Немного про блочные шифры

ОПР(Блочный шифр)

Блочный шифр это криптосистема $(\{0,1\}^n, \{0,1\}^k, \{0,1\}^n, E, D)$ где:

- $\mathcal{M} = \{0,1\}^n$
- $\mathcal{K} = \{0,1\}^k$
- $\mathcal{C} = \{0,1\}^n$
- n - длина блока
- k - длина ключа

Идея применять к маленьким кусочкам открытого текста сложные функции(которые нужно задать таблицей)

Затем перемешаем эти блоки(например с помощью линейного преобразования либо другая простая функция). Действуем этой функцией на весь большой блок открытого текста

Итеративная схема блочного шифра

Есть

- $f : \{0,1\}^n \to\!\!\!\!\to \{0,1\}^n$ - сложное, локальное преобразование
- $g : \{0,1\}^n \to\!\!\!\!\to \{0,1\}^n$ - простое, глобальное преобразование
- $h : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ берёт че-то и ключ и возращает че-то другое
- $h_k = h(\_, k)$ **т.е в преобразование закладываем ключ k**

По итогу получаем формулу для криптограммы

$$c = (h_k \circ f \circ g)^r(m)$$

- r - это число раундов

Конструкция фейстеля

Открытый текст разобъем его на 2 части(n - длина открытого текста - четное число)

$m = L_0 R_0$, где:

- $L_0, R_0 \in \{0,1\}^{\frac{n}{2}}$

теперь преобразовываем эти полублоки

$\forall i = \{1, \cdots, r\}$:

- $L_i = R_{i-1}$
- $R_i = L_{i-1} \bigoplus f(R_{i-1}, k_i)$
  - k_i - раундовый ключ, как-то получается из основного ключа

Проделываем процедуру и в конце получаем L_r, R_r.

Формула для криптограмы c:

$$c = R_r L_r$$

Как расшифровывать криптограмму c?

пусть $c = u_0 v_0$

$\forall i \in \{1, \cdots, r\}$

- $u_i = v_{i-1}$
- $v_i = u_{i-1} \bigoplus f(v_{i-1}, k_{r+1-i})$

Проделываем процедуру и получаем v_r, u_r

Тогда формула для открытого текста это

$$m = v_r u_r$$

Д-во

С помощью индукции по i нужно показать, что:

- $u_i = R_{r-i}$
- $v_i = Lr - i$

Б.И

$i = 0 : \begin{cases} u_0 = R_r \\ v_0 = L_r \end{cases}$

Ш.И от $(i-1) \to i$

- по опр конструкции Фейстеля $L_i = R_{i-1}$

$u_i = v_{i-1} = [\text{П.И}] = L_{r-i+1} = R_{r-i}$

$v_i = u_{i-1} \bigoplus f(v_{i-1}, k_{r+1-i})$

- **по П.И:**
  - $u_{i-1} = R_{r-i+1} =$
  - $v_{i-1} = L_{r-i+1} = R_{r-i}$
  - подставим

$v_i = R_{i-i+1} \bigoplus f(R_{r-i}, k_{r+1-i})$

из $R_i = L_{i-1} \bigoplus f(R_{i-1}, k_i) \Rightarrow$

$L_{i-1} = R_i \bigoplus f(R_{i-1}, k_i) \Rightarrow$

По итогу получаем, что

$L_{r-i} = R_{r-i+1} + (R_{r-i}, k_{r-i+1})$

■

Конструкция расшифрования такая же как и шифрования, кроме порядка ключей

- **При шифровании ключи используются по возрастанию**
- **При расшифровании ключи используются по убыванию**

Нам не важно какую функцию f использовать, т.к не имеет значение её обратимость → **можем выбрать сколь угодно сложную функцию**

ГОСТ 28147-89

- Блок - 64 бит
- Ключ k - 256 бит

Построение раундовых ключей

1. Берётся ключ $k = k_1 k_2 \cdots k_8$ (разбили на 8 частей по 32 бита)
2. $k_1 k_2 \cdots k_{32} = k_1 k_2 \cdots k_8 || k_1 k_2 \cdots k_8 || k_1 k_2 \cdots k_8 || k_8 k_7 \cdots k_1$

Шифрование

1. Берётся открытый текст m. его разворачивают и затем делят на 2 одинаковых блока, т.е $L_0 R_0 = \overline{m}$
2. $\forall n \in \{1, \cdots 32\}$:
   - $L_n = R_{n-1}$
   - $R_n = L_{n-1} \bigoplus f(R_{n-1} +_{32} k_n)$
3. $c = \overleftarrow{R_{32} L_{32}}$

- Это опять конструкция фейстеля
- $+_{32}$ - это сложение по модулю 2^{32}. Сложение машинных слов

Опишем f

$f : \{0,1\}^{32} \to \{0,1\}^{32}$

f(x) = y

1. Берём x, разбиваем его на 8 кусочков по 4 бита, т.е
- $x = x_1 x_2 \cdots x_8$
2. $\forall i \in \{1, \cdots, 8\} : y_i = S_i(x_i)$
- $S_i : \{0,1\}^4 >\!\!\twoheadrightarrow \{0,1\}^4$
3. $y = \ll_{11} y_1 y_2 \cdots y_8$ (это ациклические сдвиги)

Достоинства

1. Конструкция Фейстеля
2. Нет битовых операций. Программное шифрование хорошо реализуется

3. Длинный 256 битный ключ

Недостатки

1. 32 раунда $\Rightarrow$ долго работает
2. S_i - это долговременные ключи. Т.е шифровальщик должен сам задать эти блоки через некоторые блоки. Существуют плохие блоки, которые ослабляют шифр.Можно взять строчки из DES.
3. 256 бит - это слишком длинный ключ