Rainbow

Криптоалгоритм $Rainbow$ [1] шифрует 128-битовые блоки открытых данных под управлением секретного ключа такого же размера.

Пусть $X = [X_3, X_2, X_1, X_0] - 128$-битовый блок данных с 32-битовыми подблоками X_3, X_2, X_1, X_0 а $K = [K_3, K_2, K_1, K_0] - 128$-байтовый раундовый ключ такой же структуры.

Преобразования $\mathrm{G_K}$ и $\mathrm{B_K}$ определяются как

$G_K(\mathrm{X}) \equiv \{X := X \oplus K\};$
$B_K(X) \equiv \{$
$\boldsymbol{for}\ i := 0,1,2,3\ \boldsymbol{do}$
$Y_i := (X_0 \& K_i) \oplus (X_1 \& K_{i+1}) \oplus (X_2 \& K_{i+2}) \oplus (X_3 \& K_{i+3});$

Индексы приводятся по модулю 4, т.е. $K_4 \equiv K_0$, $K_5 \equiv K_1$, $K_6 \equiv K_2$, $K_7 \equiv K_3$.

$X := [Y_3, Y_2, Y_1, Y_0];$
$return(X)$
$\}.$

Пусть $Z = (z_3, z_2, z_1, z_0) - 32$-битовый блок, причем его 8-битовые подблоки (байты) z_i интерпретируются как элементы поля $\mathbb{F}_{256} \cong \mathbb{F}_2[x] \,/\, (x^8 + x^7 + x^5 + x^3 + 1)$.
Функции P_1, P_2 и P_3 определяются как

$P_1(Z) = (\pi[z_2], \tau[z_3], \pi[z_0], \tau[z_1]),$
$P_2(Z) = (\pi[z_1], \pi[z_0], \tau[z_3], \tau[z_2]),$
$P_3(Z) = (\pi[z_0], \pi[z_1], \tau[z_2], \tau[z_3]),$

где $\pi[z] = z^{37}$ и $\tau[z] = z^{193}$ – взаимно обратные подстановки на $\mathbb{F}_{256}$, т.е. $\tau = \pi^{-1}$.

Преобразование R определяется как

$R(X) \equiv \{$
$X := [P_2(X_3), P_3(X_2), P_2(X_1), P_1(X_0)];$
$return(X)$
$\}.$

Замечание. Далее будем отождествлять каждое из преобразований G_K, B_K и R с соответствующими им функциями: полагаем, например, $B_K(a) = b$, если в результате преобразования $B_K(X)$ переменная X изменяет свое значение с a на b.

Отметим, что преобразования G_K и R инволютивны, т.е.

$$G_K \circ G_K(X) = X, \;\; R \circ R(X) = X,$$

и, следовательно, совпадают с обратными к ним; преобразование B_K инволютивно, если

$$K_0 = not(K_1 \oplus K_2 \oplus K_3). \qquad (1)$$

Отметим также, что

$$G_S \circ B_K = B_K \circ G_{S'}, \qquad (2)$$

где $S' = B_K(S)$, а K удовлетворяет (1).

В N-раундовом алгоритме зашифрования (стандартное число раундов $N = 7$) используются 128-битовые раундовые подключи

$$Ke[i] = [ke_{i3}, ke_{i2}, ke_{i1}, ke_{i0}],\ i = 0, 1, \ldots, 2N + 1,$$

генерируемые на основе секретного ключа

$$SK = [SK_3, SK_2, SK_1, SK_0]$$

следующим образом:

$Ke[0] \coloneqq SK;$
$(a, b, c, d) := (3,5,7,11);$
$\boldsymbol{for}\ i := 1\ \boldsymbol{to}\ 2N + 1\ \boldsymbol{do}\ \{$
$Ke[i] := Ke[i - 1];$
$\boldsymbol{for}\ j := 0,1,2,3\ \boldsymbol{do}\ \{$

[1] Авторы шифра: *Chang-Hyi Lee* и *Jeong-Soo Kim* (Южная Корея)

$ke_{ij} := shr_a(ke_{i0}) \oplus shr_b(ke_{i1}) \oplus shr_c(ke_{i2}) \oplus shr_d(ke_{i3}) \oplus 0xb7e15163;$
$(a, b, c, d) := (b, c, d, a)$
}
};
$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ N\ \boldsymbol{do}$ {
$j := 2i + 1;$
$ke_{j0} := \boldsymbol{not}(ke_{j1} \oplus ke_{j2} \oplus ke_{j3})$
}.

Алгоритм зашифрования *Rainbow*

Вход: X – 128-битовый блок открытых данных.
$C := X;$
$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ N - 1\ \boldsymbol{do}$ {
$G_{Ke[2i]}(C);$
$B_{Ke[2i+1]}(C);$
$R(C)$
};
$G_{Ke[2N]}(C);$
$B_{Ke[2N+1]}(C)$.
Выход: C – 128-битовый блок шифртекста.

Этот же алгоритм можно использовать и для расшифрования, если раундовые подключи $Ke[i]$ заменить на подключи $Kd[i]$:

$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ N\ \boldsymbol{do}$ {
$K := Ke[2N - 2i];$
$Kd[2i] := B_{Ke[2N+1-2i]}(K);$
$Kd[2i + 1] := Ke[2N + 1 - 2i]$
}.

Этот факт вытекает из свойств (1) и (2).