Блочные шифры. Режимы блочных шифров

Лекция №4

БЛОЧНЫЕ ШИФРЫ - ИСТОРИЯ

1949 – Клод Шеннон: Перестановки + замены
1970 – Lucifer (IBM): сеть Фейстеля + SP-сеть
1973 – Конкурс НИСТ: никто не прошел!
1974 – 2-ой конкурс: выиграл DES (IBM)
1977 – DES признан официальным стандартом в США
1989 – создание ГОСТ 28147-89
1990 – публикация ГОСТ 28147-89
1997 – взлом DES на суперкомпьютере за 3 дня
1997 – конкурс на AES
2000 – выигрывает Rijndael
2002 – Rijndael признан новым официальным стандартом в США

Блочные шифры - *RC5*, *RC6*, *DES*, *3DES*, *AES*, ГОСТ 28147-89

Требования к блочным шифрам

Общие требования к блочным шифрам:

- шифр должен быть технически применим для закрытия массивов данных произвольного объема;
- шифр должен быть эффективно реализуем в виде устройства, имеющего ограниченный объем памяти.

Следовательно, криптоалгоритм, должен быть пошаговым – сообщение разбивается на блоки ограниченного размера, и за один шаг шифруется один блок:

$$P = (P_1, P_2, \ldots, P_n),\ |P_i| \le N, \text{ для } i \text{ от 1 до } n,$$

где N — максимальный размер блока.

Практически всегда размер блока полагают постоянным:

$$|P_1| = |P_2| = \ldots = |P_{n-1}| = N,\ |P_n| \le N$$

Условия стойкости (по Шеннону)

- *рассеивание* – один бит исходного текста должен влиять на несколько битов шифротекста, оптимально — на все биты в пределах одного блока. При шифровании двух блоков данных с минимальными отличиями между ними должны получаться совершенно непохожие друг на друга блоки шифротекста. Аналогично и для зависимости шифротекста от ключа — один бит ключа должен влиять на несколько битов шифротекста;

- *перемешивание* – шифр должен скрывать зависимости между символами исходного текста и шифротекста. Если шифр достаточно хорошо «перемешивает» биты исходного текста, то соответствующий шифротекст не содержит никаких статистических, и, тем более, функциональных закономерностей.

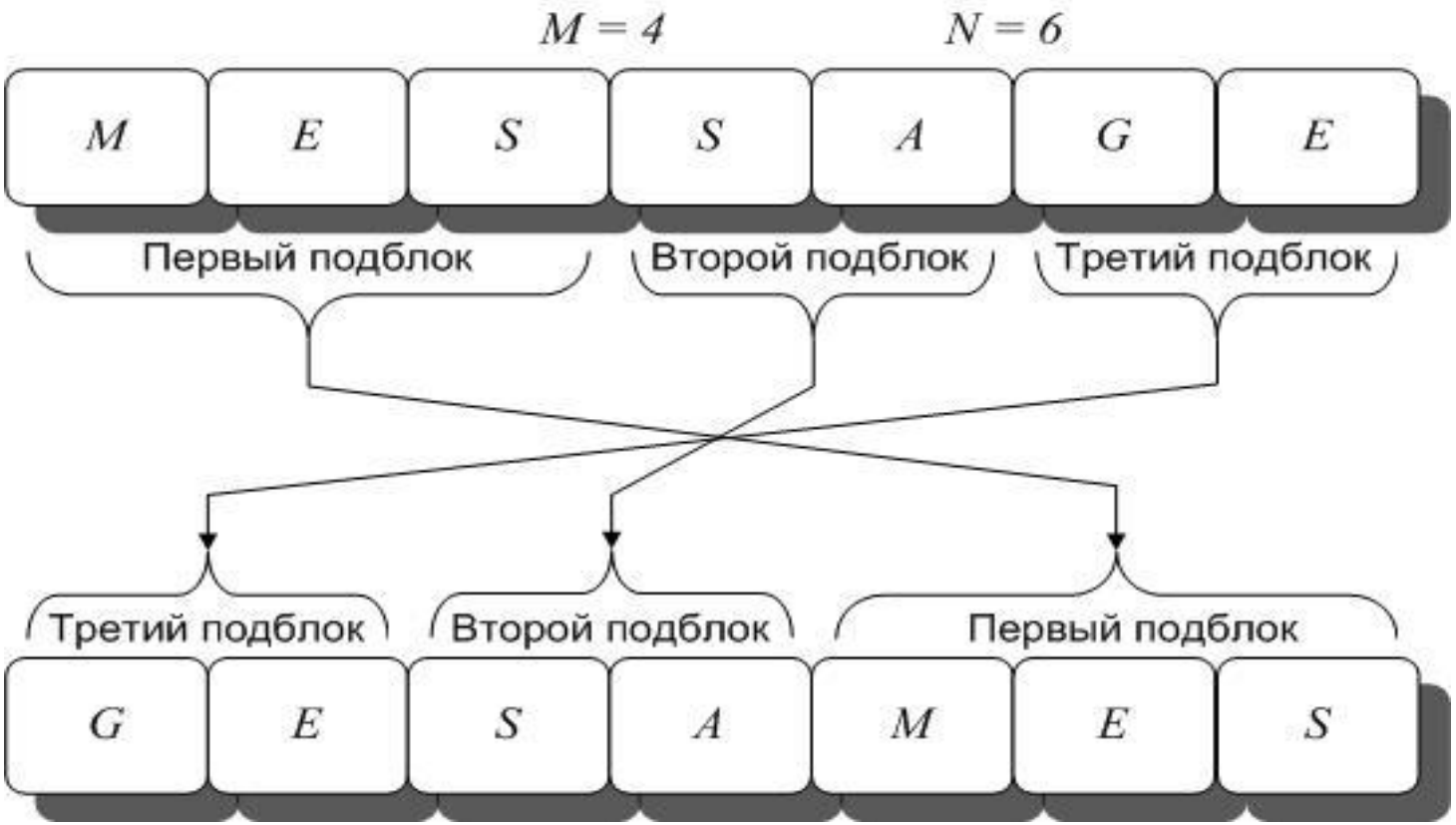
Архитектура блочных шифров

Шифр обычно составляют из более простых шифрующих преобразований. *Простое шифрующие преобразование* – преобразование, которое реализуется аппаратно относительно несложной логической схемой или программно несколькими компьютерными командами.

Основные шифрующие преобразования:

- ***перестановка*** (*permutation*) – перестановка структурных элементов шифруемого блока данных (битов, символов, цифр);
- ***замена, подстановка*** (*substitution*) – замена группы элементов шифруемого блока на другую группу по индексной таблице;
- ***функциональное преобразование*** (*function*) – различные сдвиги, логические и арифметические операций.

Шифр перестановки



Шифр замены

Замена (подстановка) может быть представлена устройство с n входами и выходами. Устройство содержит мультиплексор и демультиплексор, а также 2^n внутренних соединений их выводов, которые могут быть выполнены $2^n!$ различными способами (*ключ* блока подстановок).

Свойства блока подстановок:

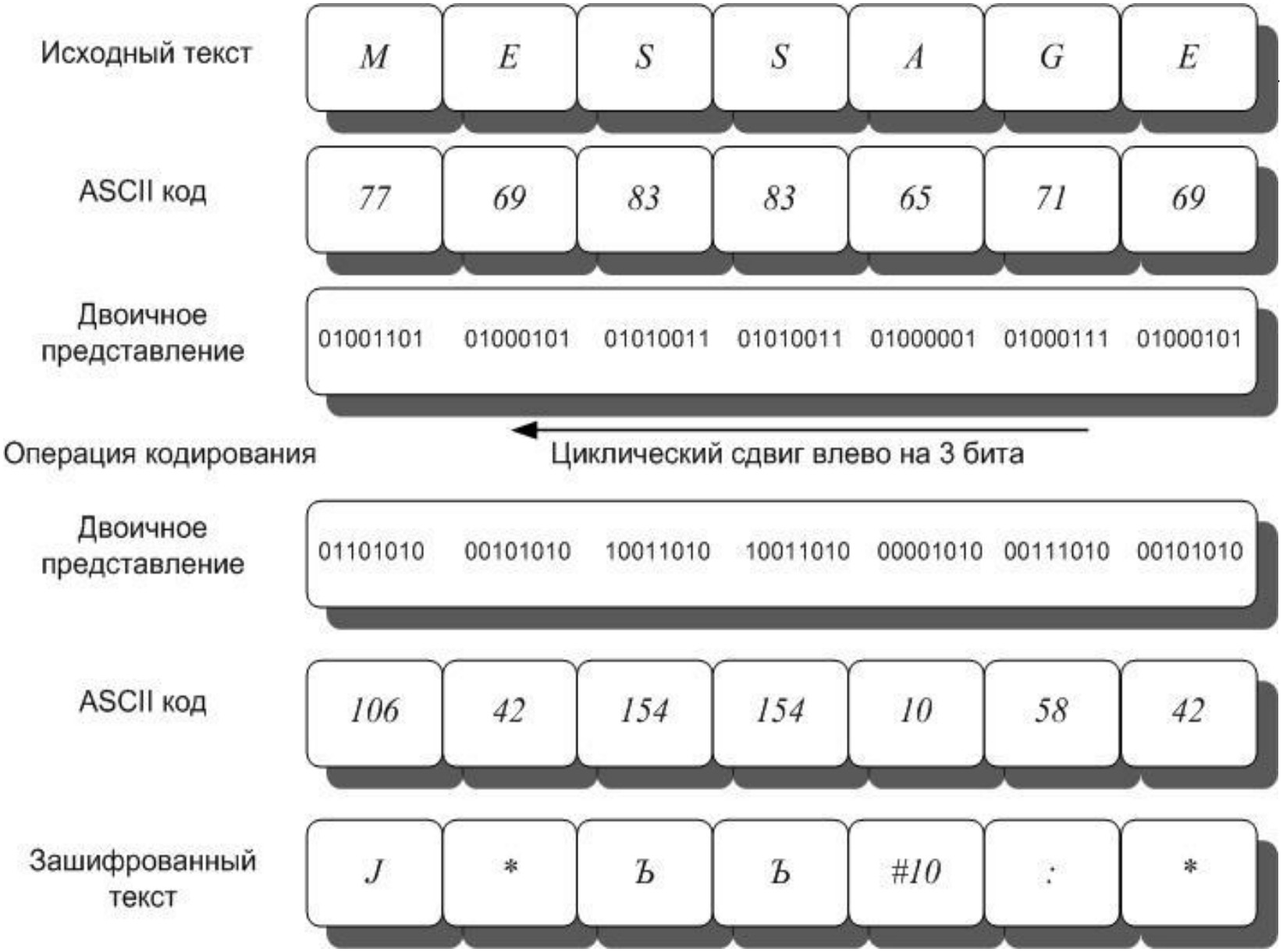
- включает любые линейные и нелинейные преобразования, может заменить любой входной блок цифр на любой выходной блок;
- аппаратно реализуется с помощью запоминающих устройств, программно – индексированным чтением из оперативной памяти, размером (в битах):

$$V = 2^n n;$$

Подстановка по таблице

	1	2	3
0	15	10	2
1	3	17	9
2	8	14	1
3	0	16	45
4	…	…	…
7	20	5	38
8	…	…	…
15	12	11	4

Скремблеры


Исходный текст
M E S S A G E
ASCII код
77 69 83 83 65 71 69
Двоичное представление
01001101 01000101 01010011 01010011 01000001 01000111 01000101
Операция кодирования
Циклический сдвиг влево на 3 бита
Двоичное представление
01101010 00101010 10011010 10011010 00001010 00111010 00101010
ASCII код
106 42 154 154 10 58 42
Зашифрованный текст
J * Ъ Ъ #10 : *

Матричное шифрование

Сообщение: ЗАБАВА = <8,1,2,1,3,1>

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}$$

Матричное шифрование

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix} \quad A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

$$B_1 = \begin{vmatrix} -17/1151 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix}$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}$$

Матрица Винжера

$$T_в = \begin{vmatrix} А & Б & В & Г & Д & \cdots & Ъ & Э & Ю & Я & \_ \\ Б & В & Г & Д & Е & \cdots & Э & Ю & Я & \_ & А \\ В & Г & Д & Е & Ж & \cdots & Ю & Я & \_ & А & Б \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \_ & А & Б & В & Г & \cdots & Ы & Ъ & Э & Ю & Я \end{vmatrix}$$

Ключевое слово: «ЗОНД»

$$T_ш = \begin{vmatrix} А & Б & В & Г & Д & Е & Ж & З & И & К & Л & М & Н & О & П & Р & С & Т & У & Ф & Х & Ц & Ч & Ш & Щ & Ъ & Ы & Ь & Э & Ю & Я & \_ \\ З & И & К & Л & М & Н & О & П & Р & С & Т & У & Ф & Х & Ц & Ч & Ш & Щ & Ъ & Ы & Ь & Э & Ю & Я & \_ & А & Б & В & Г & Д & Е & Ж \\ О & П & Р & С & Т & У & Ф & Х & Ц & Ч & Ш & Щ & Ъ & Ы & Ь & Э & Ю & Я & \_ & А & Б & В & Г & Д & Е & Ж & З & И & К & Л & М & Н \\ Н & О & П & Р & С & Т & У & Ф & Х & Ц & Ч & Ш & Щ & Ъ & Ы & Ь & Э & Ю & Я & \_ & А & Б & В & Г & Д & Е & Ж & З & И & К & Л & М \\ Д & Е & Ж & З & И & К & Л & М & Н & О & П & Р & С & Т & У & Ф & Х & Ц & Ч & Ш & Щ & Ъ & Ы & Ь & Э & Ю & Я & \_ & А & Б & В & Г \end{vmatrix}$$

ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ

1949 – Клод Шеннон «Теория связи в секретных системах». Идея итеративных блочных шифров на основе SP-сетей (перестановки + замены)

Шифр преобразует блоки открытого текста (m) постоянной длины (n) в блоки шифротекста (C) той же длины посредством циклически повторяющихся обратимых функций, известных как **раундовые функции**

$C_i = R_{k_i}(C_{i-1})$

R – раундовая функция

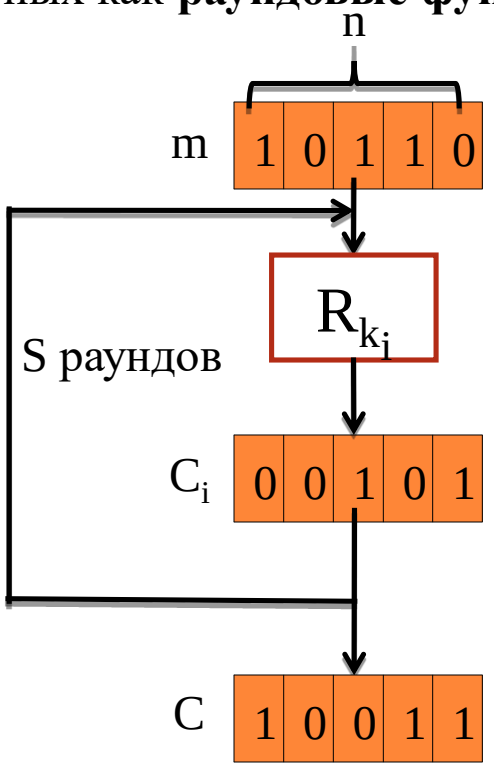
k_i – подключ , где $1 \le i \le S$

i – номер раунда

S – количество раундов

C_i - значение блока после i-го раунда

n – длина блока



SP-СЕТИ

SP-сеть = substitution-permutation network (SPN)

Чередующиеся стадии подстановки (**S**ubstitution) и перестановки (**P**ermutation)

S-блоки (substitution box or S-box) – таблица подстановки

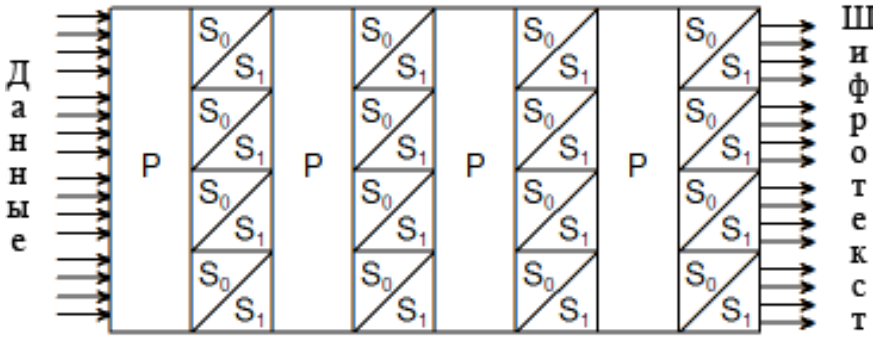
P-блоки (permutation box or P-box) – таблица перестановки

Основные критерии шифра по Шеннону:

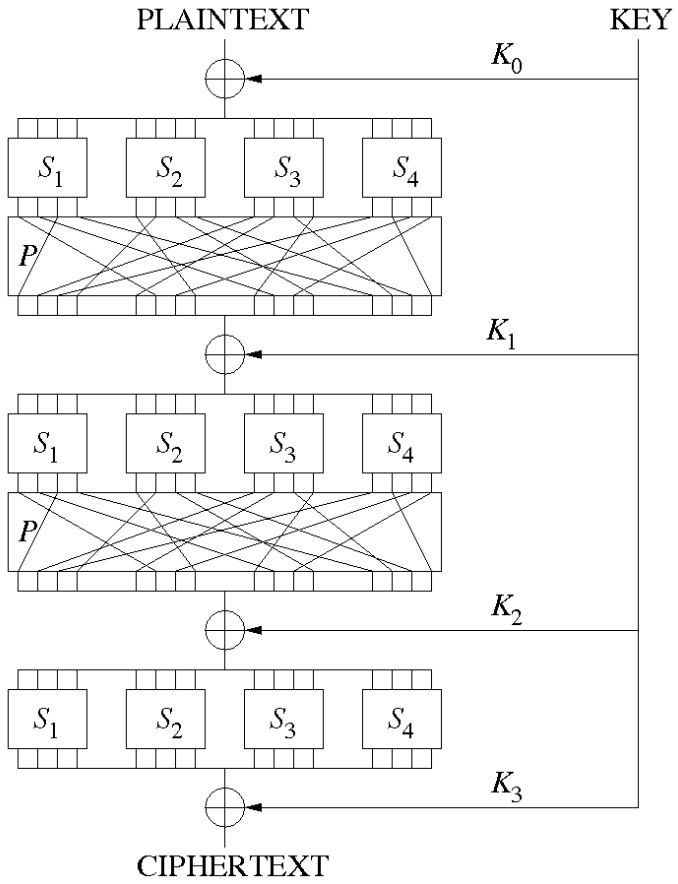
- **Рассеивание** (влияние одного символа на несколько символов шифротекста)
- **Перемешивание** (усложнение взаимосвязей между элементами данных)

SP-СЕТИ

Упрощенная SP модель (1971)



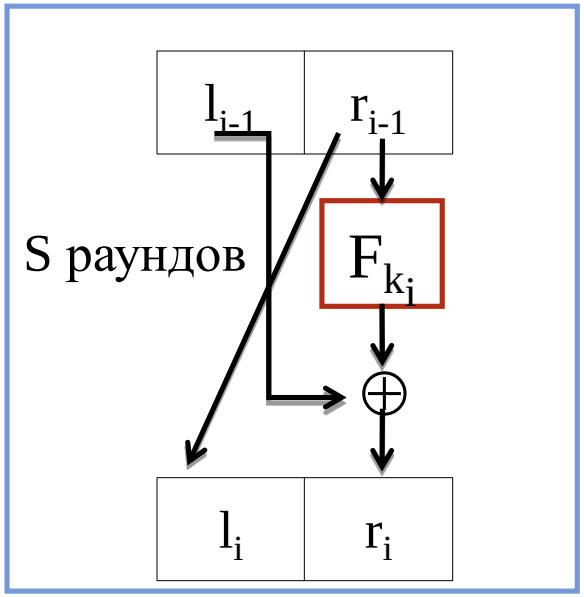
Пример SP сети с 3-мя раундами



СЕТЬ ФЕЙСТЕЛЯ

1971 – Хорст Фейстель патентует Lucifer с сетью Фейстеля

Блок открытого текста l_0 r_0



Блок шифротекста L_S R_S

Шифрование:

$l_i = r_{i-1}$, $r_i = l_{i-1} \oplus F(k_i, r_{i-1})$

Расшифрование:

$r_{i-1} = l_i$, $l_{i-1} = r_i \oplus F(k_i, l_i)$

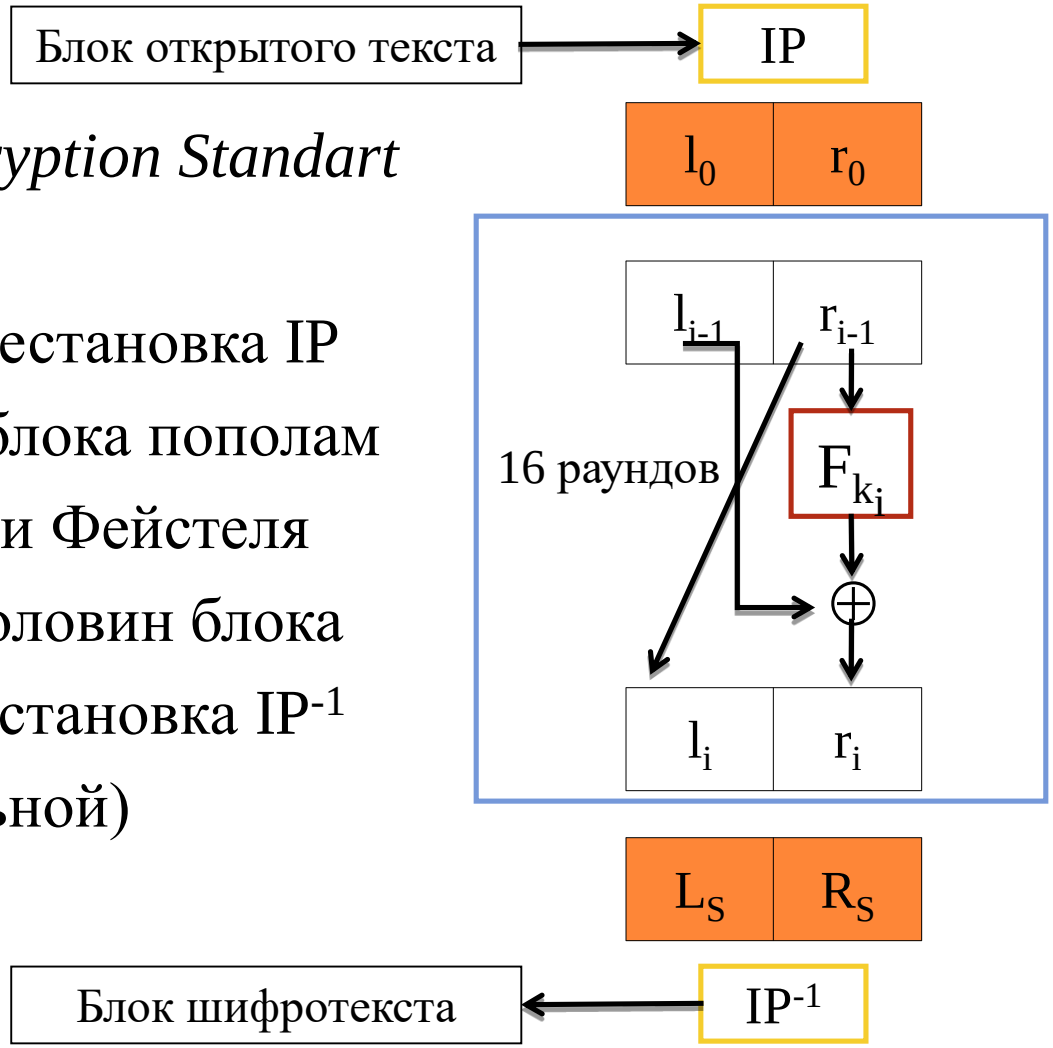
Одну и ту же схему
можно использовать
и для шифрования,
и для расшифрования

DES НА ОСНОВЕ СЕТИ ФЕЙСТЕЛЯ

DES – *Data Encryption Standart*

- Начальная перестановка IP
- Расщепление блока пополам
- 16 раундов сети Фейстеля
- Соединение половин блока
- Конечная перестановка IP^{-1}

(обратная начальной)



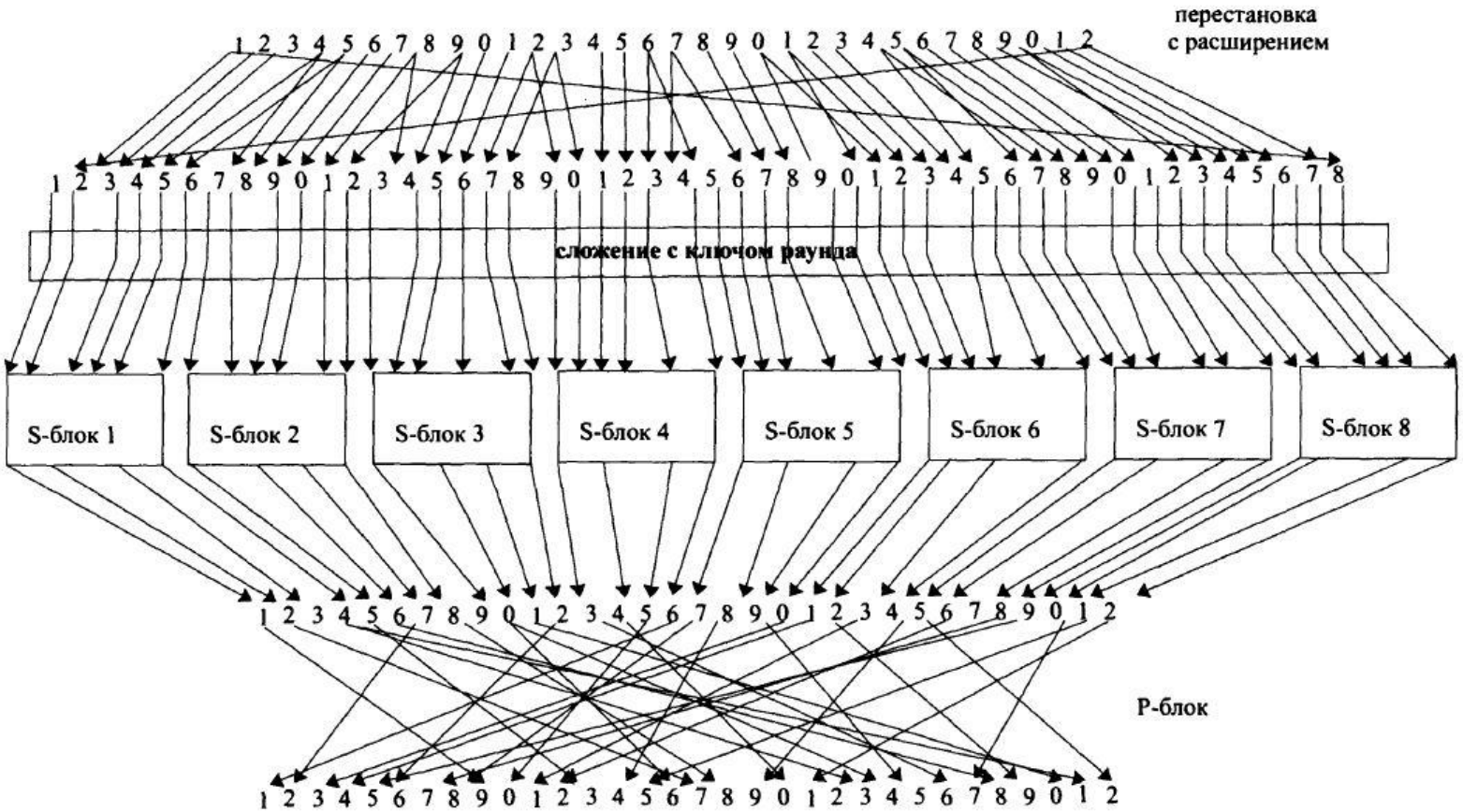
DES - СТРУКТУРА

- Число раундов ***S* = 16**
- Длина блока ***n* = 64 бита**
- Размер ключа **k – 56 бит**
- Подключи ***k1, k2,…*по 48 битов** (разворачивание из основного ключа через подстановки, перестановки и циклические сдвиги)

Действие F

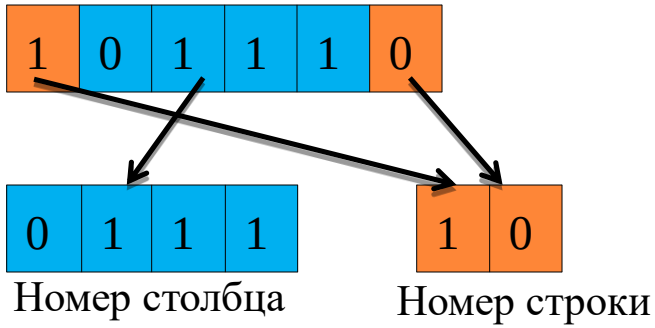
1. Перестановка с расширением (32 → 48)
2. Сложение с подключом (48 + 48)
3. Расщепление (48 = 8 частей по 6 битов)
4. Подстановки через S – блок (8 * (6 → 4) = 32)
5. Перестановки через P – блок (32 → 32)

DES - СТРУКТУРА



DES – S-БЛОКИ

На вход подается 6 бит:



S-блок №1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	5	13

На выходе получается 4 бита

Объединение блочных шифров

Двойное шифрование

$$C = E_{k2}\left(E_{k1}\left(M\right)\right); \qquad M = D_{k1}\left(D_{k2}\left(C\right)\right)$$

Тройное шифрование с двумя ключами

$$C = E_{k1}\left(D_{k2}\left(E_{k1}\left(M\right)\right)\right); \qquad M = D_{k1}\left(E_{k2}\left(D_{k1}\left(C\right)\right)\right)$$

Тройное шифрование с тремя ключами

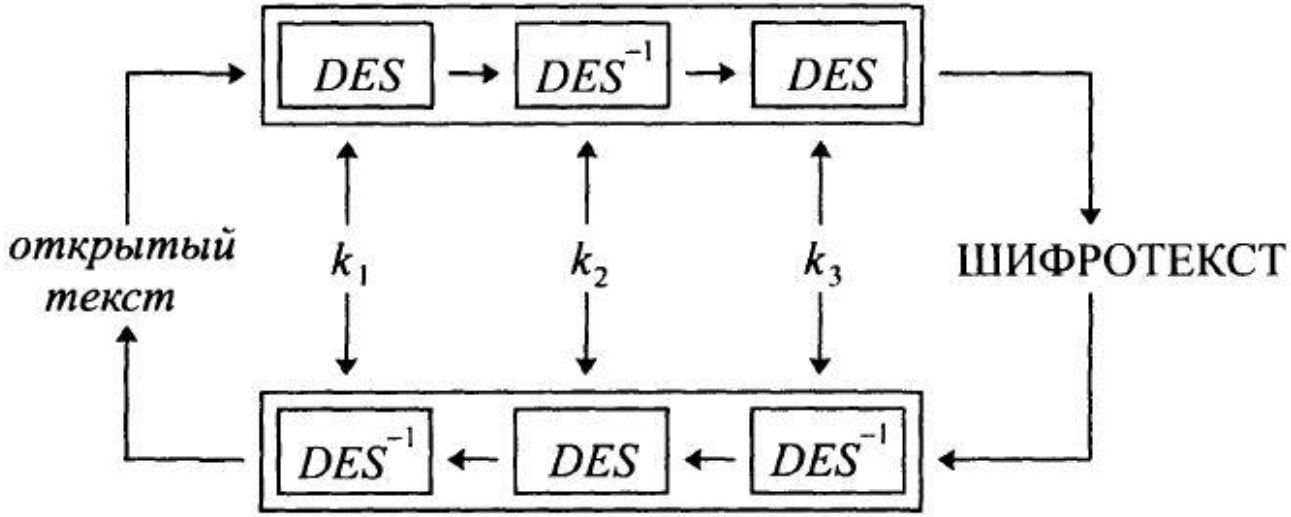
$$C = E_{k1}\left(D_{k2}\left(E_{k3}\left(M\right)\right)\right); \qquad M = D_{k1}\left(E_{k2}\left(D_{k3}\left(C\right)\right)\right)$$

3DES (TRIPLE DES)

Использует **3 ключа по 56 бит** (3*56=168)

Различные модификации 3DES:

- DES-EEE3
- **DES-EDE3**
- DES-EEE2
- DES-EDE2

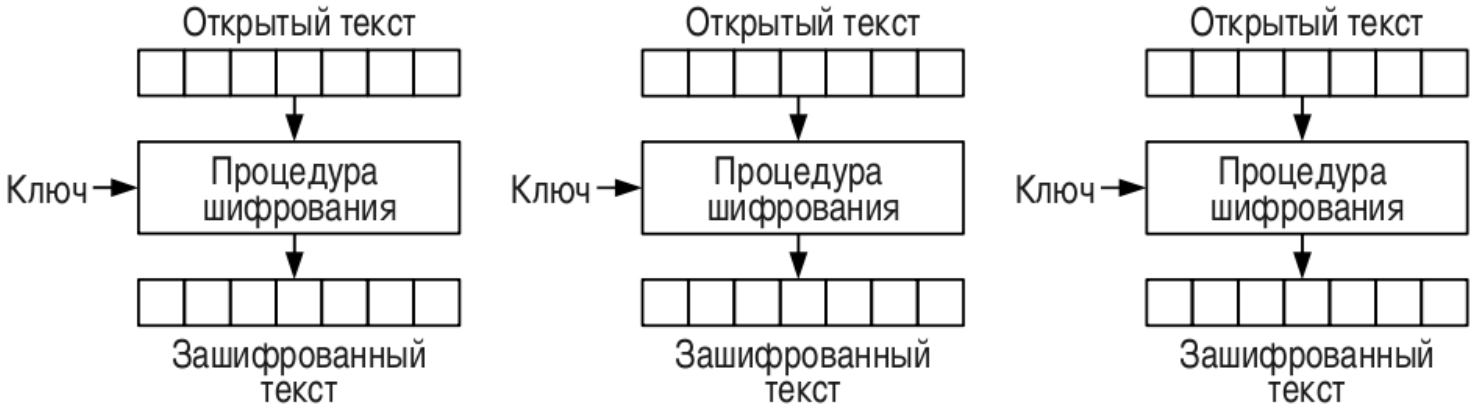


DES – РЕЖИМЫ ШИФРОВАНИЯ

Режимы шифрования:

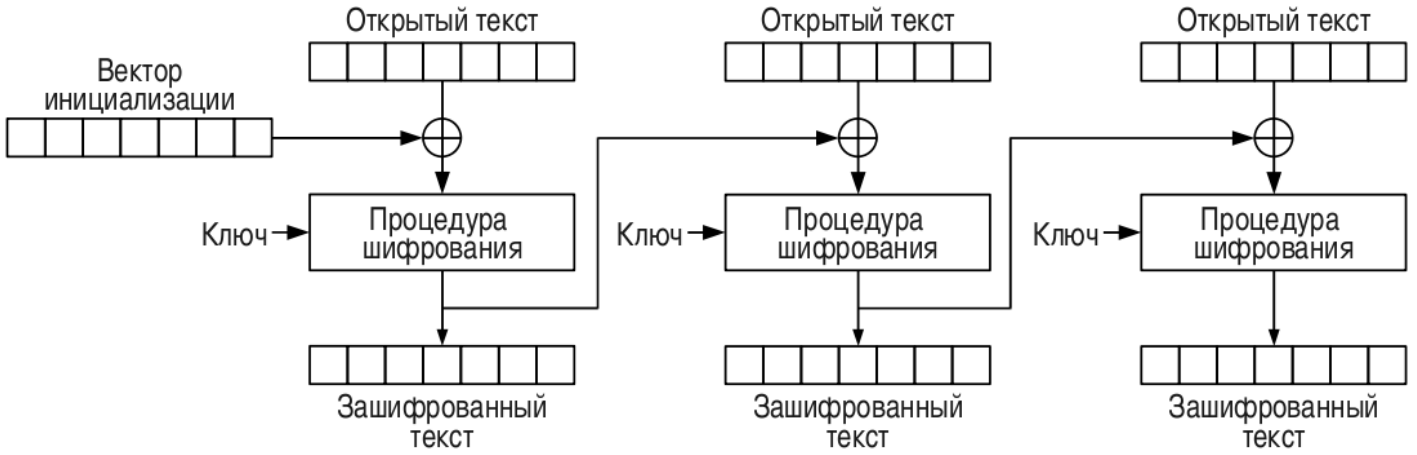
- **ECB** – Electronic Code Book (электронная кодовая книга)
- **CBC** – Cipher Block Chaining (сцепление блоков шифротекста)
- **OFB** – Output FeedBack (обратная связь вывода)
- **CFB** – Cipher FeedBack (обратная связь шифра)

РЕЖИМЫ ШИФРОВАНИЯ - ECB



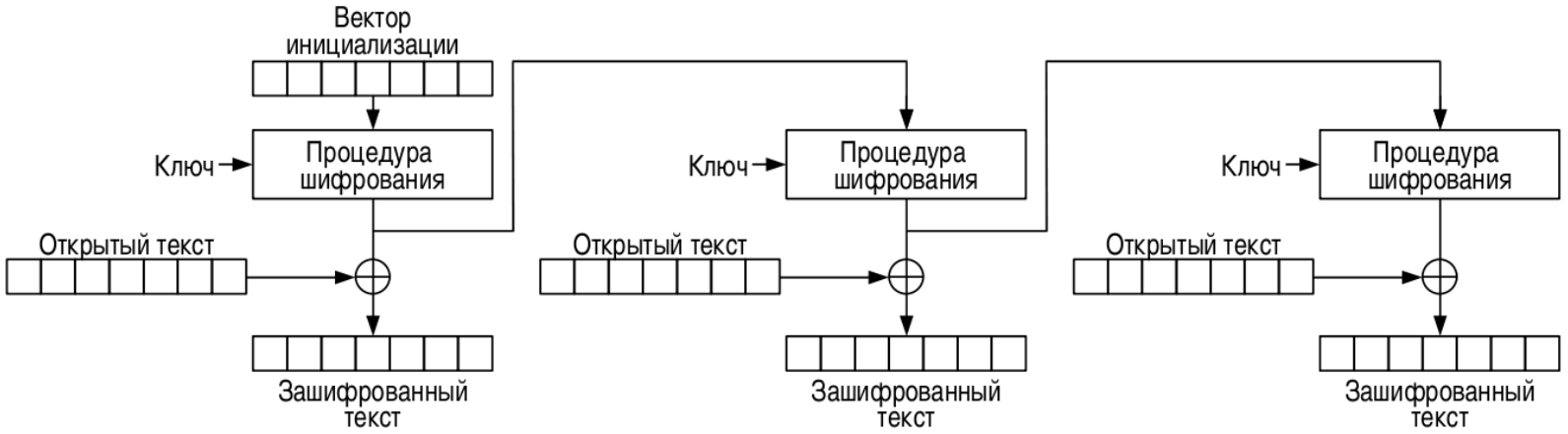
- ECB (*Electronic Code Book – Режим электронной кодовой книги)* – прост в обращении, но не защищен от атак с удалением и вставками. Ошибка в одном бите влияет на целый блок в расшифрованном тексте. Можно работать с блоками независимо и даже распараллелить вычисления.

РЕЖИМЫ ШИФРОВАНИЯ - CBC



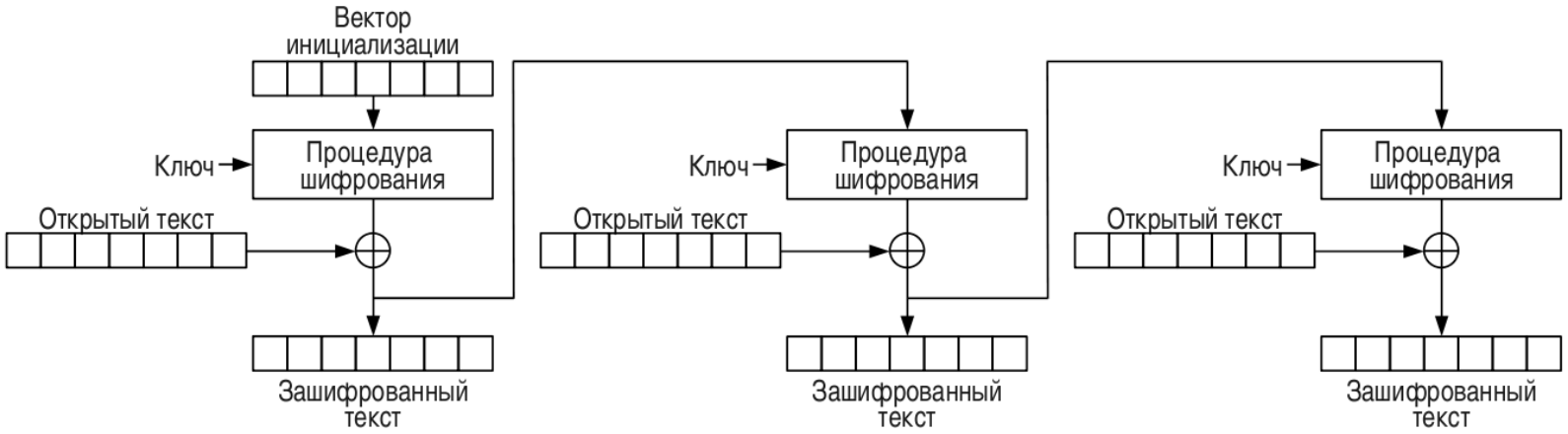
- CBC (*Cipher Block Chaining-Режим сцепления блоков)* – предотвращает потери при атаке со вставкой и удалением. Ошибки при шифровании и в открытом тексте дают ошибку не только в текущем блоке, но и портит следующие блоки.

РЕЖИМЫ ШИФРОВАНИЯ - CFB



- CFB (*Cipher FeedBack – режим обратной связи по шифротексту*) – защита от атак вставки и удаления. Ошибки в открытом тексте и при шифровании распространяются дальше по шифротексту.

РЕЖИМЫ ШИФРОВАНИЯ - OFB



- OFB (*Output FeedBack – режим обратной связи по выходу)* – Ошибка в открытом тексте остается в блоке. Ошибка при шифровании распространяется по шифротексту.

ГОСТ 28147-89

«ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

1989 – год создания

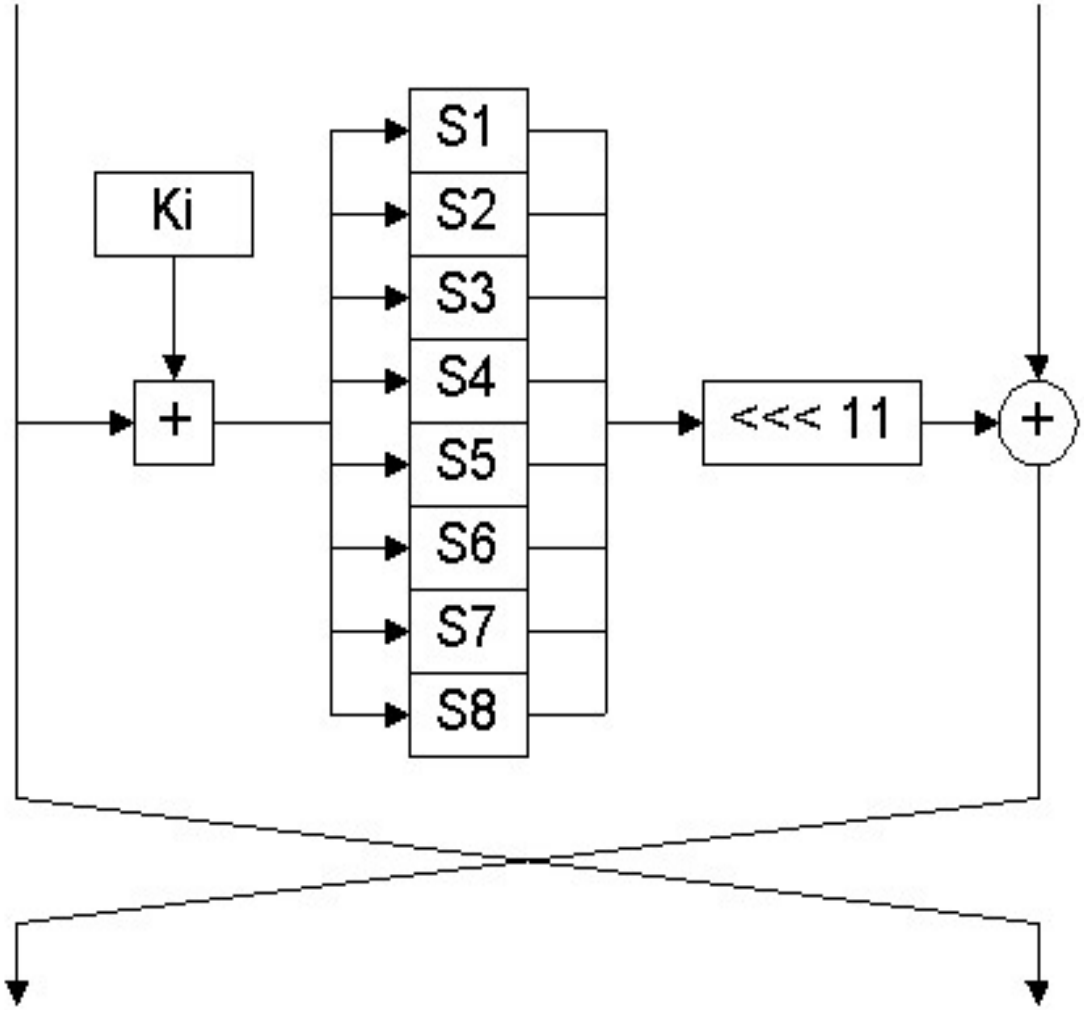
1990 – опубликован для «служебного пользования»

1994 – полностью открыт

Работает, как и DES, на основе сети Фейстеля:

- Число раундов ***S* = 32**
- Длина блока ***n* = 64 бита**
- Размер ключа **k – 256 бит**
- Подключи ***k1, k2,…, k8* по 32 бита** повторяются 4 раза

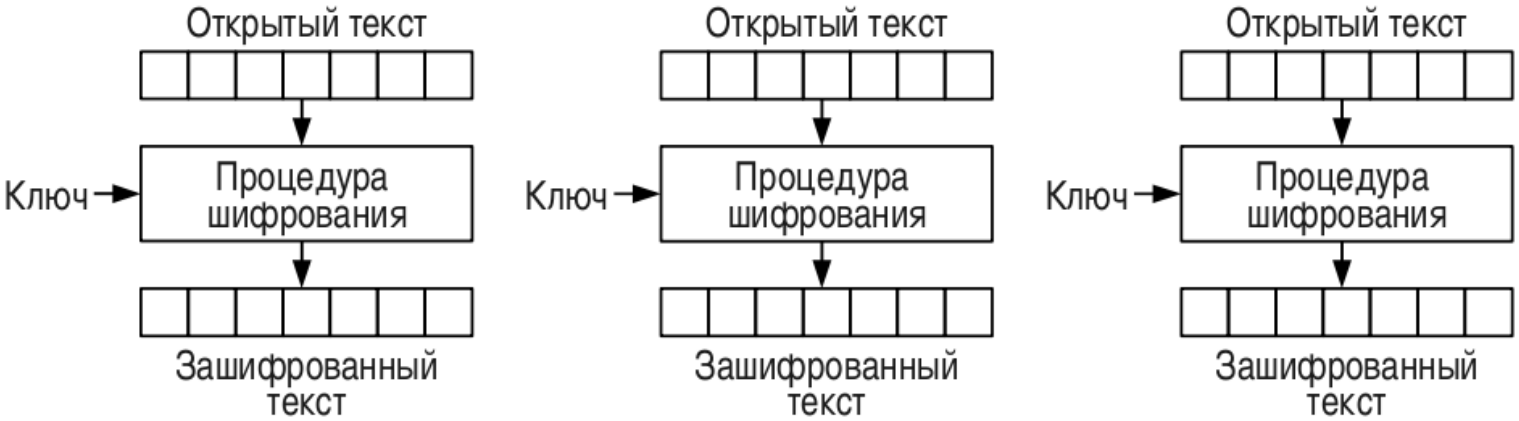
ГОСТ 28147-89



ГОСТ 28147-89 – РЕЖИМЫ ШИФРОВАНИЯ

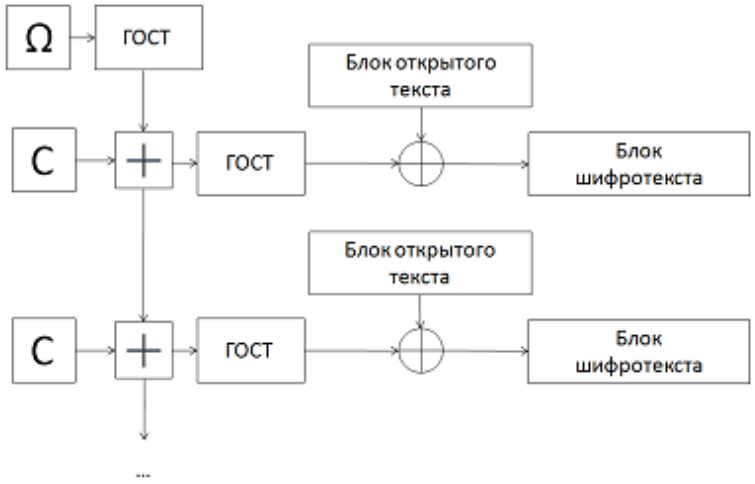
- Простая замена (ECB – electronic code book)
- Гаммирование
- Гаммирование с обратной связью (CFB – Cipher FeedBack)
- *Имитовставка* (MAC – message authentication code)

Простая замена (ECB)

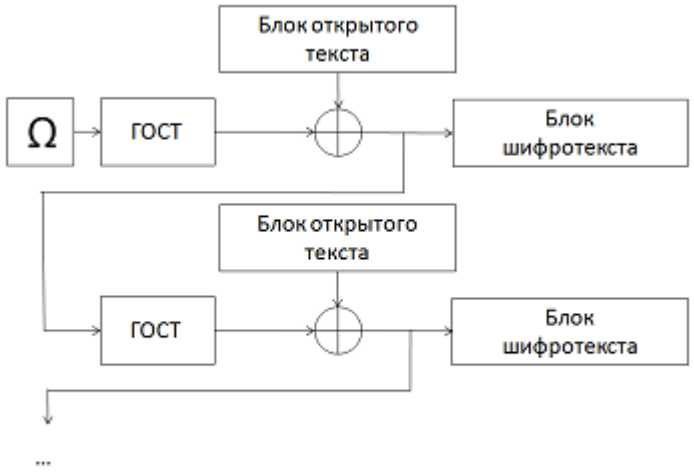


ГОСТ 28147-89 – РЕЖИМЫ РАБОТЫ

Гаммирование



Гаммирование с обратной связью (CFB)



Имитовставка (MAC)

Использование строки случайных бит

1. Генерируется строка случайных бит *R* того же размера, что и сообщение *M*.
2. R шифруется первым алгоритмом.
3. $M \oplus R$ шифруется вторым алгоритмом
4. Шифротекст сообщения является объединением результатов этапов 2 и 3.