MAGENTA

Криптоалгоритм $Magenta$[1] шифрует 128-битовые (16-байтовые) блоки открытых данных под управлением секретного ключа, длина которого может составлять 128, 192 или 256 битов.

Обозначим через B множество байтов (т.е. $B = \{0,1,\dots,255\}$, если отождествить 8-битовый байт $(x_7, x_6, \dots, x_0)$ с числом $x_7 2^7 + x_6 2^6 + \cdots + x_0$, а через B^n – множество n-байтовых векторов $(b_0, b_1, \dots, b_{n-1})$, $b_i \in B$.

В алгоритме используются следующие функции:

Функция $f\colon B \longrightarrow B$ определяется как

$$f(x) = \begin{cases} \alpha^x, \text{если } x \neq 255, \\ 0, \ \ \text{если } x = 255. \end{cases}$$

Здесь α и α^x – байты, интерпретируемые как элементы конечного поля $\mathbb{F}_{256} \cong \mathbb{F}_2[x]/p(x)$, где $p(x) = x^8 + x^6 + x^5 + x^2 + 1$ ($p(x)$ – примитивный многочлен, поэтому в качестве α можно взять байт $0x02$).

Функция $A\colon B^2 \longrightarrow B$ определяется как

$$A(x,y) = f(x \oplus f(y)),$$

где символ ⊕ обозначает побитовое сложение байтов (xor) по модулю 2.

Функция $PE\colon B^2 \longrightarrow B^2$ определяется как

$$PE(x,y) = (A(x,y), A(y,x)).$$

Функции П и Т: $B^{16} \longrightarrow B^{16}$ определяются как

$$\Pi(x_0, \dots, x_{15}) = (PE(x_{15}, x_8), PE(x_1, x_9), \dots, PE(x_7, x_{15})),$$
$$\mathrm{T}(x_0, \dots, x_{15}) = \Pi(\Pi(\Pi(\Pi(x_0, \dots, x_{15})))).$$

Функции ХЕ и ХО: $B^{16} \longrightarrow B^8$ определяются как

$$\mathrm{XE}(x_0, \dots, x_{15}) = (x_0, x_2, x_4, x_6, x_8, x_{10}, x_{12}, x_{14}),$$
$$\mathrm{XO}(x_0, \dots, x_{15}) = (x_1, x_3, x_5, x_7, x_9, x_{11}, x_{13}, x_{15}).$$

Функция Е: $B^{16} \longrightarrow B^8$ определяется как

$$\mathrm{E}(x_0, \dots, x_{15}) = \mathrm{XE}(\mathrm{C}^{(3)}(x_0, \dots, x_{15})).$$

Функция $\mathrm{C}^{(3)}\colon B^{16} \longrightarrow B^{16}$ определяется рекурсивно:

$$\mathrm{C}^{(1)}(x_0, \dots, x_{15}) = \mathrm{T}(x_0, \dots, x_{15}),$$
$$\mathrm{C}^{(j+1)}(x_0, \dots, x_{15}) = \mathrm{T}(y_0, \dots, y_{15}),\ j = 1, 2,$$

где

$$(y_0, \dots, y_7) = (x_0, \dots, x_7) \oplus \mathrm{XE}\,(\mathrm{C}^{(j)}(x_0, \dots, x_{15})),$$
$$(y_8, \dots, y_{15}) = (x_8, \dots, x_{15}) \oplus \mathrm{XO}(\mathrm{C}^{(j)}(x_0, \dots, x_{15})).$$

Алгоритм шифрования $Magenta$ построен в соответствии со схемой Фейстеля (см. рис. 1). Для блока данных $X = (x_0, \dots, x_{15}) \in B^{16}$ и раундового подключа $Y = (y_0, \dots, y_7) \in B^8$ результат одного “раунда Фейстеля” определен как

$$F_y(X) = (z_0, \dots, z_{15}),$$

где

$$(z_0, \dots, z_7) = (x_8, \dots, x_{15}),$$
$$(z_8, \dots, z_{15}) = (x_0, \dots, x_7) \oplus E(x_8, \dots, x_{15}, y_0, \dots, y_7).$$

$Magenta$ предусматривает использование -байтовых секретных ключей $K = (k_0, \dots, k_{m-1})$ с $m = 16$, 24 или 32. Раундовые подключи $\mathrm{K_i}$ определяются как

$$K = (K_1, K_2) \qquad \text{для } m = 16,$$
$$K = (K_1, K_2, K_3) \qquad \text{для } m = 24,$$
$$K = (K_1, K_2, K_3, K_4) \ \text{для } m = 32,$$

где $K_1 = (k_0, \dots, k_7)$, $K_2 = (k_8, \dots, k_{15})$, $K_3 = (k_{16}, \dots, k_{23})$, $K_4 = (k_{24}, \dots, k_{31})$.

Алгоритм состоит из 6 или 8 раундов в зависимости от длины ключа K. Результат зашифрования блока открытых данных $X \in B^{16}$ определяется как

---

[1] Авторы шифра: $M.J.Jacobson$ и $K.Huber$ (специалисты Deutsche Telecom, Германия, 1998)

$$Magenta[](X) = \begin{cases} F_{k_1} \circ F_{k_1} \circ F_{k_2} \circ F_{k_2} \circ F_{k_1} \circ F_{k_1} \circ V(P), & \text{если } K \in B^{16}, \\ F_{k_1} \circ F_{k_2} \circ F_{k_3} \circ F_{k_3} \circ F_{k_2} \circ F_{k_1} \circ V(P), & \text{если } K \in B^{24}, \\ F_{k_1} \circ F_{k_2} \circ F_{k_3} \circ F_{k_4} \circ F_{k_4} \circ F_{k_3} \circ F_{k_2} \circ F_{k_1} \circ V(P), & \text{если } K \in B^{32}. \end{cases}$$

где $F \circ G(x) = F(G(x))$, а функция V определяется как

$$V(x_0, \dots, x_{15}) = (x_8, x_9, \dots, x_{15}, x_0, x_1, \dots, x_7).$$

Преобразование $Magenta[K]$ инволютивно:

$$Magenta^{-1}[K] \circ Magenta[K](X) \equiv X.$$

Другими словами,

$$Y = Magenta[K](X) \Longrightarrow X = Magenta[K](Y).$$

Замечание. Авторы определяют преобразование зашифрования как

$$Enc[K] = Magenta[K] \circ V;$$

в этом случае обратное преобразование имеет вид: $K = (k_0k_1k_2k_3k_4k_5k_6k_7)$

$$Dec[K](C) = V \circ Enc[K] \circ V(C).$$

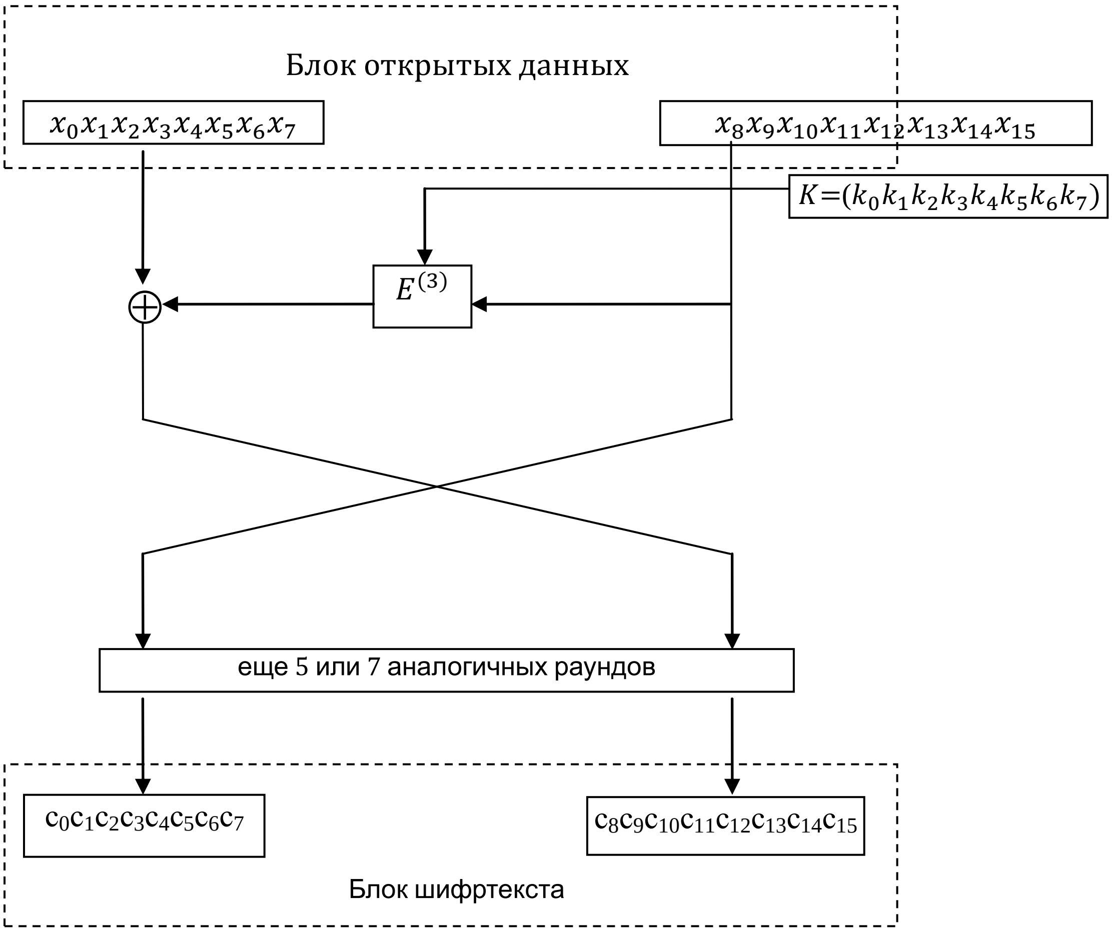

Рис. 1. Алгоритм $Magenta$