ГОСТ Р $34.12-2015$ (Кузнечик и Магма)

Стандарт криптографической защиты данных ГОСТ Р 34.12-2015 [1], введенный в действие с 1 января 2016 г., даёт описание двух базовых блочных шифров с длинами блоков $n = 128$ бит и $n = 64$ бит и длиной ключа $k = 256$ бит. (На описанный в стандарте 128-битовый шифр можно ссылаться как на блочный шифр Кузнечик (Kuznyechik), а на 64-битовый шифр — как на блочный шифр Магма (Magma).

Алгоритм Магма полностью совпадает с алгоритмом ГОСТ 28147-89 с той лишь разницей, что теперь в нём зафиксированы S-блоки, а именно:

$$S - \text{блоки ГОСТ Р } 34.12 - 2015$$

$$\begin{aligned}
S_0 &= (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1);\\
S_1 &= (6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15);\\
S_2 &= (11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0);\\
S_3 &= (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11);\\
S_4 &= (7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12);\\
S_5 &= (5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0);\\
S_6 &= (8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7);\\
S_7 &= (1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2).
\end{aligned}$$

Далее рассматривается шифр ***Кузнечик***.

Обозначения

V^*	— множество всех двоичных строк конечной длины, включая пустую строку;
V_s	— множество всех двоичных строк длины s, где s – целое неотрицательное число; ***нумерация подстрок и компонент строки осуществляется справа налево, начиная с нуля***;
$U \times W$	— декартово произведение множества U и W;
$\|A\|$	длина строки $A \in V_s$ (если A – пустая строка, то $\|A\| = 0$);
$A\|\|B$	— конкатенация строк $A, B \in V^*$, т.е. строка из $V_{\|A\|+\|B\|}$, в которой подстрока с большими номерами компонент из $V_{\|A\|}$ совпадает со строкой A, а подстрока с меньшими номерами компонент из $V_{\|B\|}$ совпадает со строкой B;
$A \lll 11$	— циклический сдвиг строки $A \in V_{32}$ на 11 компонент в сторону компонент, имеющих большие номера;
$\oplus$	— операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;
$\mathbb{Z}_{2^s}$	— кольцо вычетов с операциями сложения и умножения по модулю 2^s;
$\mathbb{F}$	— конечное поле $\mathbb{F}_{2^8} = GF(2)[x]\,/\,p(x)$, где $p(x) = x^8 + x^7 + x^6 + x + 1 \in GF(2)[x]$; элементы поля $\mathbb{F}$ представляются целыми числами, причем элементу $z_0 + z_1 \cdot \theta\ + \cdots + z_7 \cdot \theta^7 \in \mathbb{F}$

[1] Шифр разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО «Информационные технологии и коммуникационные системы» («ИнфоТеКС»).

соответствует число $z_0 + 2z_1 + \dots + 2^7 z_7$, где $z_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$, и θ обозначает класс вычетов по модулю $p(x)$, содержащий x;

$Vec_s: \mathbb{Z}_{2^s} \to V_s$ — биективное отображение, сопоставляющее элементу кольца $\mathbb{Z}_{2^s}$ его двоичное представление, т.е. для любого элемента $z \in \mathbb{Z}_{2^s}$, представленного в виде $z_0 + 2z_1 + \dots + 2^{s-1} z_{s-1}$, *где* $z_i \in \{0, 1\}$, $i = 0, 1, \dots, s-1$, выполнено равенство $Vec_s(z) = z_{s-1} || \dots || z_1 || z_0$;

$Int_s: V_s \to \mathbb{Z}_{2^s}$ — отображение Vec_s^{-1}, обратное к отображению Vec_s;

$\Delta: V_8 \to \mathbb{F}$ — биективное отображение, сопоставляющее двоичной строке из V_8 элемент поля $\mathbb{F}$ следующим образом: строке $z_7 || \dots || z_1 || z_0$, $z_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$, соответствует элемент $z_0 + z_1 \cdot \theta + \dots + z_7 \cdot \theta^7 \in \mathbb{F}$;

$\nabla: \mathbb{F} \to V_8$ — отображение Δ^{-1}, обратное к отображению Δ.

$\Phi \circ \Psi$ — композиция отображений, при которой отображение □ действует первым, т.е. $\Phi \circ \Psi(X) = \Phi \circ (\Psi(X))$;

Φ^s — композиция отображений Φ^{s-1} и Φ, причем $\Phi^1 = \Phi$.

Используемые преобразования

При реализации алгоритмов зашифрования и расшифрования используются следующие преобразования:

Нелинейное биективное преобразование множества двоичных векторов

Нелинейное биективное преобразование множества двоичных векторов V_8 задается подстановкой $\pi: \mathbb{Z}_{2^8} \to \mathbb{Z}_{2^8}$. Данная подстановка задана массивом $\pi = \big(\pi(0), \pi(1), \dots, \pi(255)\big) =$
(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).

Линейное преобразование

Линейное преобразование задается отображением $\ell: V_8 \to V_8$, которое определяется следующим образом:

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

для любых $a_i \in V_8$, $i = 0, 1, \ldots, 15$, где операции сложения и умножения осуществляются в поле $\mathbb{F}$, а константы являются элементами поля в указанном ранее смысле.

$X[k]: V_{128} \to V_{128}$ — $X[k](a) = k \oplus a$, где $k, a \in V_{128}$;

$S: V_{128} \to V_{128}$ — $S(a) = S(a_{15}|| \ldots ||a_0) = \pi(a_{15})|| \ldots ||\pi(a_0)$, где $a = a_{15}|| \ldots ||a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \ldots, 15$;

$S^{-1}: V_{128} \to V_{128}$ — преобразование S^{-1}, обратное к преобразованию S: $S^{-1}(a) = S^{-1}(a_{15}|| \ldots ||a_0) = \pi^{-1}(a_{15})|| \ldots ||\pi^{-1}(a_0)$, где $a = a_{15}|| \ldots ||a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \ldots, 15$, π^{-1} – подстановка, обратная к подстановке π;

$R: V_{128} \to V_{128}$ — $R(a) = R(a_{15}|| \ldots ||a_0) = \ell(a_{15}, \ldots, a_0)||a_{15}|| \ldots ||a_1$, где $a = a_{15}|| \ldots ||a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \ldots, 15$;

$L: V_{128} \to V_{128}$ $L(a) = R^{16}(a)$, где $a \in V_{128}$;

$R^{-1}: V_{128} \to V_{128}$ — преобразование R^{-1}, обратное к преобразованию R:

$$R^{-1}(a) = R^{-1}(a_{15}|| \ldots ||a_0) = a_{14}||a_{13}|| \ldots ||a_0||\ell(a_{14}, a_{13}, \ldots, a_0, a_{15}),$$

где $a = a_{15}|| \ldots ||a_0 \in V_{128}$, $a_i \in V_8$, $i = 0,1,\ldots,15$;

$L^{-1}: V_{128} \to V_{128}$ — $L^{-1}(a) = (R^{-1})^{16}(a)$, где $a \in V_{128}$;

$F\,[k]: V_{128} \times V_{128} \to V_{128} \times V_{128}$ $F\,[k](a_1, a_0) = (L \circ S \circ X[k](a_1) \oplus a_0, a_1)$, где $k, a_0, a_1 \in V_{128}$.

Этап предвычислений:
Алгоритм вычисления итерационных (раундовых) ключей

Алгоритм вычисления итерационных (раундовых) ключей использует итерационные константы $C_i \in V_{128}$, $i = 1, 2, \ldots, 32$, которые определены следующим образом:

$$C_i = L(Vec_{128}(i)), i = 1, 2, \ldots, 32.$$

Итерационные ключи $K_i \in V_{128}$, $i = 1, 2, \ldots, 10$, вырабатываются на основе секретного ключа $K = k_{255}|| \ldots ||k_0 \in V_{256}, k_i \in V_1$, $i = 0, 1, \ldots, 255$, и определяются равенствами:

$$K_1 = k_{255}|| \ldots ||k_{128};$$
$$K_2 = k_{127}|| \ldots ||k_0;$$
$$(K_{2i+1}, K_{2i+2}) = F\,[C_{8(i-1)+8}] \ldots F\,[C_{8(i-1)+1}](K_{2i-1}, K_{2i}), i = 1, 2, 3, 4.$$

Алгоритм зашифрования

Алгоритм зашифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \ldots, 10$, реализует подстановку $\mathcal{E}_{K_1,\ldots,K_{10}}$, заданную на множестве V_{128} в соответствии с равенством

$$\mathcal{E}_{K_1,\ldots,K_{10}}(a) =$$

$$X[K_{10}] \circ L \circ S \circ X[K_9] \circ \ldots \circ L \circ S \circ X[K_2] \circ L \circ S \circ X \circ L \circ S \circ X[K_1](a),$$

где $a \in V_{128}$.

Алгоритм расшифрования

Алгоритм расшифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \ldots, 10$, реализует подстановку $\mathcal{D}_{K_1,\ldots,K_{10}}$, заданную на множестве V_{128} в соответствии с равенством

$$\mathcal{D}_{K_1,\ldots,K_{10}}(a) = X[K_1] \circ S^{-1} \circ L^{-1} \circ X[K_2] \circ \ldots \circ S^{-1} \circ L^{-1} \circ X[K_9] \circ S^{-1} \circ L^{-1} \circ X[K_{10}](a),$$

где $a \in V_{128}$.

Контрольные примеры

См. Приложение А в официальном документе о ГОСТ Р 34.12-2015 [ ]