СИММЕТРИЧНЫЕ ШИФРЫ

Курс криптографии

кафедра БИТ НИУ ИТМО

СОДЕРЖАНИЕ

- Основные принципы современных симметричных алгоритмов
- Алгоритм DES, режимы шифрования
- Алгоритм ГОСТ 28147-89, режимы шифрования
- Алгоритм Rijndael (AES)
- Область поточных шифров и регистров сдвига с линейной обратной связью

СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ ШИФРЫ

Алгоритм шифрования является **симметричным**, если процесс шифрования и расшифровывания используют **один и тот же ключ**.

Процесс шифрования $C = E_k(m)$

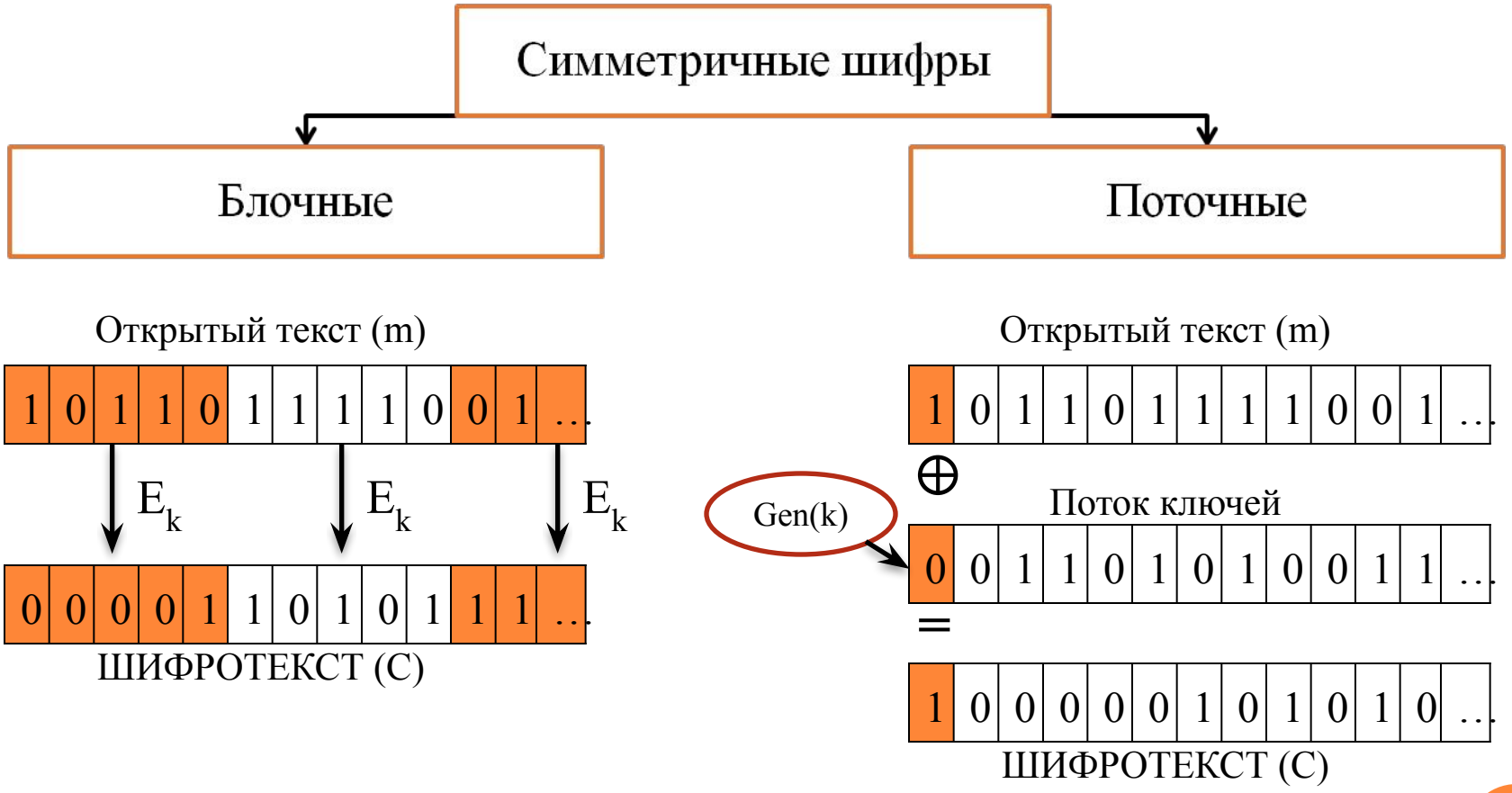
Процесс расшифровывания $m = D_k(C)$

Алгоритм шифрования является **асимметричным**, если процесс шифрования и расшифровывания **используют два различных ключа**.

Процесс шифрования $C = E_{k1}(m)$

Процесс расшифровывания $m = D_{k2}(C)$

СИММЕТРИЧНЫЕ ШИФРЫ – БЛОЧНЫЕ И ПОТОЧНЫЕ



СИММЕТРИЧНЫЕ ШИФРЫ – БЛОЧНЫЕ И ПОТОЧНЫЕ

Сравнение блочного и поточного шифра:

- Блочный более общий, трансформируется в поточный.
- Поточный шифр имеет более математизированную структуру.
- Поточные шифры не очень удобны с точки зрения программного обеспечения, но высоко эффективны с точки зрения аппаратной реализации.
- Блочные шифры удобны и для программных и аппаратных средств, но не допускают быстрой обработки информации.
- Аппаратные средства функционируют быстрее, чем программное обеспечение, но это за счет снижения гибкости.

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

БЛОЧНЫЕ ШИФРЫ – 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**

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

R – раундовая функция

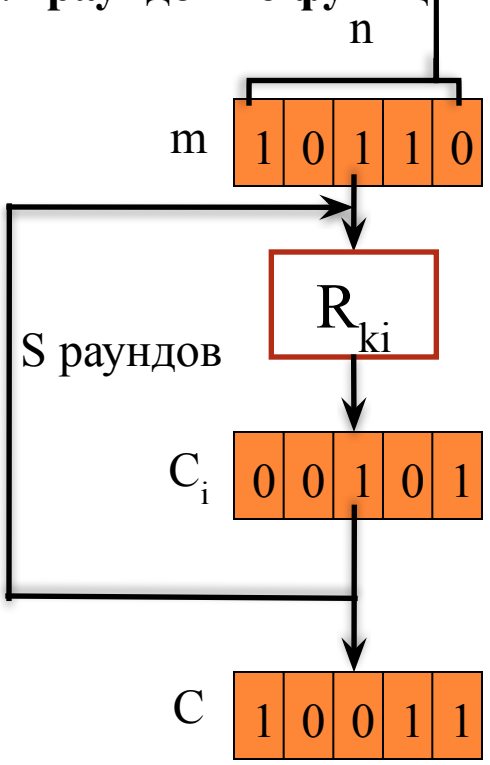
k_i – подключ , где $1 \le i \le S$

i – номер раунда

S – количество раундов

C_i - значение блока после i-го раунда

n – длина блока



БЛОЧНЫЕ ШИФРЫ – 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 принципы шифра по Шеннону:

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

БЛОЧНЫЕ ШИФРЫ - СЕТЬ ФЕЙСТЕЛЯ

1971 – Хорст Фейстель патентует Lucifer с сетью Фейстеля

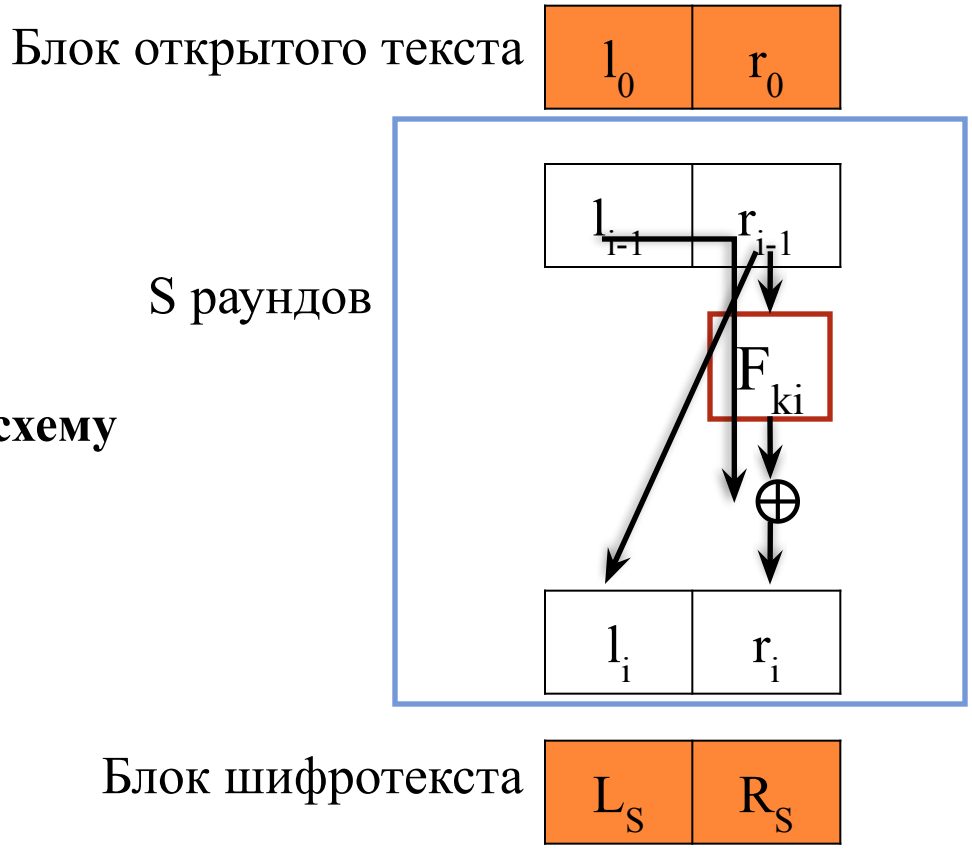
<u>Шифрование:</u>

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

<u>Расшифрование:</u>

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

- **Одну и ту же микросхему** можно использовать и для шифрования, и для расшифрования (!!!)

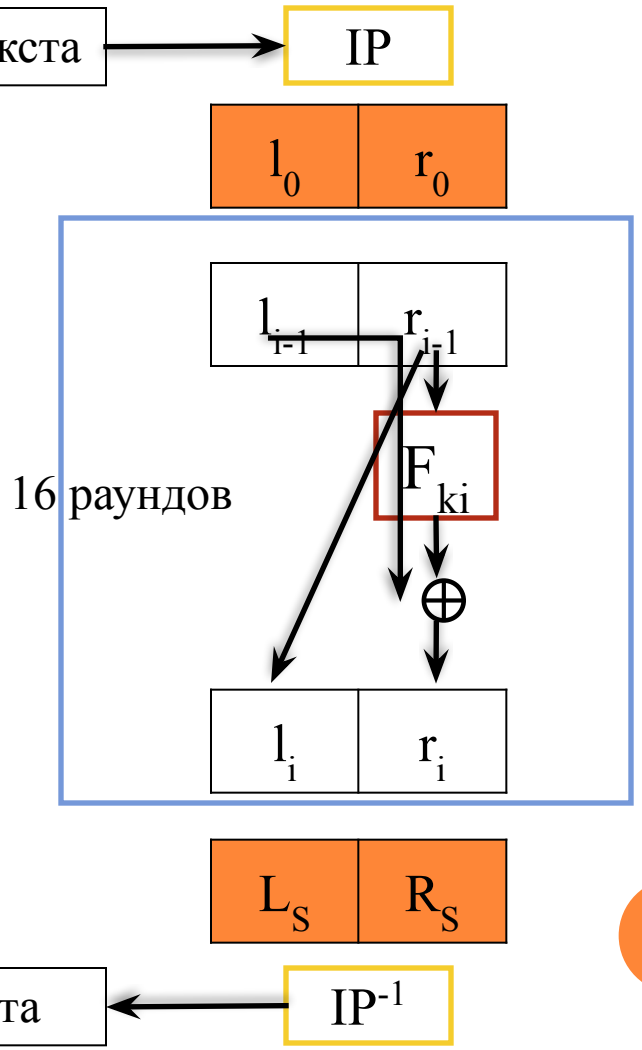


DES – НА ОСНОВЕ СЕТИ ФЕЙСТЕЛЯ

DES – *Data Encryption Standart*

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

(обратная начальной)



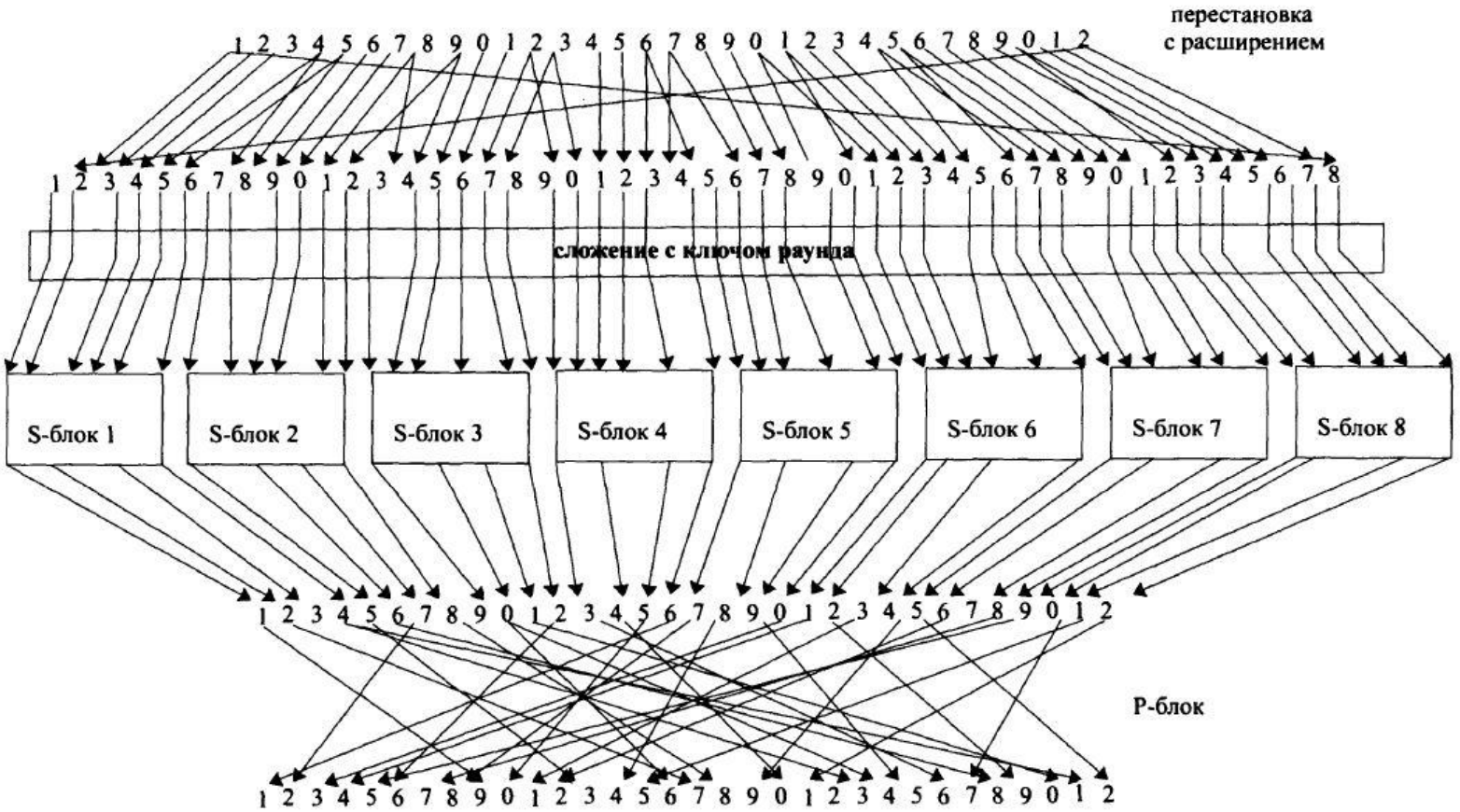
DES - СТРУКТУРА

- 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

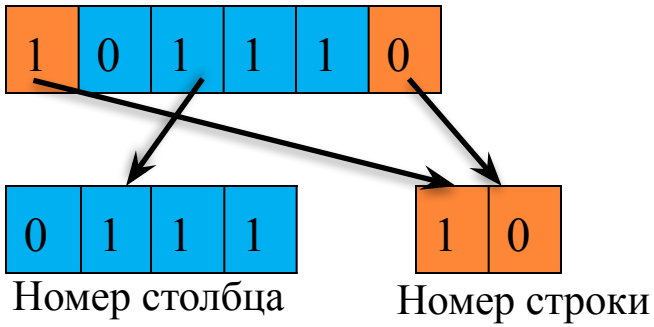
1. Перестановка с расширением (32 → 48) (зачем расширение???)
2. Сложение с подключом (48 + 48)
3. Расщепление (48 = 8 частей по 6 битов)
4. Подстановки через S – блок (8 * (6 → 4) = 32)
5. Перестановки через P – блок (32 → 32)

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

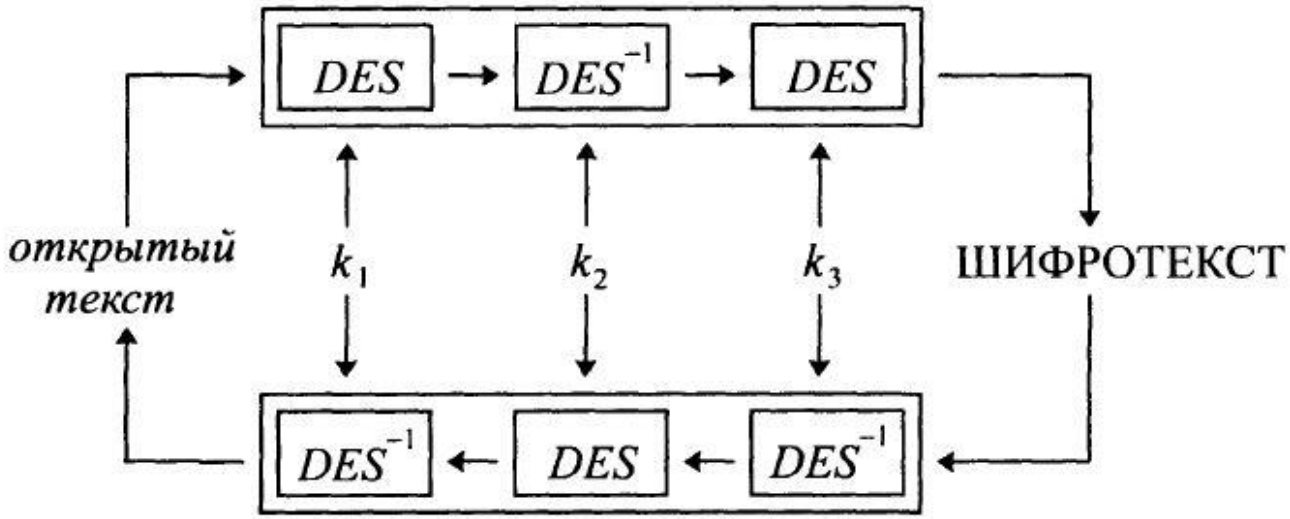
На выходе получается 4 бита

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

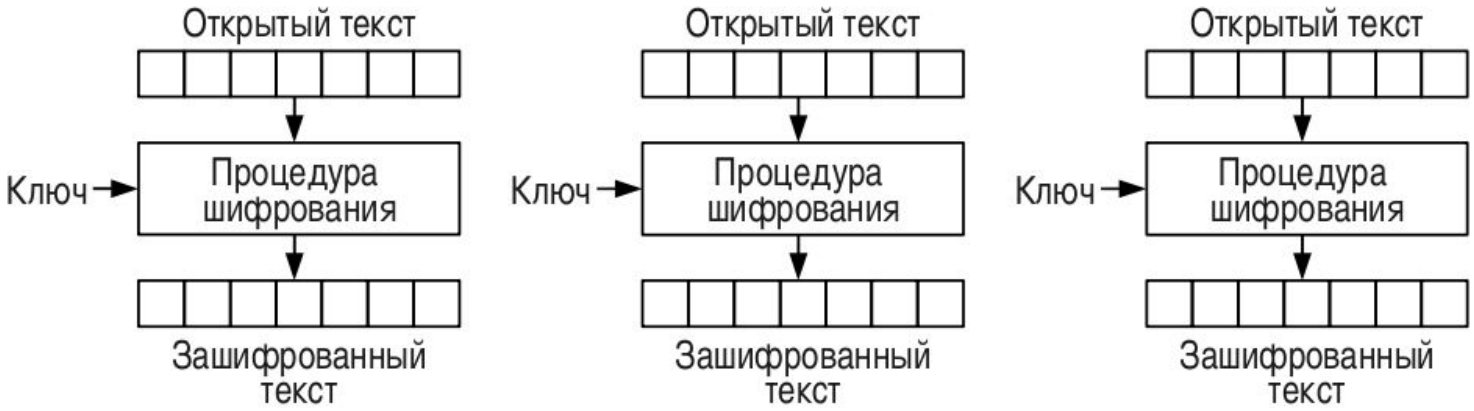
Сообщение: **Заплати старосте 200 руб**

Вставка? Удаление? Повторы? Помехи при передаче?

Режимы шифрования:

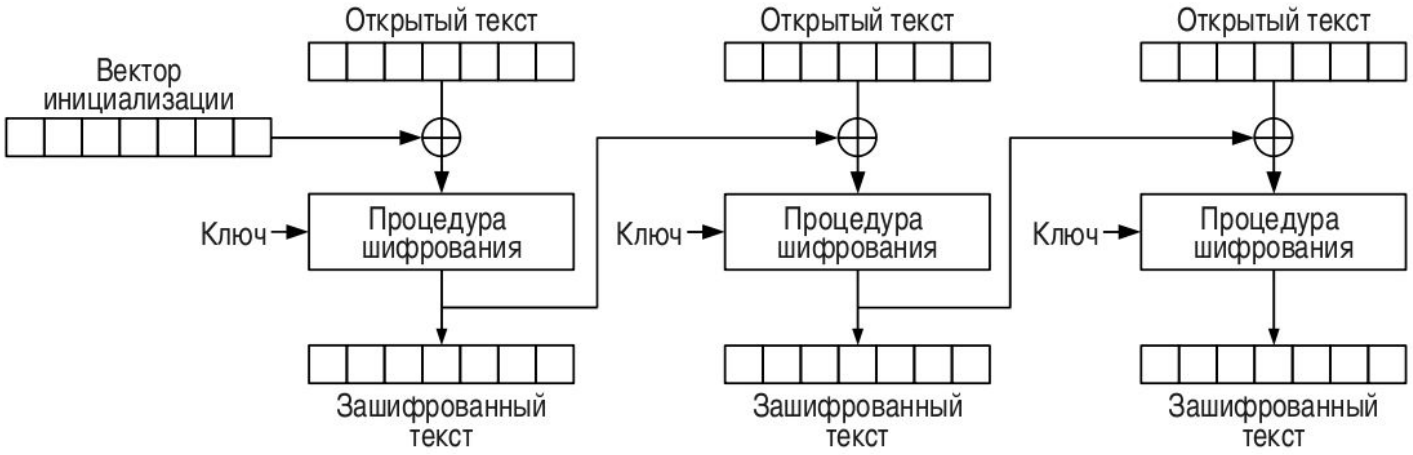
- **ECB** – Electronic Code Book (электронная кодовая книга)
- **CBC** – Cipher Block Chaining (сцепление блоков шифротекста)
- **OFB** – Output FeedBack (обратная связь вывода)
- **CFB** – Cipher FeedBack (обратная связь шифра)

РЕЖИМЫ ШИФРОВАНИЯ - ECB



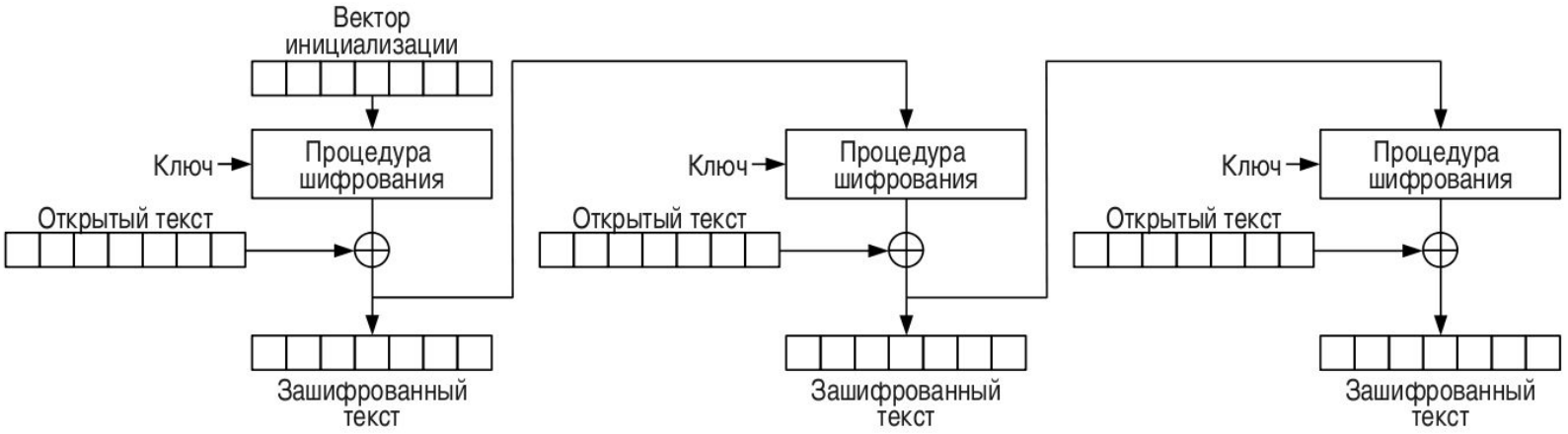
- ECB (*Electronic Code Book – Режим электронной кодовой книги)* – прост в обращении, но не защищен от атак с удалением и вставками. Ошибка в одном бите влияет на целый блок в расшифрованном тексте. Можно работать с блоками независимо и даже распараллелить вычисления.

РЕЖИМЫ ШИФРОВАНИЯ - CBC



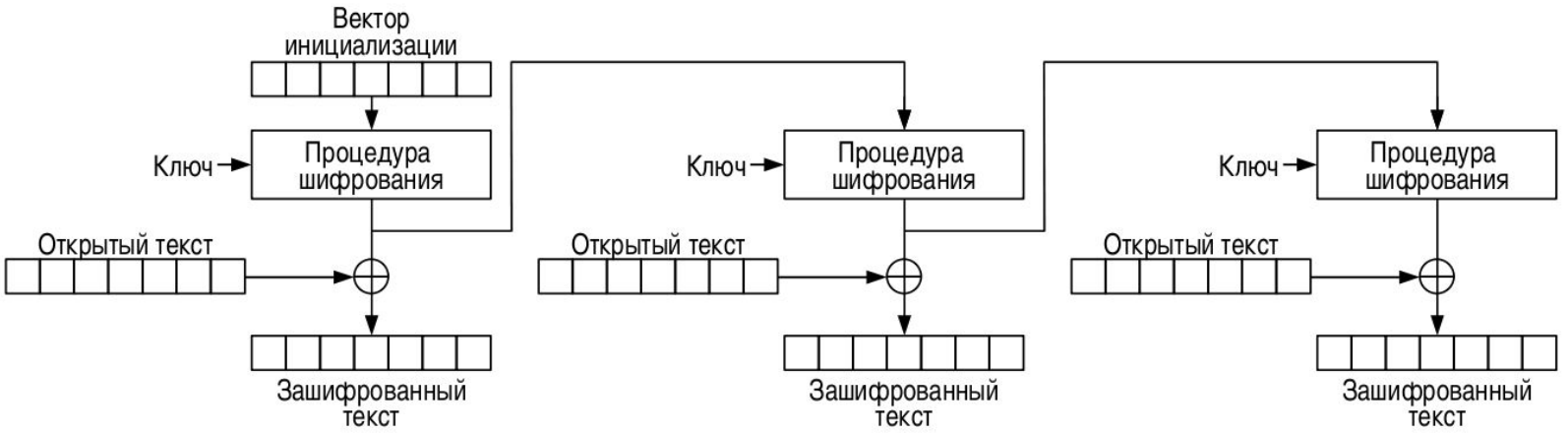
- CBC (*Cipher Block Chaining-Режим сцепления блоков)* – предотвращает потери при атаке со вставкой и удалением. Ошибки при шифровании и в открытом тексте дают ошибку не только в текущем блоке, но и портит следующие блоки.

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 (?)

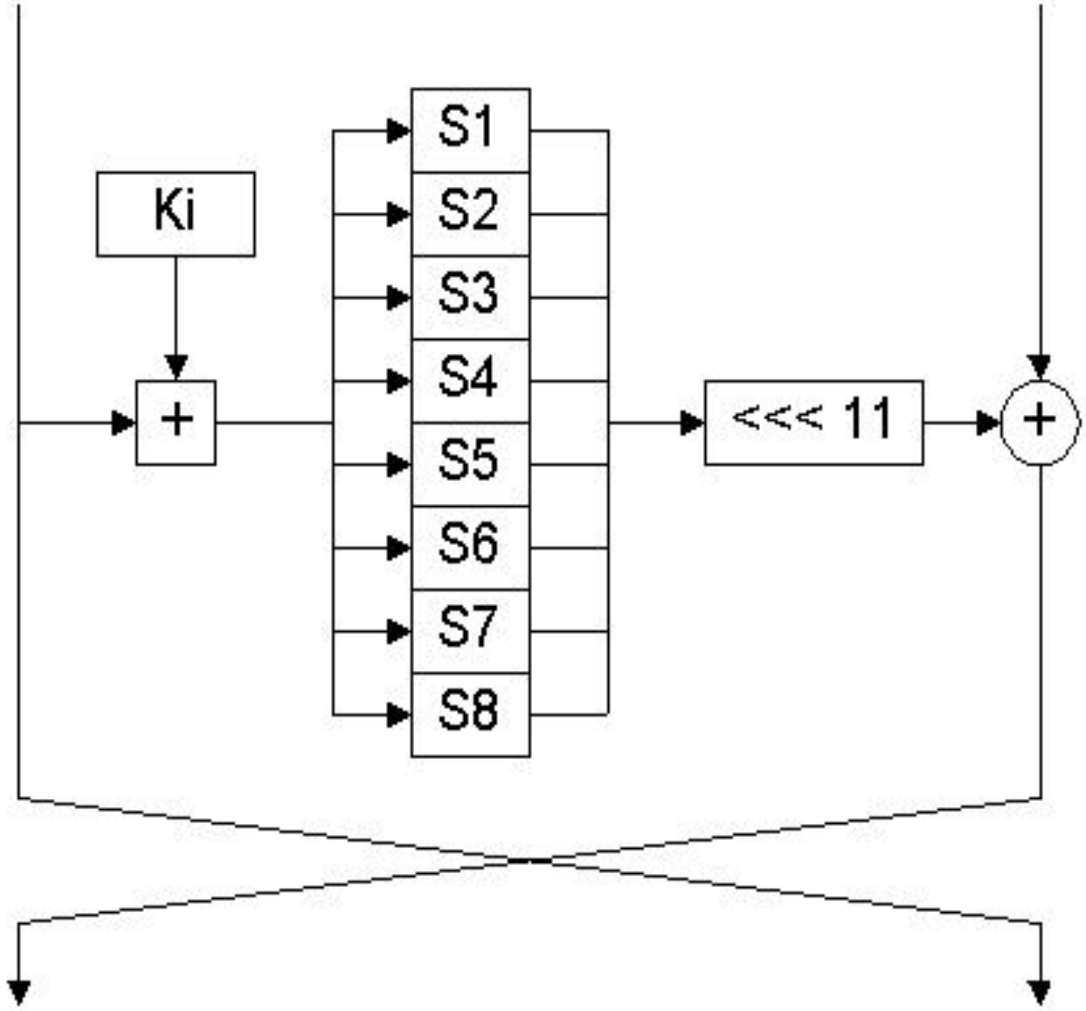
1990 – опубликован для «служебного пользования»

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

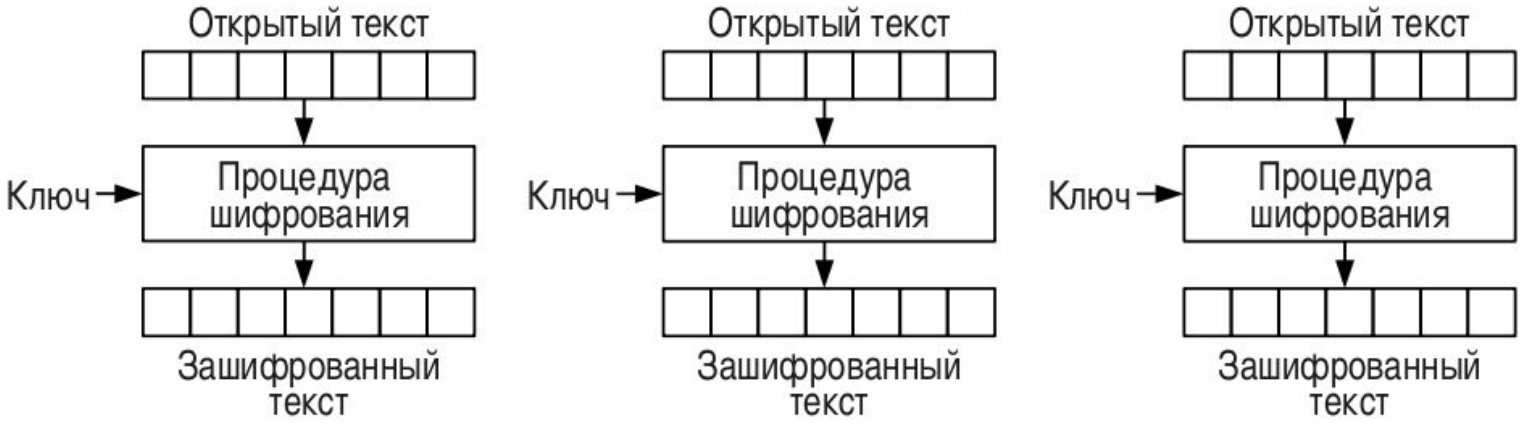
ГОСТ 28147-89



ГОСТ 28147-89 – РЕЖИМЫ ШИФРОВАНИЯ

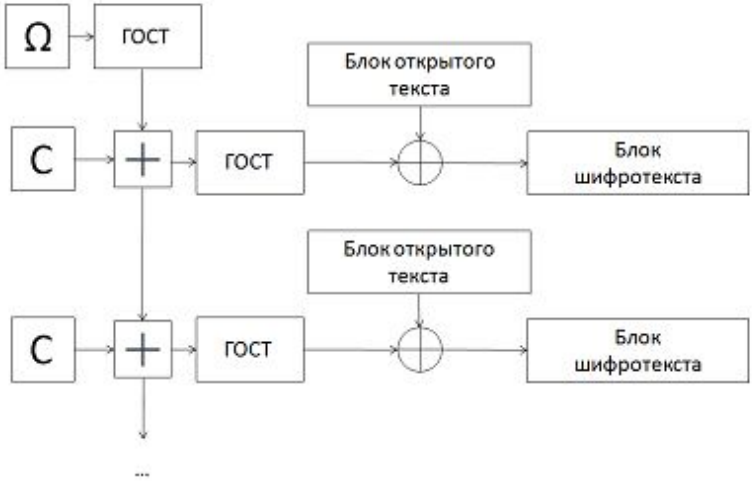
- Простая замена (ECB – electronic code book)
- Гаммирование
- Гаммирование с обратной связью (CFB – Cipher FeedBack)
- *Имитовставка* (MAC – message authentication code)

Простая замена (ECB)

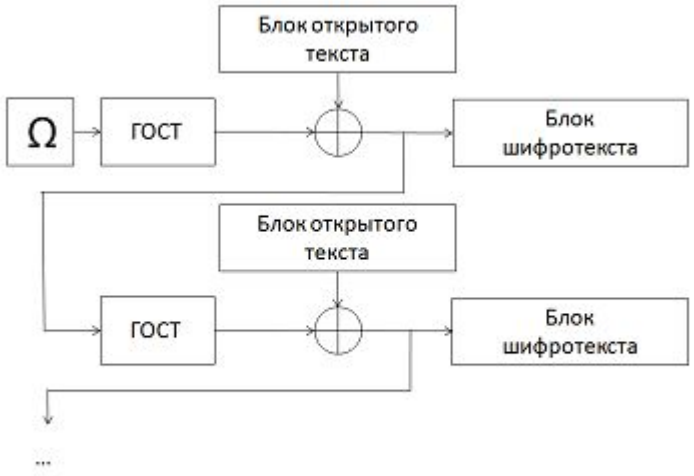


ГОСТ 28147-89 – РЕЖИМЫ РАБОТЫ

Гаммирование



Гаммирование с обратной связью (CFB)



Имитовставка (MAC)

ГОСТ 28147-89 – ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Преимущества

- Криптостойкость (устойчив к линейному и дифференциальному криптоанализу)*
- Скорость работы, эффективность реализации*
- 4 режима работы, возможность аутентификации (имитовставка)

Недостатки

- Не описан способ генерации ключей и таблиц замены – существуют слабые ключи и слабые таблицы замены*

* Субъективно. Существуют различные мнения на этот счет

RIJNDAEL – ПОБЕДИТЕЛЬ AES

1997 – конкурс на AES

2000 – выигрывает Rijndael

2002 – Rijndael признан новым официальным стандартом в США

Разработан 2-мя бельгийскими криптографами: **Rij**men и **Dae**men

Rijndael – **настраиваемый** блочный алгоритм, блоки по 128, 192 или 256 бит.
Но стандартом является только блок в **128 бит**.
Количество раундов зависит от размера блока и длины ключа.

Количество раундов

блок/ ключ	128	192	256
128	**10**	**12**	**14**
192	**12**	**12**	**14**
256	**14**	**14**	**14**

RIJNDAEL - СТРУКТУРА

Блок представляется в виде **матрицы состояний** 4*4(для 128 бит):

32	88	a2	8d
ba	1a	34	b2
f6	30	98	03
43	5a	21	cc

Раундовая функция состоит из:

1. SubBytes – замена по Sbox-ам
2. ShiftRows – сдвиг строк
3. MixColumns – преобразование колонок
4. AddRoundKey – сложение с подключом

RIJNDAEL - SUBBYTES

32	88	a2	8d
ba	1a	34	b2
f6	30	98	03
43	5a	21	cc

Sbox →

4d	d2	c0	bd
8a	bc	9a	d3
bb	29	51	a4
c7	3a	88	b1

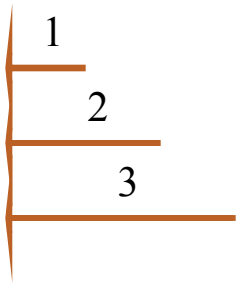
<u>Sbox-ы имеют математизированную структуру:</u>

1. Байт s = 32h = 00110010 = x^5+x^4+x
2. К многочлену s вычисляется обратный многочлен x по модулю $x^8+x^4+x^3+x+1$ (неприводим)
3. Многочлен x умножается на фиксированную матрицу 8*8 и получается многочлен y, который и является результатом Sbox-а.

RIJNDAEL – SHIFTROWS & MIXCOLUMNS

ShiftRows

32	88	a2	8d
ba	1a	34	b2
f6	30	98	03
43	5a	21	cc



32	88	a2	8d
1a	34	b2	ba
98	03	f6	30
cc	43	5a	21

MixColumns

32	88	a2	8d
1a	34	b2	ba
98	03	f6	30
cc	43	5a	21

*

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

=

59	88	a2	8d
20	34	b2	ba
c2	03	e6	30
9d	43	5a	21

*На самом деле умножение на таблицу есть умножение столбца a(X) на фиксированный многочлен c(X) по модулю многочлена $M(X) = X^4 + 1$

RIJNDAEL – ADDROUNDKEY

59	88	a2	8d
20	34	b2	ba
c2	03	e6	30
9d	43	5a	21

$\oplus$

RoundKey

34	03	b2	41
ba	10	81	ac
4c	53	b8	ea
83	c0	00	bd

$=$

72	88	a2	8d
c1	34	b2	ba
90	03	e6	30
ed	43	5a	21

Псевдокод:

```
AddRoundKey(S, K[0]);
for (i=l; i<=9; i++) {
    SubBytes(S);
    ShiftRows(S);
    MixColumns(S) ;
    AddRoundKey(S, K[i]);
}
SubBytes(S);
ShiftRows(S);
AddRoundKey(S,K[10])
```

ПОТОЧНЫЕ ШИФРЫ

m0, m1,… биты открытого текста

k0, k1,… биты ключевого потока

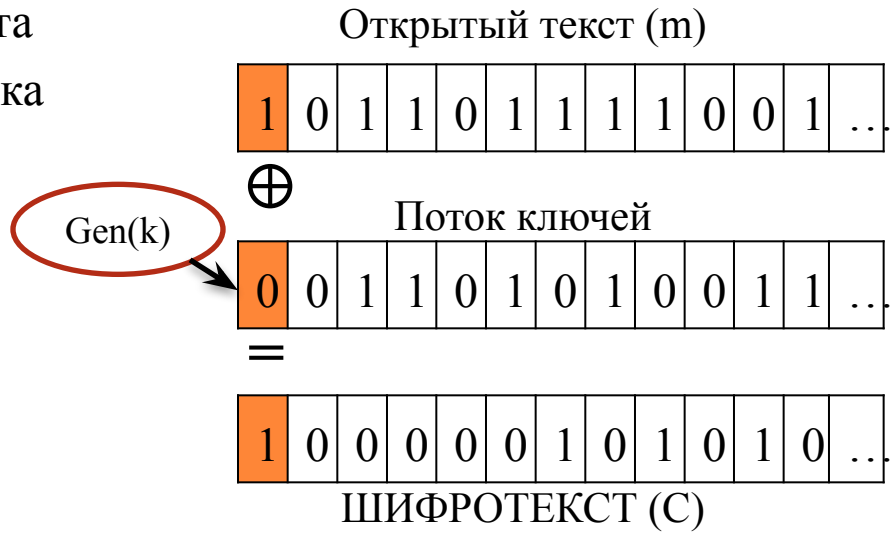
Шифрование :

$$C_i = m_i \oplus k_i$$

Расшифрование:

$$m_i = C_i \oplus k_i$$

Gen(k) – Генератор ключевого потока



ПОТОЧНЫЕ ШИФРЫ – ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Преимущества

- Простая схема шифрования и дешифрования (просто XOR)
- Высокая скорость (исп. для потоковых данных: видео-, аудио-)
- Нет накопления ошибки

Недостатки

- Проблема распределения ключей -нельзя использовать один и тот же ключ дважды:

$$C_1 \oplus C_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

- Проблема генерации ключевого потока

ПОТОЧНЫЕ ШИФРЫ – ТРЕБОВАНИЯ К ГЕНЕРАТОРУ КЛЮЧЕВОГО ПОТОКА

<u>Ключевой поток должен:</u>

- Иметь большой период.

Найдется **n: $k_i = k_i + n$** для $\forall i$

n – период последовательности

- Иметь псевдо-случайные свойства.

В идеале, если кто-то знает первый миллиард битов ключевой последовательности, вероятность угадать следующий бит не должна превышать 50%.

ПОТОЧНЫЕ ШИФРЫ – ОДНОРАЗОВЫЙ ШИФР-БЛОКНОТ

- В 1917 Гильберт Вернам запатентовал одноразовый шифр-блокнот (шифр Вернама)
- Суть – XOR с ключом той же длины, что и сообщение
- При этом ключ должен обладать тремя критически важными свойствами:

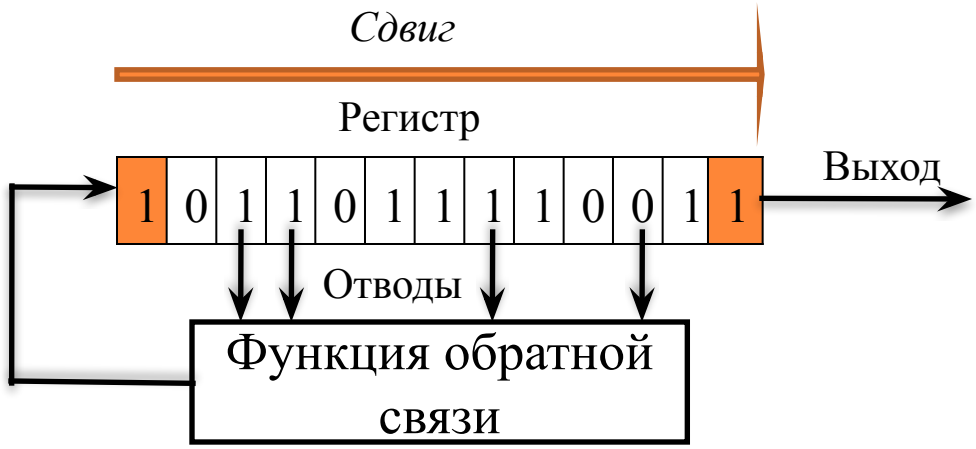
  - иметь случайное равномерное распределение;

  - совпадать по размеру с заданным открытым текстом;

  - применяться только один раз.

- <u>Обладает абсолютной криптостойкостью</u>

ПОТОЧНЫЕ ШИФРЫ - РСЛОС



- **РСЛОС** – **Р**егистр **С**двига с **Л**инейной **О**братной **С**вязью (**LFSR - L**inear **F**eedback **S**hift **R**egister)
- Для функции обратной связи рекомендуется использовать нелинейные функции. Однако это сложно осуществимо на практике

РСЛОС – ЛИНЕЙНАЯ ФУНКЦИЯ ОБРАТНОЙ СВЯЗИ

<u>В качестве функции обратной связи берется логическая операция **XOR**:</u>

$[c_1,\ldots c_l]$ – последовательность битов, на отводах – 1, остальные – 0

$[s_{l-1}, \ldots s_1, s_0]$ - начальное положение регистра

<u>На выходе регистра получается:</u>

$s_0, s_1, \ldots s_{l-1}, s_l, s_{l+1}, \ldots$

где для j >= 1 :

$$\mathbf{s_j = c_1 \cdot s_{j-1} \oplus c_2 \cdot s_{j-2} \oplus \ldots \oplus c_l \cdot s_{j-l}}$$

Свойства выдаваемой РСЛОС последовательности связанны со свойствами двоичного **многочлена ассоциированного с регистром** :

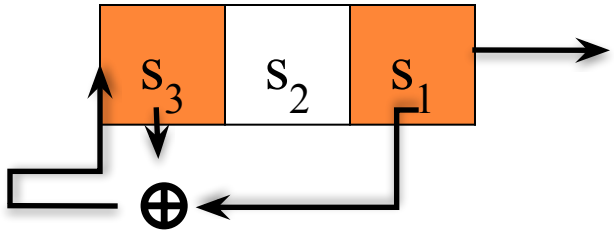
$$\mathbf{C(X) = 1+c_1X+c_2X^2+\ldots+c_lX^l \in F_2[X]}$$

РСЛОС - ПРИМЕР

РСЛОС с ассоциированным многочленом

$X^3 + X^1 + 1$

$s_j = s_{j-3} \oplus s_{j-1}$



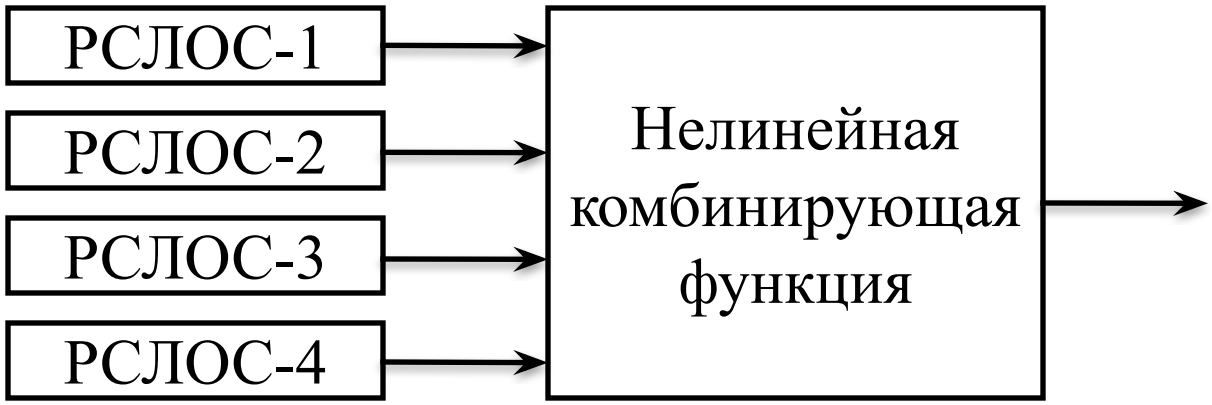
Номер шага	Состояние	Ген-мый бит
0	[0,0,1]	-
1	[1,0,0]	1
2	[1,1,0]	0
3	[1,1,1]	0
4	[0,1,1]	1
5	[1,0,1]	1
6	[0,1,0]	1
7	[0,0,1]	0

РСЛОС - КОМБИНИРОВАНИЕ

Комбинирующая функция:

$$f(x_1,x_2,x_3,x_4,x_5)=1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \cdot x_5 \oplus x_1 \cdot x_2 \cdot x_3 \cdot x_5$$

Пусть есть n РСЛОС с попарно различными периодами $l_1, \ldots l_n$, каждый из которых больше 2, тогда линейная сложность потока ключей, генерируемого $f(x_1, \ldots x_n)$, вычисляется с помощью $f(l_1, \ldots l_n)$



СТАНДАРТ GSM – A3, A5, A8

- **GSM** (Groupe Spécial Mobile, позже Global System for Mobile Communications) — глобальный стандарт цифровой мобильной сотовой связи. Разработан под эгидой ETSI в конце 1980-х.

<u>Шифрование в GSM обеспечивается 3 стандартами:</u>

- A3 – аутентификация (генерирует SRES по RAND и K_i)
- A5 – поточный шифр (шифрует разговор с помощью K_c)
- A8 – создание сеансовых ключей (генерирует K_c по RAND и K_i)

A3, A5, A8 и K_i зашиты в SIM-карте абонента.

A5 – ПОТОЧНЫЙ ШИФР В GSM

Существует несколько модификаций:

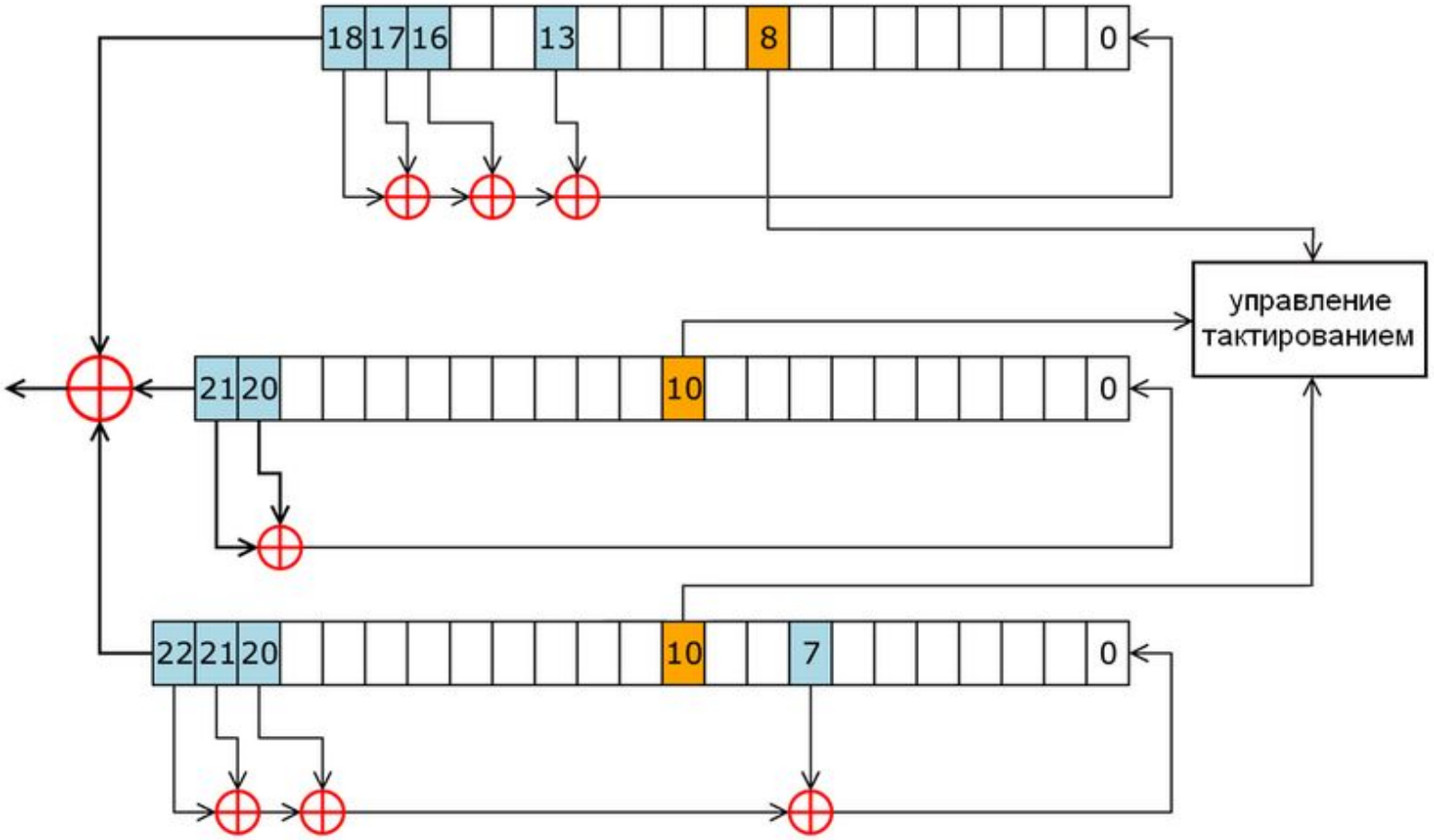
- A5/0 : шифрования нет
- A5/1 : стандарт
- A5/2 : понижена криптостойкость, добавлен еще 1 регистр
- A5/3 : новый алгоритм KASUMI (1999), утвержден для 3G

A5/1:

1. 3 РСЛОС (R1, R2, R3) по 19, 22 и 23 бита
2. Многочлены обратных связей:

- $X^{19} + X^{18} + X^{17} + X^{14} + 1$ для R1
- $X^{22} + X^{21} + 1$ для R2
- $X^{23} + X^{22} + X^{21} + X^{8} + 1$ для R3

A5/1 - СТРУКТУРА



A5/1 - СТРУКТУРА

Управление тактированием осуществляется специальным механизмом:

- в каждом регистре есть **биты синхронизации**: 8 (R1), 10 (R2), 10 (R3),
- вычисляется функция

F = x&y|x&z|y&z, где x, y и z — биты синхронизации R1, R2 и R3

- сдвигаются только те регистры, у которых **бит синхронизации равен F** (фактически, сдвигаются регистры, синхробит которых принадлежит большинству)

Выходной бит системы — результат операции XOR над выходными битами регистров.