## $\boldsymbol{Three\ Way}$ $(\boldsymbol{3-Way})$ и $\boldsymbol{Base\ King}$

Криптоалгоритмы 3-$Way$ и $Base\ King$ [1] имеют одинаковую идеологию. Алгоритмы шифруют $n$-битовые блоки открытых данных под управлением секретного ключа такого же размера. Для 3-$Way$ значение $n = 96$, а для $Base\ King$ – вдвое больше, т.е. 192.

***Общая схема.*** В качестве базовых преобразований при конструировании указанных шифров используются биективные (т.е. взаимно однозначные) преобразования пространства $n$-битовых блоков $\mathbb{F}_2^n$:

$\gamma -$ *нелинейное* преобразование,

$\theta -$ линейное преобразование (для *диффузии*),

$\sigma[k] -$ аффинное преобразование (побитовое сложение по модулю 2 шифруемого блока с *раундовым подключом*, т.е. $\sigma[k](X) \equiv \{X := X \oplus k\}$),

$\pi_i$ – перестановки битов (для *конфузии*, или *битовой дисперсии*).

Базовые преобразования подбираются так, чтобы выполнялись следующие соотношения (их смысл состоит в том, что бы сконструировать симметричный алгоритм, который можно использовать как для зашифрования, так и для расшифрования):

$$\theta^{-1} = \mu \circ \theta \circ \mu, \qquad \gamma^{-1} = \mu \circ \gamma \circ \mu, \tag{1}$$

$$\pi_2^{-1} = \mu \circ \pi_1^{-1} \circ \mu, \qquad \pi_1^{-1} = \mu \circ \pi_2^{-1} \circ \mu, \tag{2}$$

где $\mu -$ некоторая инволютивная перестановка битов в -битовом блоке, т.е. $\gamma^{-1} = \mu$.

Конструируемые шифры являются итеративными (но не сетями Фейстеля) и состоят из $m$ итераций раундового преобразования $\rho$, выполняемого над блоком данных $X$ под управлением раундовых подключей $k_0, k_1, \ldots, k_{m-1}$, и входного преобразования $\mu \circ \omega$ под управлением раундового подключа $k_m$:

$\rho[k_j](X) \equiv \pi_2 \circ \gamma \circ \pi_1 \circ \theta \circ \sigma[k](X)$,

$\omega[k_m](X) \equiv \theta \circ \sigma[k_m]$.

Таким образом, $m$-раундовое шифрующее преобразование определяется как

$B_m[k_0, k_1, \ldots, k_m] \equiv \mu \circ \omega[k_m] \circ \rho[k_{m-1}] \circ \ldots \circ \rho[k_1] \circ \rho[k_0]$.

Обратное преобразование имеет вид:

$B_m^{-1}[k_0, k_1, \ldots, k_m]^{-1} = \rho^{-1}[k_0] \circ \rho^{-1}[k_1] \circ \ldots \circ \rho^{-1}[k_{m-1}] \circ \omega^{-1}[k_m] \circ \mu^{-1}$.

Используя соотношения (1), (2) и вытекающие из них соотношения:

$\sigma[k] \circ \mu = \sigma[\mu(k)]$,

$\sigma[k] \circ \theta^{-1} = \theta^{-1} \circ \sigma[\theta(k)]$,

$\sigma[k] \circ \theta^{-1} \circ \mu = \mu \circ \theta \circ \sigma[\mu(\theta(k))]$,

$\rho^{-1}[k] = \sigma[k] \circ \theta^{-1} \circ \pi_1^{-1} \circ \gamma^{-1} \circ \pi_2^{-1} = \mu \circ \theta \circ \sigma[\gamma(\theta(k))] \circ \pi_2 \circ \gamma \circ \pi_1 \circ \mu$,

можно показать, что преобразование $B_m^{-1}$ приводится к виду:

$$B_m^{-1}[ke_0, ke_1, \ldots, ke_m] = B_m[kd_0, kd_1, \ldots, kd_m],$$

где

$$kd_i = ke_{m-i},\ i = 0, 1, \ldots, m.$$

Другими словами, для зашифрования и расшифрования может быть использован только один и тот же алгоритм:

### Алгоритм зашифрования/расшифрования

*Вход*: $X - n$-битовый блок открытых данных/шифртекста.

*Примечание*. При зашифровании используются раундовые подключи $k_i = ke_0, ke_1, \ldots, ke_m$, а при расшифровании подключи $k_i = kd_0, kd_1, \ldots, kd_m$.

$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ m-1\ \boldsymbol{do}\ \{\sigma[k_i](X);\ \theta(X);\ \pi_1(X);\ \gamma(X); \pi_2(X)\};$

---

[1] Автор шифров: *Joan Daemen* (Бельгия)

$\sigma[k_m](X)$; $\theta(X)$; $\mu(X)$.

*Выход*: $X$ – $n$-битовый блок шифртекста/открытых данных.

*Замечание*. На самом деле в 3-$Way$ используется шифрующее преобразование

$ThreeWay[k_0, k_1, ..., k_m] = \omega[k_m] \circ \rho[k_{m-1}] \circ ... \circ \rho[k_0]$,

т.е. отсутствует заключительное преобразование $\mu$. В этом случае

$ThreeWay^{-1}[k_0, k_1, \dots, k_m] = \mu \circ ThreeWay[\mu(\theta(k_m)), \mu(\theta(k_{m-1})), ..., \mu(\theta(k_0))]$.

Раундовые подключи зашифрования вычисляются на основе секретного ключа $k$ по правилу $ke_i := k \oplus c_i$, $i = 0, 1, \dots, m$, где $c_i$ – раундовые константы, способ формирования которых указывается ниже при описании конкретных шифров.

Общая схема алгоритмов 3-$Way$ и $BaseKing$ представлена на рис. 1.

**3-*Way*.** Алгоритм оперирует с блоками данных $X$, представленными в виде трех 32-битовых слов: $X = (x_0, x_1, x_2)$; индексы у $x_i$ приводятся по модулю 3, т.е. $x_i \equiv x_{i \bmod 3}$. Базовые преобразования определяются следующим образом:

$\gamma(X) \equiv \{$
  ***for*** $i := 0$ ***to*** $2$ ***do*** $y_i := x_i \oplus (x_{i+1} \vee (\neg x_{i+2}))$;
  $(x_0, x_1, x_2) := (y_0, y_1, y_2)$
$\}$;

$\theta(X) \equiv \{$
  ***for*** $i := 0$ ***to*** $2$ ***do*** $y_i := shl_8 x_i \oplus shl_{24} x_i \oplus x_{i+1} \oplus rol_8 x_{i+2} \oplus shr_8 x_{i+2}$;
  $z := rol_{16}(x_0 \oplus x_1 \oplus x_2)$;
  $(x_0, x_1, x_2) := (x_0 \oplus y_0 \oplus z, x_1 \oplus y_1 \oplus z, x_2 \oplus y_2 \oplus z)$
$\}$;

$\pi 1(X) \equiv \{$
  $x_0 := rol_{22} x_0$; $x_2 := rol_2 x_2$
$\}$;

$\pi 2(X) \equiv \{$
  $x_0 := rol 1 x_0$; $x_2 := rol_{22} x_2$
$\}$.

Преобразование $\mu(X)$ меняет порядок битов в блоке $X$ на обратный (сначала меняется порядок битов в каждом из слов $x_0, x_1, x_2$, а затем слова $x_0$ и $x_2$ меняются местами).

96-битовые раундовые константы $c_i$, определяющие значения раундовых подключей зашифрования, формулируются следующим образом:

$g := 0x00000b0b$;
***for*** $i := 0$ ***to*** $m$ ***do*** $\{$
  $ci := (rol_{16} g, 0x00000000, g)$;
  $g := rol_1 g$;
  ***if*** $(g \,\&\, 0x00010000) \neq$ ***then*** $g := g \oplus 0x00011011$
$\}$.

Отметим, что последовательность $c_i$ периодична с периодом 12, а стандартное значение для $m$ – числа раундов шифрования – также равно 12.

***BaseKing*.** Алгоритм оперирует с блоками данных $X$, представленными в виде 12 16-битовых слов: $X = (x_0, x_1, \dots, x_{11})$; индексы приводятся по модулю 12, т.е. $x_i \equiv x_{i \bmod 12}$. Базовые преобразования определяются следующим образом:

$\gamma(X) \equiv \{$
  ***for*** $i := 0$ ***to*** $11$ ***do*** $y_i := x_i \oplus (x_{i+4} \vee (\neg x_{i+8}))$;
  $(x_0, x_1, \dots, x_{11}) := (y_0, y_1, \dots, y_{11})$
$\}$;

$\theta(X) \equiv \{$

$\quad \boldsymbol{for}\ i := 0\ \boldsymbol{to} 11\ \boldsymbol{do}$

$\quad y_i := x_i \oplus x_{i+2} \oplus x_{i+6} \oplus x_{i+7} \oplus x_{i+9} \oplus x_{i+10} \oplus x_{i+11};$

$\quad z := rol_{16}(x_0 \oplus x_1 \oplus x_2);$

$\quad (x0, x1, \ldots, x11) := (y0, y1, \ldots, y11)$

$\};$

$\pi[s_0, s_1, \ldots, s_{11}](X) \equiv \{$

$\quad \boldsymbol{for}\ i := 0\ \boldsymbol{to} 11\ \boldsymbol{do}\ \{$

$\quad\quad t := s_i;$

$\quad\quad x_i := ror_t\ x_i$

$\quad \}$

$\};$

(*Замечание*. Здесь $s_i$ – целые числа, определяющие величину циклического сдвига влево битов, образующих 16-битовый блок $x_i$.)

$\pi_1(\mathrm{X}) \equiv \pi\,[0, 8, 1, 15, 5, 10, 7, 6, 13, 14, 2, 3];$

$\pi_2(\mathrm{X}) \equiv \pi\,[13, 14, 2, 3, 10, 9, 6, 11, 1, 15, 8, 0].$

Преобразование $\mu(X)$ – инверсия порядка подблоков в $X$:

$\mu(X) \equiv \{\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ 5\ \boldsymbol{do}\ x_i \leftrightarrow x_{11-i}\}.$

192-раундовые константы $c_i$, используемые при вычислении раундовых подключей, формируются следующим образом:

$g := 0\mathrm{x}000b;$

$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ m\ \boldsymbol{do}\ \{$

$\quad c_i := (0,0, g, g, 0,0,0,0, g, g, 0,0);$

$\quad g := rol_1 g;$

$\quad \boldsymbol{if}\ g > 255\ \boldsymbol{then}\ g := g \oplus 0\mathrm{x}0111$

$\}.$

Как и в случае шифра 3-$Way$, последовательность $c_i$ периодична с периодом 12, и стандартное значение $m = 12$.

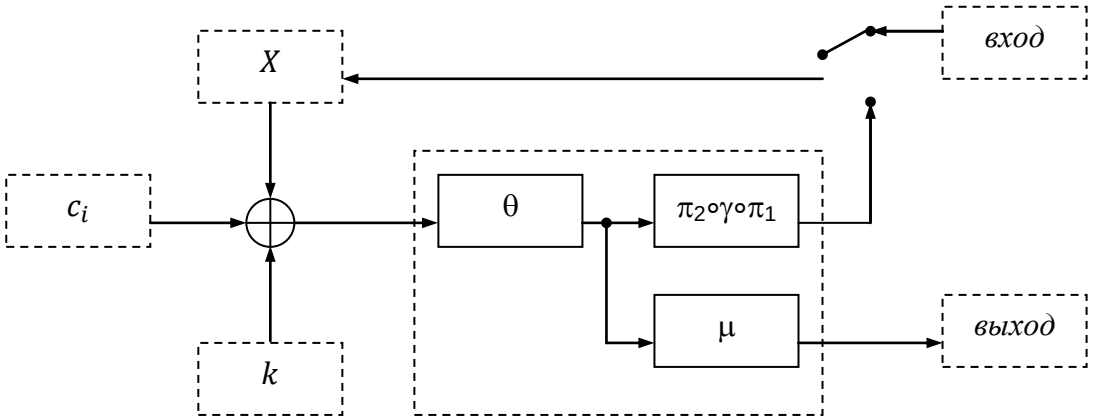


Рис. 1. *Схема алгоритмов* 3-$Way$ *и* $BaseKing$