Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

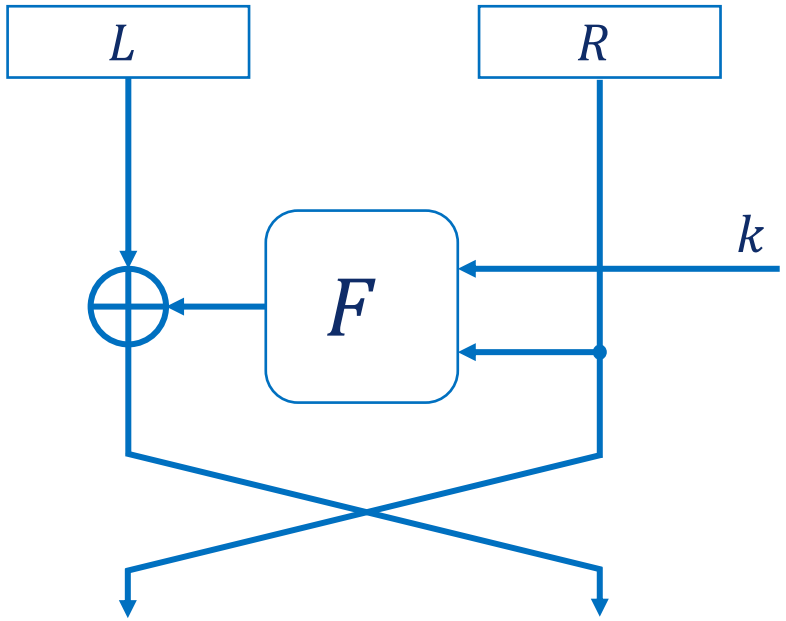
Зарубежные стандарты симметричного шифрования

Data Encryption Standard

- **Data Encryption Standard** (**DES**) — первый стандарт симметричного шифрования.
- История создания:
  - 1972 г. — инициатива НБС США о создании стандарта.
  - 1976 г. — DES принят в качестве стандарта.
  - 1977 г. — публикация стандарта FIPS PUB 46.
- Характеристики шифра:
  - Длина блока: 64 бита;
  - Длина ключа: 64 (56) бита;
  - Число раундов: 16;
  - Основа: сеть Фейстеля.

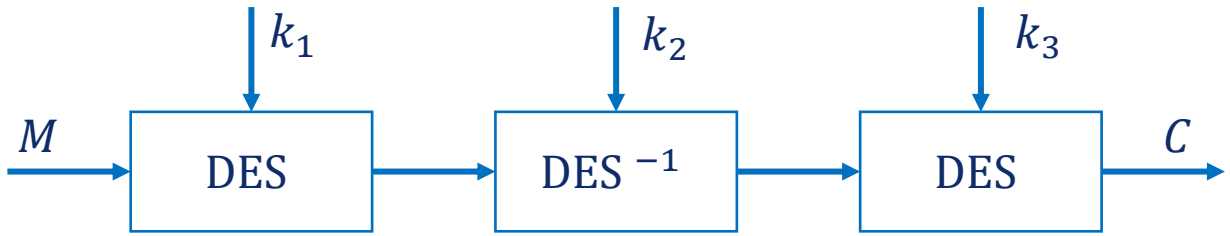
Схема шифрования DES

- **Нелинейная функция F**:
  - перестановка с расширением до 48 бит;
  - поразрядное сложение по модулю 2 с 48-битовым раундовым ключом;
  - замена 8-ми 6-битовых блоков на 4-битовые блоки посредством таблиц замен, называемых S-блоками;
  - перестановка с помощью P-блока.

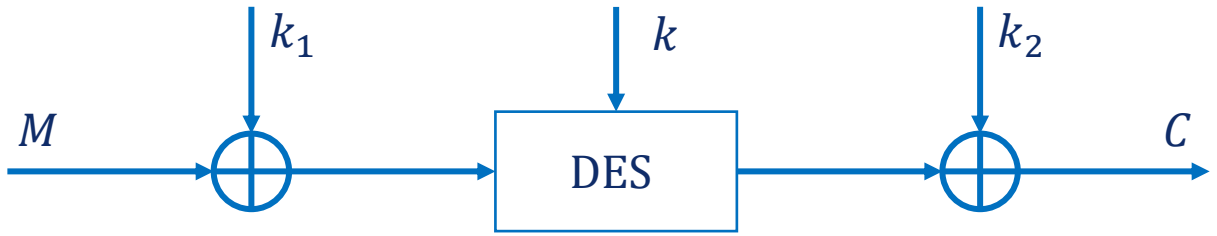


Модификации DES

- **3-DES:**



- **DESX:**



Advanced Encryption Standard

- **Advanced Encryption Standard** (**AES**).
- История создания:
  - 1997 г. — объявление конкурса на создание AES.
  - 1999 г. — финал конкурса (5 шифров).
  - 2000 г. — выбор победителя (Rijndael).
  - 2001 г. — публикация стандарта FIPS PUB 197.
- Характеристики шифра:
  - Длина блока: 128 бит;
  - Длина ключа: 128/192/256 бит;
  - Число раундов: 10/12/14;
  - Основа: SP-сеть.

Этапы раунда зашифрования

- Блоки представляются в виде матриц байтов:
  - $\mathbf{A} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$
- Этапы раунда зашифрования реализуют преобразования матрицы $\mathbf{A}$:
  - **SubBytes**: замена элементов матрицы;
  - **ShiftRows**: циклический сдвиг строк матрицы;
  - **MixColumns**: перемешивание столбцов матрицы;
  - **AddRoundKey**: наложение раундового ключа.

SubBytes

- Замена байтов блока данных мультипликативно обратными значениями в поле Галуа F_{2^8}, построенном с помощью неприводимого многочлена $f = x^8 + x^4 + x^3 + x + 1$.
- Аффинное преобразование результата предыдущей замены:

$$-\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

ShiftRows

- Циклический сдвиг строк влево на число позиций, равное номеру строки:

$$- \ \mathbf{A} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \mapsto \acute{\mathbf{A}} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}$$

MixColumns

- Представление столбцов как многочленов третьей степени:
  - $\mathbf{A} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$

$$a(x) = a_{00} + a_{10}x + a_{20}x^2 + a_{30}\,x^3$$

- Умножение многочленов-столбцов на многочлен-константу, заданный над F_{2^8}:
  - $\acute{a}(x) = a(x) \cdot c(x) \left(\mathrm{mod}\, x^4 + 1\right)$;
  - $c(x) = (0,0,0,0,0,0,1,0) + (0,0,0,0,0,0,0,1) \cdot x + (0,0,0,0,0,0,0,1) \cdot x^2 + (0,0,0,0,0,0,1,1) \cdot x^3$.

Развертывание раундовых ключей

- **AddRoundKey:**
  - Поразрядное сложение по модулю 2 блока данных и раундового ключа.
- Обозначения:
  - K — массив столбцов матрицы исходного ключа;
  - W — массив столбцов матриц раундовых ключей;
  - N_k — число столбцов в ключе;
  - N_r — число раундов;
  - RC — массив раундовых констант;
  - $\mathrm{RotBytes}$ — циклический сдвиг влево на один байт.
- $RC_i = x^i \ (\mathrm{mod}\ x^8 + x^4 + x^3 + x + 1)$

Алгоритмы развертывания раундовых ключей

- Длина ключа 128, 192 бита:

```
for (i = 0; i < Nk; i++)
{
    W[i]=K[i];
}
for (i=Nk; i < 4*(Nr + 1); i++)
{
    T = W[i-1];
    if (i % Nk == 0)
        T = SubBytes(RotBytes(T))^RC[i/Nk]);
    W[i] = W[i - Nk]^T;
}
```

- Длина ключа 256 бит:

```
for (i = 0; i < Nk; i++)
{
    W[i]=K[i];
}
for (i=Nk; i < 4*(Nr + 1); i++)
{
    T = W[i-1];
    if (i % Nk == 0)
        T = SubBytes(RotBytes(T))^RC[i/Nk]);
    else if (i % Nk == 4)
        T = SubBytes(T);
    W[i] = W[i - Nk]^T;
}
```

Алгоритмы зашифрования и расшифрования

- **Зашифрование:**

```
AddRoundKey(S, K[0]);
for (i = 1; i < Nr; i++)
{
        SubBytes(S);
        ShiftRows(S);
        MixColumns(S);
        AddRoundKey(S,K[i]);
}
SubBytes(S);
ShiftRows(S);
AddRoundKey(S, K[Nr]);
```

- **Расшифрование:**

```
AddRoundKey(S, K[Nr]);
InvShiftRows(S);
InvSubBytes(S);
for (i = Nr - 1; i > 0; i--)
{
        AddRoundKey(S, K[i]);
        InvMixColumns(S);
        InvShiftRows(S);
        InvSubBytes(S);
}
AddRoundKey(S, K[0]);
```

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru