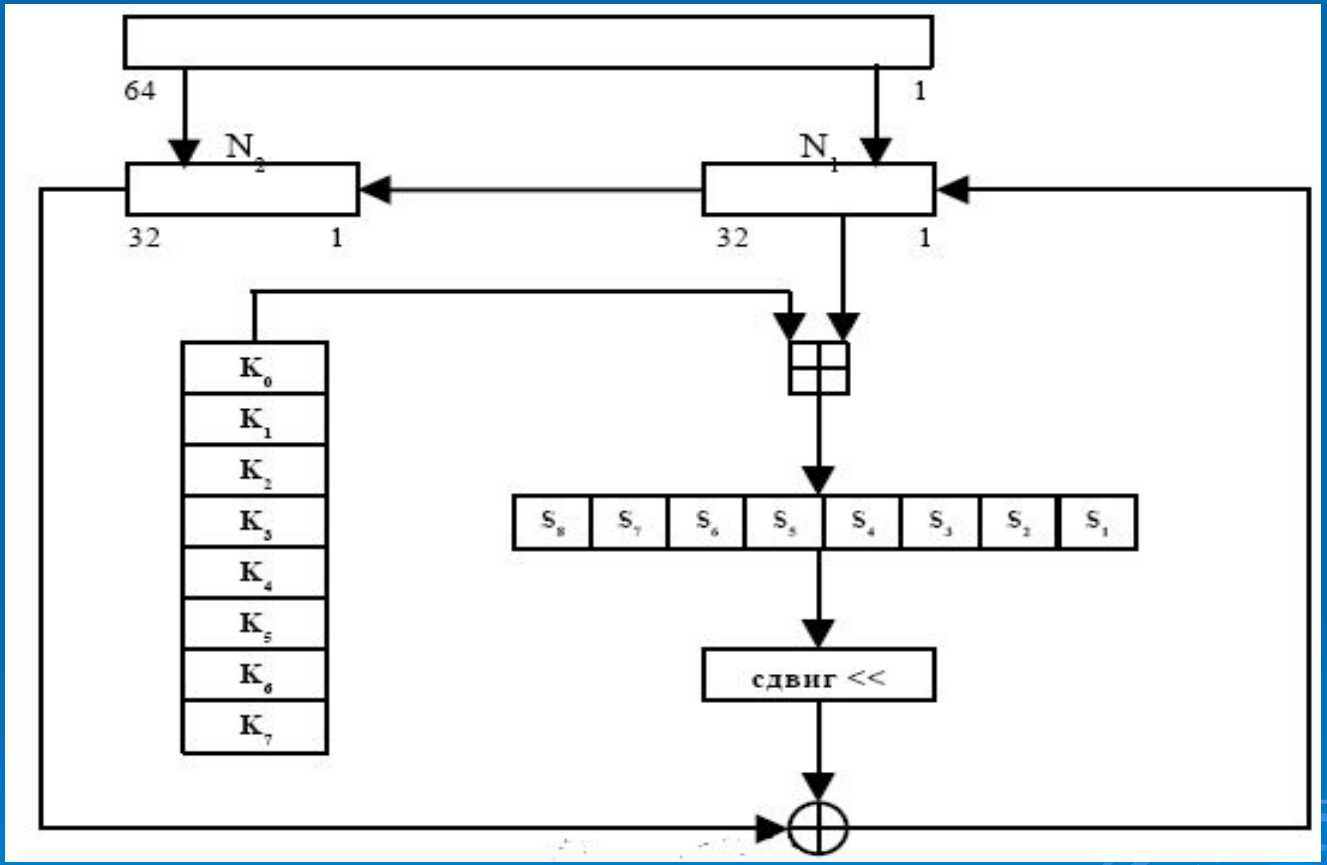
Функция шифрования f (DES)



Модификации 3DES:
С двумя ключами DES
С тремя ключами DES

Стандарт ГОСТ

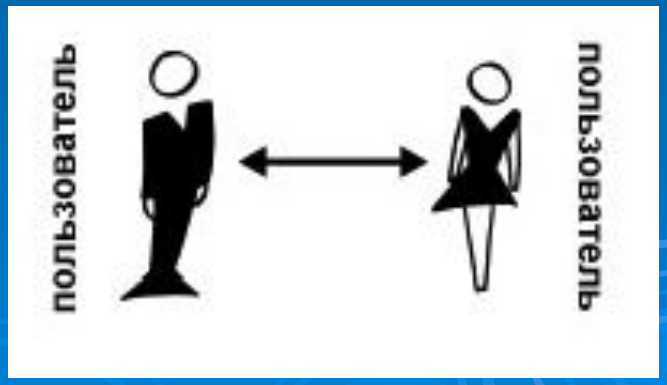
Размер блока – 64 бит. Ключ – 256 бит ; 32 цикла работы



⊕ - Побитовое сложение по модулю 2

⊞ - Побитовое сложение по модулю 2^{32}

Распределение ключей



Прямое доверие

Достоинства и недостатки симметричных систем шифрования

Преимущества криптографии с симметричными ключами:

- **Производительность**
- **Стойкость** (при длине ключа 256 бит необходимо произвести 10 в 77 степени переборов для определения ключа)

Недостатки криптографии с симметричными ключами:

- **Распределение ключей**. Так как для шифрования и расшифрования используется один и тот же ключ, то при использовании криптографии с симметричными ключами требуются очень надежные механизмы для распределения ключей.
- **Масштабируемость.** Так как используется единый ключ между отправителем и каждым из получателей, то количество необходимых ключей возрастает в геометрической прогрессии. Для 10 пользователей нужно 45 ключей, а для 100 уже 499500.
- **Ограниченное использование.** Так как криптография с симметричными ключами используется только для шифрования данных и ограничивает доступ к ним, то при ее использовании невозможно обеспечить аутентификацию (установление подлинности отправляющей стороны) и неотрекаемость

- Некоторые вопросы теории чисел

Простые и составные числа

- Опр: Если целое число большее 1 не имеет делителей не равных 1 и самого этого числа, то оно называется простым, иначе составным
- Пусть pi-простые числа
- a - составные

$$a = p1^{\alpha 1} * p2^{\alpha 2} * .. * pk^{\alpha k}$$

Функция Эйлера

- Опр: Функция Эйлера φ(a) – функция которая определяет для каждого целого положительного a значение φ(a) равное числу чисел из ряда 1,2, ..a-1 которые взаимно просты с a. При этом полагается что φ(1)=1
- φ(2)=1, φ(3)=2, φ(4)=2, φ(5)=4 ..

φ(p)=p-1, если p - простое

$$\varphi(a) = (p1^{\alpha 1} - p1^{\alpha 1-1}) * .. * (pk^{\alpha k} - pk^{\alpha k-1})$$

Сравнения

- Опр: Числа a и b, которые при делении на одно и то же положительное число m дают один и тот же остаток называют сравнимыми по модулю m
- $a=b \bmod m \quad \sim \quad a=b + m*t$

Теорема Эйлера

$$a^{\varphi(m)} = 1 \bmod m$$

Если a – простое, и (a, p)=1

$$a^{p-1} = 1 \bmod p$$

Решение линейных сравнений

- Опр: Выражение ax=b mod m называется линейным сравнением.
- Если (a,m)=1 оно имеет единственное решение:

$$x = b \cdot a^{\varphi(m)-1} \bmod m$$

- Если m=p –простое, (a,p)=1

$$x = b \cdot a^{p-2} \bmod p$$

Пример

$$x = b \cdot a^{p-2} \bmod p$$

- 3x=5 mod 7
- x=5*3^{6-1} mod 7
- x=5*3^5 mod 7=5*3*3^4 mod 7=
- 1*3^4 mod 7=3^2*3^2 mod7 = 2*2 mod 7 = 4 mod 7
- Проверка: 3*4 mod 7 = 5 mod 7
- Задание: 5x=3 mod 11

Показатели

- Наименьшее из чисел γ : $a^{\gamma} = 1 \bmod m$, НОД(a,m)=1 называется показателем числа a по модулю m.
- Если показатель a по модулю m равен φ (m), то a называется первообразным (примитивным) корнем по модулю m.

Индексы-дискретные логарифмы

- Пусть p – простое, и для некоторого целого числа y из множества {0,1..p-1} имеет место представление

$$a = g^y \bmod p$$

тогда y – называют дискретным логарифмом или индексом числа a по основанию g

$$y = ind_g a$$

Пример

- $3=5^y \bmod 7$ $y=\text{ind}_5 3$
- Вычисляется подбором:
- $y=1$ $5^1 \bmod 7 \neq 3$
- $y=2$ $5^2 \bmod 7 = 25 \bmod 7 = 4 \neq 3$
- $y=3$ $5^3 \bmod 7 = 125 \bmod 7 = 4*5 \bmod 7 = 6 \neq 3$
- $y=4$ $5^4 \bmod 7 = 625 \bmod 7 = 6*5 \bmod 7 = 2 \neq 3$
- $y=5$ $5^5 \bmod 7 = 3125 \bmod 7 = 2*5 \bmod 7 = 3$

- $\text{Ind}_5 3=5$

- Задание $2=3^y \bmod 7$