В госте 2 шифра:

1. Кузнечик
   - Блок - 128 бит
   - Ключ - 256 бит
2. Магма
   - Блок - 64 бит
   - Ключ - 256 бит

- Оба шифра имеют функциональное описание

Байт - триедин:

- это число от 0 до 255
- это цепочка битов $\{0,1\}^8$
- это элемент поля F = GF(256)

Кузнечик

Функции

главное поле $F = GF(256) = F[x]_{/p[x]\cdot f(x)}$

- $p(x) = x^8 + x^7 + x^6 + x + 1$
  - убедись, что p(x) не приводим над $\mathbb{Z}_2$ так же как и в AES

перестановка

- $\Pi : \{0,1\}^8 >\!\!\twoheadrightarrow \{0,1\}^8$
- перестановка задаётся с помощью численного представления

$S' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233,$
$119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101,$
$90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143,$
$160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42,$
$104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156,$
$183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178,$
$177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223,$
$245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236,$
$222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0,$
$98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163,$
$165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136,$
$217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133,$
$97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).$

Рис. 1: Перестановка П

-

Линейное преобразование

- $l : (\{0,1\}^8)^{16} \to \{0,1\}^8$
- ещё можно записать как
  - $l(F^{16}) \to F$
  - $l(\vec{x}) = (\vec{x}, \vec{a})$
    - это скалярное умножение на $\vec{a}$. Умножение проводится в поле F, сложение это XOR
    - $\vec{a}$ = см фото
    -

$X[k] : \{0,1\}^{128} >\!\!\twoheadrightarrow \{0,1\}^{128}$

- X[k](a)= a $\bigoplus$ k, где $k \in \{0,1\}^{128}$

$S : \{0,1\}^{128} >\!\!\twoheadrightarrow \{0,1\}^{128}$

- разделили a на 16 кусочков размером с байт
  - S(a) = $S(a_15||a_14||\cdots||a_0) = (\Pi(a_{15})||\Pi(a_{14})||\cdots||\Pi(a_0))$
- Можно изготовить обратную функцию
  - $S^{-1} = (\Pi^{-1}||\cdots||\Pi^{-1})$

$R : \{0,1\}^{128} >\!\!\twoheadrightarrow \{0,1\}^{128}$

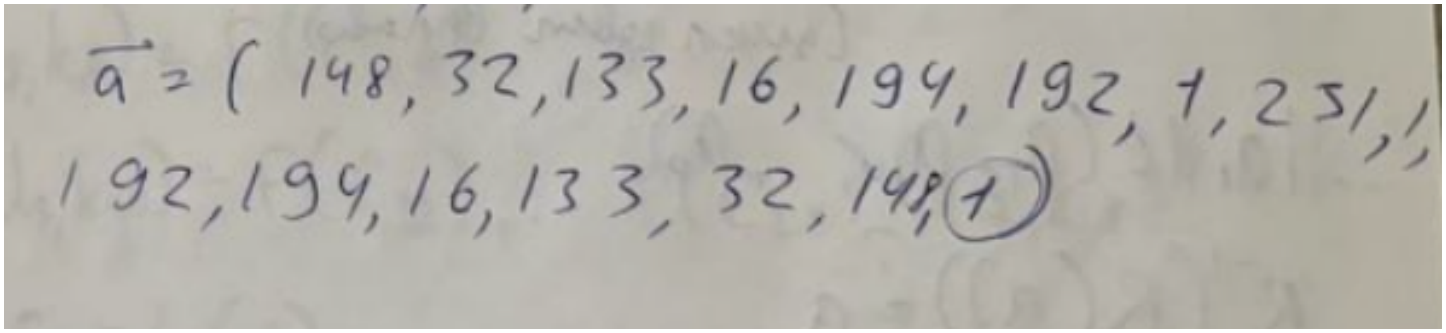

Рис. 2: это вектор $\vec{a}$

- каждый кусочек по байту
- $R(a) = R(a_{15}||\cdots||a_0) = l(a_{15},\cdots,a_0)||a_{15}||a_{14}||\cdots||a_1$
- $R^{-1}(a) = R^{-1}(a_{15}||\cdots||a_0) = a_{15}||a_{14}||\cdots||a_1||l(a_{15},\cdots,a_0)\$$
  - Чтобы доказать $R^{-1}(a)$ - это действительно обратный, то $\measuredangle(R^{-1}(R(a)))$.

$L = R^{16}$

- $L^{-1} = (R^{-1})^{16}$

Алгоритм построения ключа

Вход:

- $k \in \{0,1\}^{256}$

Выход

- $k_1,\cdots k_{10} \in \{0,1\}^{128}$

$k_1k_2 = k$

$(k_3,k_4) = F(C_8)(F(C_7)\cdots F(C_1)(k_1,k_2))$

$(k_5,k_6) = F(C_16)(F(C_15)\cdots F(C_9)(k_3,k_4))$

...

$(k_9,k_{10}) = F(C_{32})(F(C_{31})\cdots F(C_{25})(k_7,k_8))$

где

- $C_i = L(i)$
  - мы i представляем как цепочку из 128 бит и применяем к нему функцию L
- $F(C) : \{0,1\}^{128} \times \{0,1\}^{128} >\twoheadrightarrow \{0,1\}^{128} \times \{0,1\}^{128}$
  - $F(C)(a_1,a_0) = (L(S(X(C)(a_1)))XOR(a_0),a_1)$

Шифрование

$E_k(a) = X[k_{10}]LSX[k_9]\cdots L(S(X[k_1](a)))$

- Функции применяются справа налево
- По существу - 9 раундов
- по суть $X[k_i]$ - прибавление k_i ключа
- S - сильно нелинейное локальное преобразование
- L - линейное локальное преобразование

Расшифрование

$D_k(a) = X[k_1]S^{-1}L^{-1}X[k_2]\cdots S^{-1}L^{-1}X[k_{10}](a)$

Достоинства

- раундов меньше
- быстрее ГОСТа, DES
- описание проще чем у AES # Недостатки
- есть функция L - которая долго считается

Магма

Фиксированные перестановки $\Pi_i : \{0,1\}^4 >\twoheadrightarrow \{0,1\}^4$

π_0' = (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1);
π_1' = (6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15);
π_2' = (11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0);
π_3' = (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11);
π_4' = (7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12);
π_5' = (5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0);
π_6' = (8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7);
π_7' = (1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2).

Рис. 3: alt text

Функции

$t : \{0,1\}^{32} \to \{0,1\}^{32}$ * $t(a) = t(a_7||a_6||\cdots||a_0) = \Pi_7(a_7)||\cdots||\Pi_0(a_0)$

$g[k] : \{0,1\}^{32} \to \{0,1\}^{32}$

- $g[k](a) = (t(a \boxplus k)) \ll 11$
- $\boxplus$ - это сложение по модулю 32

$G[k] : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32} \times \{0,1\}^{32}$

- $G[k](a_1, a_0) = (a_0, g[k](a_0) \bigoplus a_1)$

$G^*[k] : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{64}$

- $G^*[k](a_1, a_0) = (g[k](a_0) \bigoplus a_1)||a_0$

Алгоритм построения раундовых ключей ключей

Берём k и бьем его на 8 частей

$k = k_1||k_2||\cdots||k_8$

Берём k и бьем его на 8 частей, но нумеровать начинаем с 9

$k = k_9||k_{10}||\cdots||k_{16}$

и тд кроме последнего последний $k = k_{32}||k_{31}||\cdots||k_{25}$

Шифрование

$E_k(a) = E_k(a_1||a_0) = G^*[k_{32}](G[k_{31}](\cdots(G[k_1](a_1, a_0))))$

- 32 раунда конструкции Фейстеля

Расшифрование

$D_k(a) = D_k(a_1||a_0)G^*[k_1](G[k_2](\cdots(G[k_1](a_1, a_0))))$

Достоинства

- ликвидированы долговременные ключи. Поставлены фиксированные перестановки у ГОСТА 89 года
- самый древний действующий стандарт

Недостатки

- медленный шифр за счёт малого блока и 32 раундов

Итерационные ключи $K_i \in V_{32}$, $i = 1, 2, \ldots, 32$, вырабатываются на основе ключа $K = k_{255}||\ldots||k_0 \in V_{256}$, $k_i \in V_1$, $i = 0, 1, \ldots, 255$, и определяются равенствами:

$$K_1 = k_{255}||\ldots||k_{224};$$
$$K_2 = k_{223}||\ldots||k_{192};$$
$$K_3 = k_{191}||\ldots||k_{160};$$
$$K_4 = k_{159}||\ldots||k_{128};$$

$$K_5 = k_{127}||\ldots||k_{96};$$
$$K_6 = k_{95}||\ldots||k_{64}; \quad (18)$$
$$K_7 = k_{63}||\ldots||k_{32};$$
$$K_8 = k_{31}||\ldots||k_0;$$
$$K_{i+8} = K_i,\ i = 1, 2, \ldots, 8;$$
$$K_{i+16} = K_i,\ i = 1, 2, \ldots, 8;$$
$$K_{i+24} = K_{9-i},\ i = 1, 2, \ldots, 8.$$

Рис. 4: alt text