БЛОЧНЫЕ ШИФРЫ

БЛОЧНЫЙ ШИФР

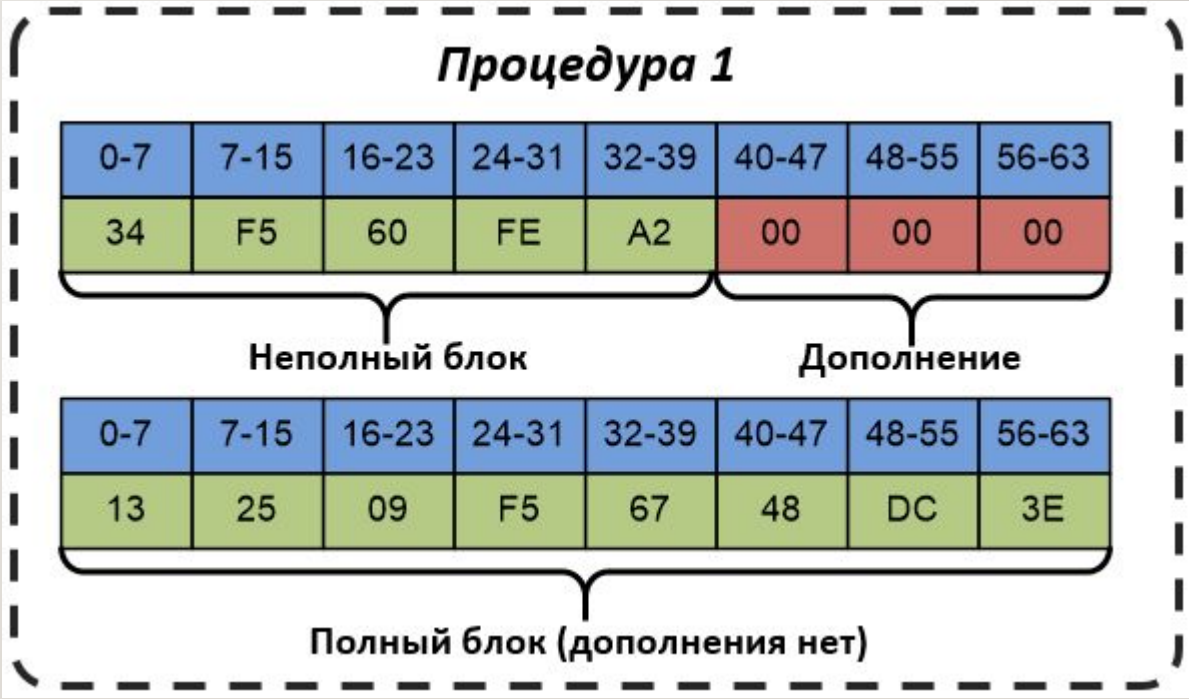
- Шифр с симметричным ключом, разбивающий перед шифрованием открытый текст на n-битовые блоки и далее шифрующий сообщение блоками.
- Алгоритмы дешифрования и шифрования – инверсные, оба работают на одном и том же секретном ключе.
- Современные блочные шифры обрабатывают блоки длиной n = 64, 128, 256, 512, 1024 бит.

ПРИМЕР

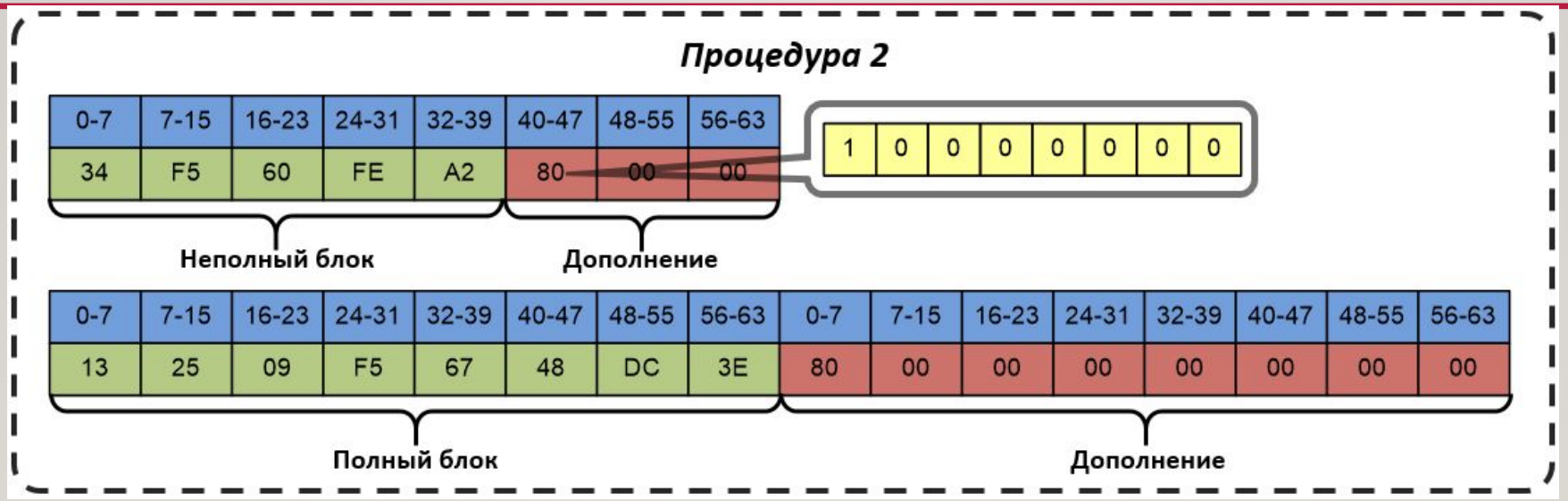
- Сколько дополнительных бит надо добавить к сообщению длиной 100 символов, если кодирование одного символа требует 8 бит и блочный шифр работает с блоками длиной 64 бита?

ОПЕРАЦИЯ ДОПОЛНЕНИЯ СООБЩЕНИЯ ГОСТ 34.13—2015. ПРОЦЕДУРА 1

Остаток в сообщении дополняется нулями до размера полного блока



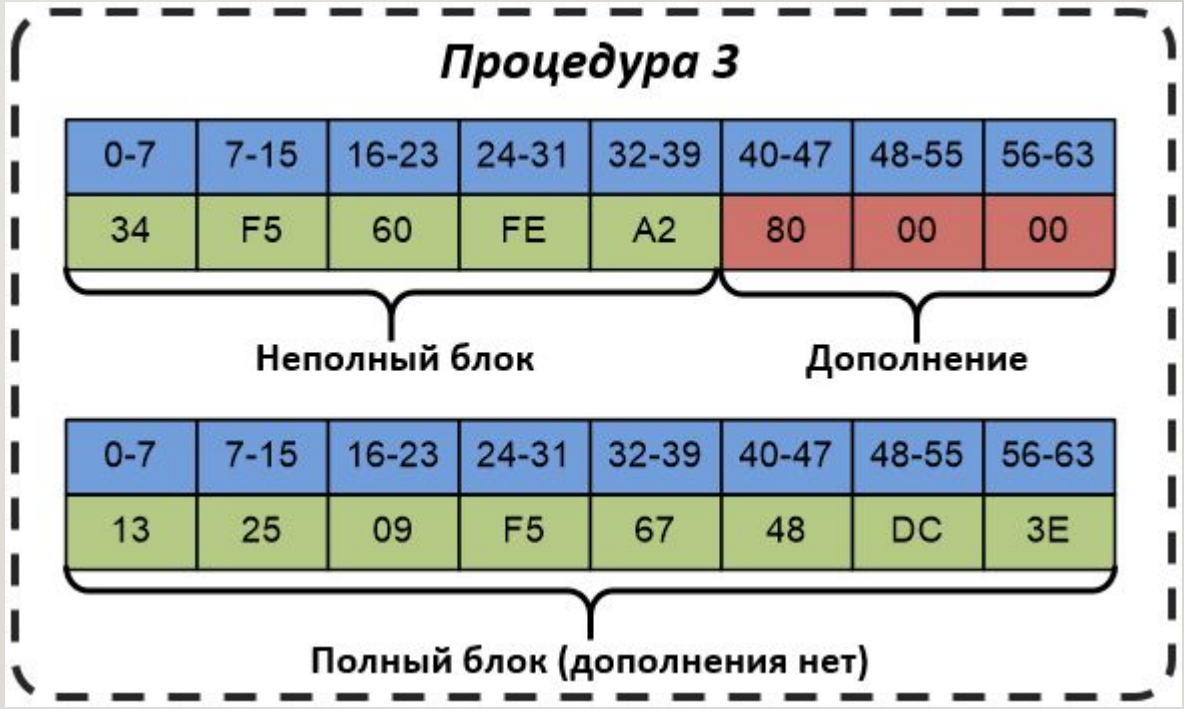
ОПЕРАЦИЯ ДОПОЛНЕНИЯ СООБЩЕНИЯ ГОСТ 34.13—2015. ПРОЦЕДУРА 2



1. В первый бит остатка пишется единица, а остальное место заполняется нулями до размера полного блока.
2. Добавляется целый дополнительный блок, начинающийся с единичного бита, с заполнением остальных разрядов этого дополнительного блока нулями.

ОПЕРАЦИЯ ДОПОЛНЕНИЯ СООБЩЕНИЯ ГОСТ 34.13—2015. ПРОЦЕДУРА 3

Если длина сообщения кратна размеру блока, то никаких дополнений делать не нужно, в противном случае остаток исходного сообщения дополняется до размера полного блока единичным начальным битом с последующим заполнением нулями.



БЛОЧНЫЙ ШИФР. ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ

1) если шифр спроектирован как шифр подстановки, каждый бит открытого текста может быть заменен на 0 или 1, тогда исходный текст и шифротекст могут иметь различное число единиц.
2) если шифр спроектирован как шифр перестановки, то биты открытого текста только меняются местами.

ПРИМЕР

Блочный шифр шифрует блок размером n=64 бита. Зашифрованный текст содержит 10 единиц.

Сколько проб при полном переборе должен выполнить криптоаналитик, чтобы получить открытый текст, соответствующий перехваченному шифротексту, если:

а) шифр спроектирован как шифр подстановки;

б) шифр спроектирован как шифр перестановки.

ОТВЕТ

- А) 2^{64}
- Б) $C_{64}^{10} \approx 151 \cdot 10^9$

ОСНОВНЫЕ ОПЕРАТОРЫ БЛОКОВЫХ ШИФРОВ:

1) операторы перестановки, называемые P-боксами;

2) операторы подстановки, называемые S -боксами;

3) операция исключающего ИЛИ;

4) циклический сдвиг;

5) замена;

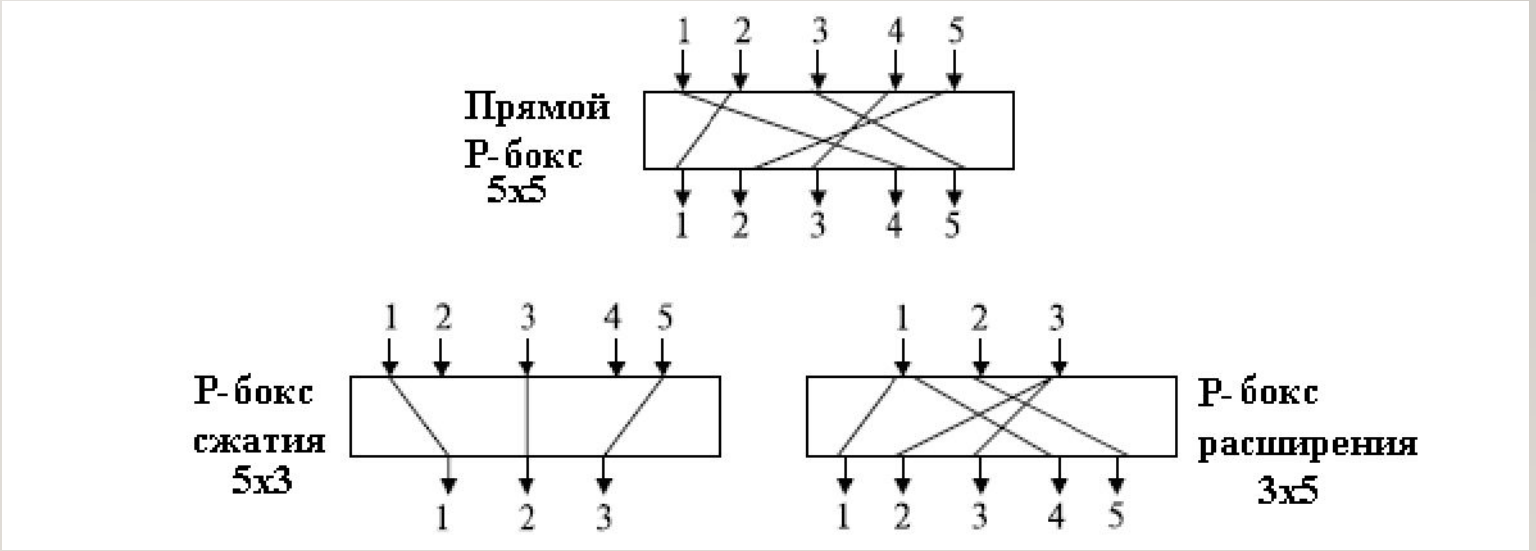
6) разбиение и объединение блока.

P-БОКСЫ

P-бокс (блок перестановки) подобен традиционному шифру перестановки.

Возможны 3 типа P-боксов:

- прямые P-боксы (простая перестановка символов, n входов и n выходов, всего возможно n! отображений);
- P-боксы расширения
- P-боксы сжатия



S -БОКСЫ

S -бокс (блок подстановки) – это миниатюрный шифр подстановки.

На вход в S -бокс может подаваться n -битовый блок, а на выходе выйти уже m-битовый блок, где не всегда m = n

S -боксы делятся на **линейные** и **нелинейные**.

В линейном S -боксе эту связь можно записать в виде линейных соотношений

В нелинейном S -боксе линейные соотношения для каждого выхода задать нельзя.

ПРИМЕР

S -бокса размера 3x2. Первый бит входа определяет строку, два следующих бита входа определяют столбец. Два бита на выходе – это значение на пересечении выбранных строки и столбца.

Биты 101 преобразуются в биты 00

Самый левый бит входа ↓	00	01	10	11
0	00	10	01	11
1	10	00	11	01

← Самые правые биты входа

ОПЕРАЦИЯ XOR

Свойства операции XOR:

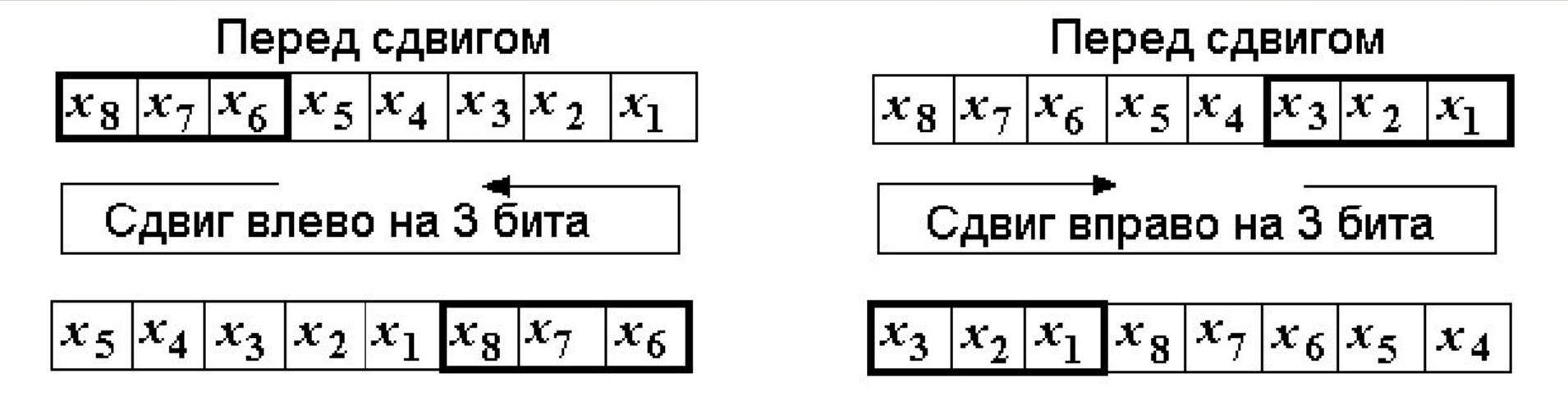
1. Замкнутость: если x, y – n-битовые слова, то $x \oplus y = z$, где z – n-битовое слово.
2. Ассоциативность: $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.
3. Коммутативность: $x \oplus y = y \oplus x$.
4. Существование нулевого элемента с условием $x \oplus (00...0) = x$.
5. Существование инверсии – операция XOR слова с самим собой дает нулевой элемент $x \oplus x = (00...0)$.

ЦИКЛИЧЕСКИЙ СДВИГ

Циклический правый (левый) сдвиг сдвигает каждый бит в n -битовом слове на k позиций вправо(влево).

Свойства циклического сдвига:

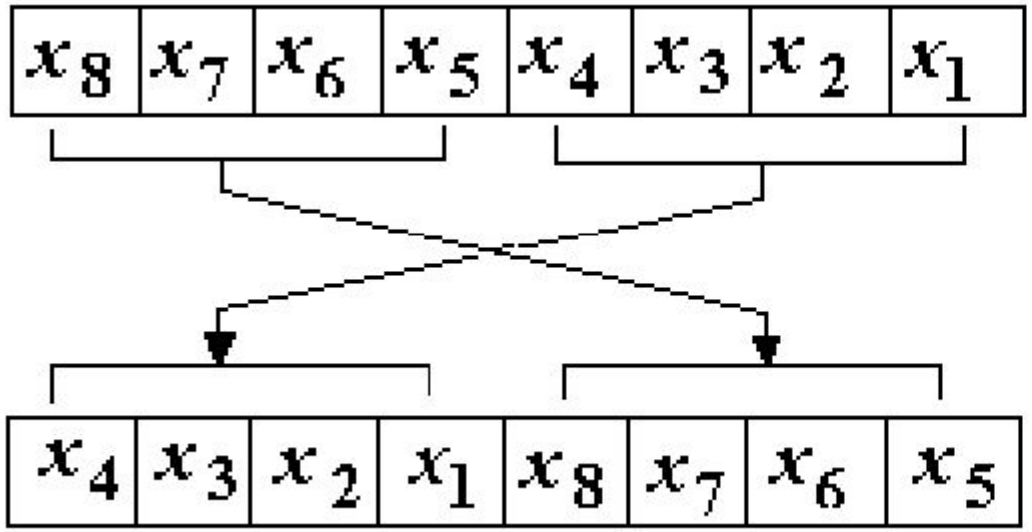
- смещение по модулю n (если k>n, то входная информация сдвигается на k modn бит;
- если смещение делается неоднократно, то вновь может появиться исходное n -битовое слово



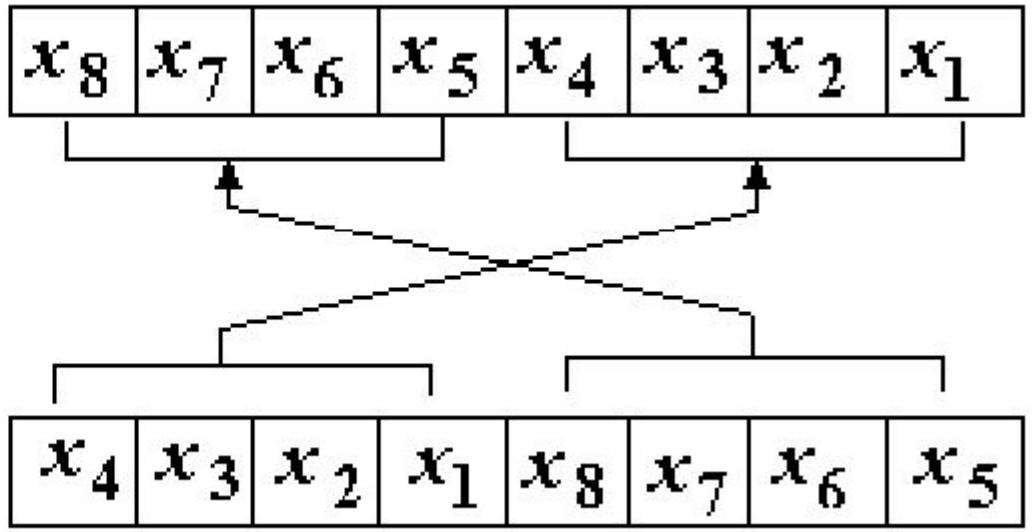
ЗАМЕНА

Замена - частный случай операции циклического сдвига на k=n / 2 битов (где n – четное).

Шифрование



Расшифрование



РАЗБИЕНИЕ И ОБЪЕДИНЕНИЕ

Разбиение разделяет n-битовое слово пополам, создавая два слова равной длины.

Объединение связывает два слова равной длины, чтобы создать n - битовое слово.

Эти операции инверсны друг другу: если одна используется для шифрования, то другая – для расшифрования.

РАУНДЫ БЛОЧНЫХ ШИФРОВ

Однократное применение комбинации операторов блоковых шифров называется раундом блокового шифра.

Для каждого раунда из основного секретного ключа k шифра с помощью алгоритма разворачивания ключа генерируется подключ раунда ki.

ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ БЛОКОВЫХ ШИФРОВ

- Сеть Фейстеля
- Подстановочно-перестановочная сеть
- Шифры со структурой квадрат

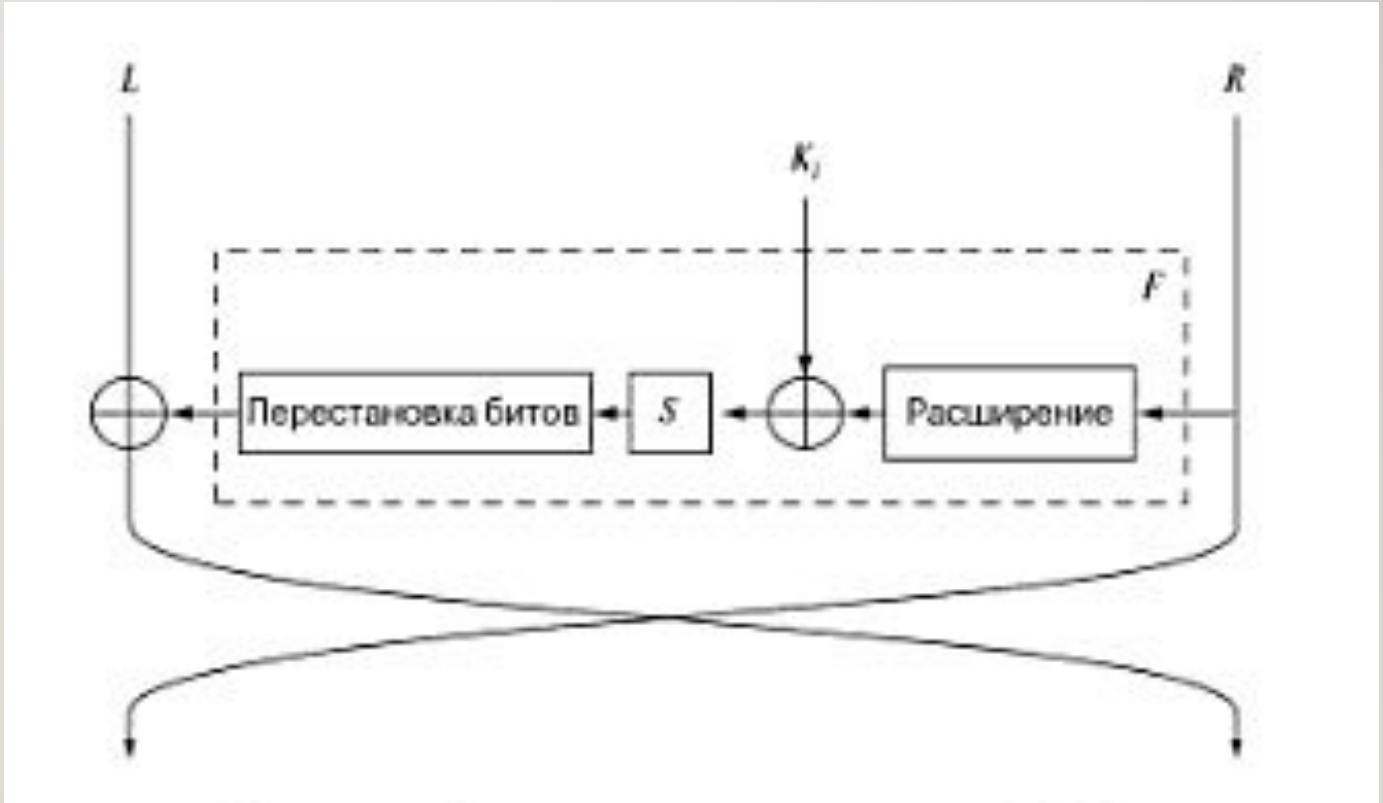
ТРЕБОВАНИЯ К СОВРЕМЕННЫМ БЛОЧНЫМ ШИФРАМ

- ***Высокая стойкость.***
- ***Наличие лавинного эффекта.***
- ***Стойкость к атакам по выбранному тексту.***
- ***Переносимость.***
- ***Эффективность работы на микропроцессорах.***
- ***Экономичная реализация в виде электронных устройств.***
- ***Эффективность работы с любыми видами входных данных.***
- ***Простой программный код реализации.***
- ***Плоское пространство ключей.***

DES (DATA ENCRYPTION STANDARD)

- Ключ 56 бит
- Размер блока 64 бит
- Раундов 16
- Раундовые подключи 48 бит
- S-матрицы 8 таблиц соответствий,

6 бит ⟶ 4-бита



ФУНКЦИОНАЛЬНЫЕ БЛОКИ DES

- Шифр Файстеля - упрощает структуру шифра и гарантирует перемешивание правой и левой половин текста;
- Сложение текста с подключом с помощью операции XOR гарантирует перемешивание ключа и данных;
- Сочетание S-матриц, функции расширения и перестановки битов обеспечивает диффузию.

СЛАБЫЕ МЕСТА

- Каждый из подключей представляет собой не более чем выборку битов ключа шифрования.

Слабые ключи (в шестнадцатеричной системе исчисления)	
До удаления проверочных бит (64 бита)	Действующий ключ (56 бит)
0101 0101 0101 0101	0000000 0000000 = $[0]^{28}[0]^{28}$
1F1F 1F1F 1F1F 1F1F	0000000 FFFFFFF = $[0]^{28}[1]^{28}$
E0E0 E0E0 E0E0 E0E0	FFFFFFF 0000000 = $[1]^{28}[0]^{28}$
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF = $[1]^{28}[1]^{28}$

- Свойство комплементарности (дополнения) - если зашифровать дополнение открытого текста с помощью дополнения ключа, мы получим значение, которое является дополнением шифрованного текста.

$$y = E_k(x) \Rightarrow \overline{y} = E_{\overline{k}}(\overline{x})$$

TRIPLE DES

Схема, основанная на повторных приложениях DES.

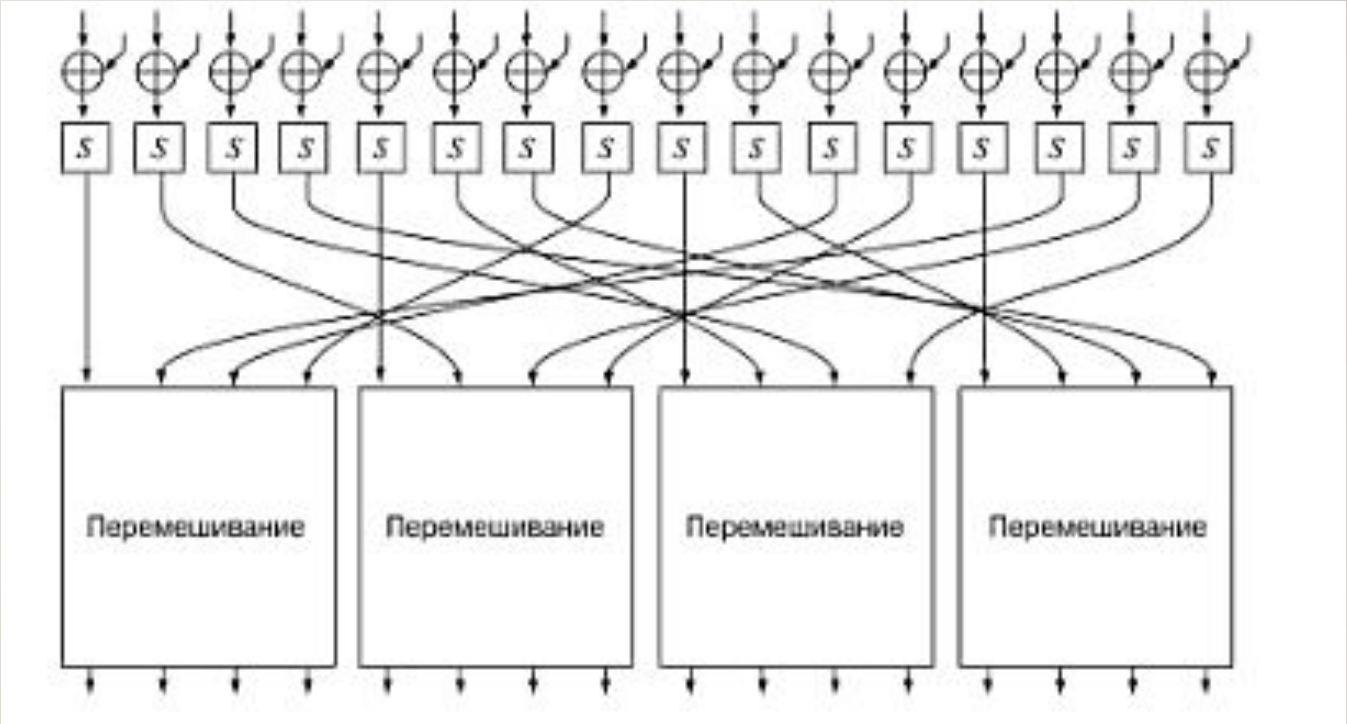
Используется для обеспечения совместимости с существующими системами.

Недостатки:

- Слабые ключи;
- Свойство комплементарности;
- Скорость.

AES (ADVANCED ENCRYPTION STANDARD)

- Ключ 128, 192, 256 бит
- Размер блока 128 бит
- Раундов 10-14
- Раундовые подключи 128 бит



ФУНКЦИОНАЛЬНЫЕ БЛОКИ AES

- Операции XOR складывают значения ключа с данными;
- S- матрицы обеспечивают нелинейность;
- Функции перемешивания и перестановки гарантируют наличие диффузии.

TWOFISH

- Ключ 128, 192, 256 бит
- Размер блока 128 бит
- Раундов 16
- Раундовые подключи 128 бит
- S-матрицы не являются постоянными