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

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

ГОСТ Р 34.12-2015

Общее описание

ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

- Шифр «**Магма**»:
  - соответствует ГОСТ 28147-89;
  - использует фиксированный блок замен;
- Шифр «**Кузнечик**»:
  - длина блока: 128 бит;
  - длина ключа: 256 бит;
  - число раундов: 10;
  - основа: SP-сеть.

Основные обозначения

V^*	множество всех двоичных строк конечной длины, включая пустую строку;
V_s	множество всех двоичных строк длины s;
$\|A\|$	длина строки $A \in V^*$;
$A \parallel B$	конкатенация строк $A, B \in V^*$;
$\mathbb{F}$	поле Галуа F_{2^8}, построенное с использованием многочлена $p(x) = x^8 + x^7 + x^6 + x + 1$;
$Vec_s: \mathbb{Z}_{2^s} \to V_s$	преобразование элемента кольца $\mathbb{Z}_{2^s}$ в двоичную строку из V_s;
$Int_s: V_s \to \mathbb{Z}_{2^s}$	преобразование s-разрядной строки в элемент кольца $\mathbb{Z}_{2^s}$;
$\Delta: V_8 \to \mathbb{F}$	преобразование 8-разрядной строки в элемент поля Галуа;
$\nabla: \mathbb{F} \to V_8$	преобразование элемента поля Галуа в двоичную строку из V_8;
$\Phi\Psi$	композиция отображений Φ и Ψ;
Φ^s	композиция отображений вида $\underbrace{\Phi\Phi \cdots \Phi}_{s}$.

Элементарные преобразования

- Нелинейное биективное преобразование $\pi = Vec_8\,\pi'\,Int_8 : V_8 \to V_8$:
  - замена байт;
  - $\pi' = \begin{pmatrix} 0 & 1 & \dots & 254 & 255 \\ 252 & 238 & \dots & 99 & 182 \end{pmatrix}$.
- Линейное преобразование $l : V_8^{16} \to V_8$:
  - свертка 16-байтового слова в один байт посредством линейного преобразования в поле Галуа;
  - $l(a_{15}, a_{14}, \dots, a_0) = \nabla\left(\sum_{i=0}^{15} \alpha_i \Delta(a_i)\right) = \nabla\big(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta(a_0)\big)$.

Этапы раунда зашифрования

- Состояние блока данных:
  - $a \in V_{128}$.
- Наложение раундового ключа $k \in V_{128}$ на блок данных:
  - $X[k](a) = k \oplus a$.
- Замена байтов в блоке данных:
  - $S(a) = S(a_{15} \| \cdots \| a_0) = \pi(a_{15}) \| \cdots \| \pi(a_0)$.
- Перемешивание блока данных:
  - $L(a) = R^{16}(a)$;
  - $R(a) = R(a_{15} \| \cdots \| a_0) = l(a_{15}, a_{14}, \ldots, a_0) \| a_{15} \| \cdots \| a_1$.

Этапы раунда расшифрования

- Обратное наложение раундового ключа $k \in V_{128}$ на блок данных:
  - $X^{-1}[k](a) = X[k](a) = k \oplus a$;
- Обратная замена байтов в блоке данных:
  - $S^{-1}(a) = S^{-1}(a_{15} \| \cdots \| a_0) = \pi^{-1}(a_{15}) \| \cdots \| \pi^{-1}(a_0)$;
- Обратное перемешивание блока данных:
  - $L^{-1}(a) = \left(R^{-1}\right)^{16}(a)$;
  - $R^{-1}(a) = R^{-1}(a_{15} \| \cdots \| a_0) = a_{14} \| \cdots \| a_0 \| l(a_{14}, a_{13}, \ldots, a_0, a_{15})$.

Обратимость преобразования R

- $R(a) = R(a_{15} \| a_{14} \| \cdots \| a_0) = l(a_{15}, a_{14}, \dots, a_0) \| a_{15} \| \cdots \| a_1 = \acute{a}_{15} \| \acute{a}_{14} \| \cdots \| \acute{a}_0 = \acute{a}.$
- $R^{-1}(\acute{a}) = R^{-1}(\acute{a}_{15} \| \acute{a}_{14} \| \acute{a}_{13} \| \cdots \| \acute{a}_0) = \acute{a}_{14} \| \acute{a}_{13} \| \cdots \| \acute{a}_0 \| l(\acute{a}_{14}, \acute{a}_{13}, \dots, \acute{a}_0, \acute{a}_{15}) =$
$= a_{15} \| a_{14} \| \cdots \| a_1 \| l\big(a_{15}, a_{14}, \dots, a_1, l(a_{15}, a_{14}, \dots, a_0)\big).$

- $l\big(a_{15}, a_{14}, \dots, a_1, l(a_{15}, a_{14}, \dots, a_0)\big) = \nabla\Big(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta\big(l(a_{15}, a_{14}, \dots, a_0)\big)\Big).$

- $l\big(a_{15}, a_{14}, \dots, a_1, l(a_{15}, a_{14}, \dots, a_0)\big) = \nabla\Big(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta\Big(\nabla\big(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + \mathbf{1} \cdot \boldsymbol{\Delta(a_0)}\big)\Big)\Big).$

Обратимость преобразования R

- $l(a_{15}, a_{14}, \dots, a_1, l(a_{15}, a_{14}, \dots, a_0)) = \nabla(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + \mathbf{1} \cdot \boldsymbol{\Delta(a_0)})$.

- $l(a_{15}, a_{14}, \dots, a_1, l(a_{15}, a_{14}, \dots, a_0)) = \nabla(1 \cdot \Delta(a_0)) = \nabla(\Delta(a_0)) = a_0$, так как $\forall \alpha \in F_{2^n}$ верно $\alpha + \alpha = 0$.

- $R^{-1}(\acute{a}) = a_{15} \parallel a_{14} \parallel \cdots \parallel a_1 \parallel a_0 = a$.

Развертывание раундовых ключей

- Вычисление раундовых констант:
  - $C_i = L(Vec_{128}(i)), i = \overline{1,32}.$
- Вычисление первых двух раундовых ключей как двух частей ключа шифрования:
  - $K = k_{255} \| k_{254} \| \cdots \| k_0,$
  - $K_1 = k_{255} \| k_{254} \| \cdots \| k_{128}, K_2 = k_{127} \| k_{126} \| \cdots \| k_0,$
- Вычисление 8 раундовых ключей на основе первых двух:
  - $(K_{2i+1},\ K_{2i+2}) = F\left[C_{8(i-1)+8}\right] \ldots F\left[C_{8(i-1)+1}\right](K_{2i-1},\ K_{2i}), i = \overline{1,4};$
  - $F[k](a_1,\ a_0) = (LSX[k](a_1) \oplus a_0,\ a_1).$

Зашифрование

- Полный раунд зашифрования:
  - наложение раундового ключа $X[K_i]$, $i = \overline{1,9}$;
  - замена байтов S;
  - перемешивающее преобразование L.
- Неполный раунд зашифрования:
  - наложение раундового ключа $X[K_{10}]$.

- Зашифрование блока данных $a \in V_{128}$:
  - $E_{K_1,K_2,\dots,K_{10}}(a) = X[K_{10}]LSX[K_9] \dots LSX[K_3]LSX[K_2]LSX[K_1](a)$

Расшифрование

- Полный раунд расшифрования:
  - обратное перемешивающее преобразование L^{-1};
  - обратная замена байтов S^{-1};
  - обратное наложение раундового ключа $X[K_i]$, $i = \overline{1,9}$;
- Неполный раунд расшифрования:
  - обратное наложение раундового ключа $X[K_{10}]$.

- Расшифрование блока данных $a \in V_{128}$:
  - $D_{K_1,K_2,\dots,K_{10}}(a) = X[K_1]S^{-1}L^{-1}X[K_2]S^{-1}L^{-1}X[K_3]S^{-1}L^{-1} \dots X[K_9]S^{-1}L^{-1}X[K_{10}](a).$

Спасибо за внимание!

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

+7 923 403 09 21
oevsyutin@hse.ru