## *Khazad*

Криптоалгоритм $Khazad$ [1] шифрует 8-байтовые блоки открытых данных под управлением 16-байтового секретного ключа.

$Khazad$ – итеративный шифр. Алгоритм оперирует с 8-байтовыми блоками данных $\mathrm{X} = (x_0, x_1,..., x_7)$ и 8-байтовыми ключами $ke = (ke_0, ke_1,..., ke_7)$, которые рассматриваются как элементы векторного пространства $\mathbb{F}_{256}^8$ над конечным полем $\mathbb{F}_{256} \cong \mathbb{F}_2[x] \,/\, f(x)$, где $f(x) = x^8 + x^4 + x^3 + x^2 + 1$.

Раундовая функция $\rho[k]$: $\mathbb{F}_{256}^8 \to \mathbb{F}_{256}^8$ с параметром $k \in \mathbb{F}_{256}$ ($k$ – раундовый подключ) является композицией трех функций:

$$\rho[k] \equiv \sigma[k] \circ \theta \circ \gamma,$$

где $f \circ g(x) = f(g(x))$.

Нелинейная функция $\gamma$: $\mathbb{F}_{256}^8 \to \mathbb{F}_{256}^8$ определяется как

$$\gamma(x_0, x_1,..., x_7) = (S[x_0], S[x_1],..., S[x_7]),$$

где $S$: $\mathbb{F}_{256} \to \mathbb{F}_{256}$, $x \mapsto S[x]$ – инволютивная подстановка, заданная табл. 1. Поскольку $S[S[x]] = x$ для любого $x \in \mathbb{F}_{256}$, то $\gamma^{-1} = \gamma$.

Линейная функция $\theta$: $\mathbb{F}_{256}^8 \to \mathbb{F}_{256}^8$ определяется как

$$\theta(x_0, x_1,..., x_7) = (x_0, x_1,..., x_7)\mathrm{H},$$

где $\mathrm{H}$ – $8 \times 8$-матрица над $\mathbb{F}_{256}$:

$$H = \begin{pmatrix} U & V \\ V & U \end{pmatrix},$$

$$U = \begin{pmatrix} 0\text{x}01 & 0\text{x}03 & 0\text{x}04 & 0\text{x}05 \\ 0\text{x}03 & 0\text{x}01 & 0\text{x}05 & 0\text{x}04 \\ 0\text{x}04 & 0\text{x}05 & 0\text{x}01 & 0\text{x}03 \\ 0\text{x}05 & 0\text{x}04 & 0\text{x}03 & 0\text{x}01 \end{pmatrix}, \qquad V = \begin{pmatrix} 0\text{x}06 & 0\text{x}08 & 0\text{x}0\text{B} & 0\text{x}07 \\ 0\text{x}08 & 0\text{x}06 & 0\text{x}07 & 0\text{x}0\text{b} \\ 0\text{x}0\text{B} & 0\text{x}07 & 0\text{x}06 & 0\text{x}08 \\ 0\text{x}07 & 0\text{x}0\text{B} & 0\text{x}08 & 0\text{x}06 \end{pmatrix}.$$

Можно проверить, что $H^2 = E$ – единичная матрица. Поэтому $\theta^{-1} = \theta$. Функция $\sigma[k]$: $\mathbb{F}_{256}^8 \to \mathbb{F}_{256}^8$ с параметром $k \in \mathbb{F}_{256}$ определяется как

$$\sigma[k](x) \equiv \mathrm{X} \oplus k.$$

Очевидно, что $\sigma^{-1}[k] = \sigma[k]$.

$R$-раундовая функция шифрования с раундовыми подключами $ke^0$, $ke^1$,..., $ke^R$, генерируемыми на основе секретного ключа $K$, – определяется как

$$Khazad[K](\mathrm{X}) \equiv \sigma[ke^R] \circ \gamma \circ \rho[ke^{R-1}] \circ ... \circ \rho[ke^1] \circ \sigma[ke^0](X).$$

Обратная функция имеет вид:

$$Khazad^{-1}[K](X) = \sigma[ke^0] \circ \rho^{-1}[ke^1] \circ ... \circ \rho^{-1}[ke^{R-1}] \circ \gamma \circ \sigma[ke^R].$$

Используя соотношения

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

нетрудно показать, что

$$Khazad^{-1}[K](X) = \sigma[kd^R] \circ \gamma \circ \rho[kd^{R-1}] \circ \ldots \circ \rho[kd^1] \circ \sigma[kd^0],$$

где $ke^0 = kd^{\mathrm{R}}$; $kd^i = kd^{\mathrm{R}-i}$; $0 < i < \mathrm{R}$; $kd^R = ke^0$. Другими словами для зашифрования и расшифрования может быть использован один и тот же алгоритм:

### Алгоритм зашифрования/расшифрования *Khazad*

*Вход*: $X$ – 8-байтовый блок открытых данных/шифртекста.

При зашифровании используются раундовые подключи $k^i = ke^i$, а при расшифровании $k^i = kd^i$, $i = 0, 1, \ldots, R$.

$X := \sigma[k^0](X)$;

***for*** $i := 1$ ***to*** $R - 1$ ***do*** $\mathrm{X} := \sigma\left[k^i\right]\left(\theta\left(\gamma(X)\right)\right)$;

$X := \sigma[k^R](\gamma(X))$.

*Выход*: $\mathrm{X}$ – 8-байтовый блок шифртекста/открытых данных.

Стандартное число раундов $R = 8$.

---

[1] Авторы шифра: *Paulo S.L.M. Barreto* (Бразилия) и *Vincent Rijmen* (Бельгия)

Раундовые подкдючи $ke^i \in \mathbb{F}_{256}^8$ генерируются на основе 16-байтового секретного ключа $K = (k_0, k_1,\ldots, k_{15})$ по правилу

$ke^{-2} := (k_0, k_1,\ldots, k_7)$;

$ke^{-1} := (k_8, k_9,\ldots, k_{15})$;

$\boldsymbol{for}\ r := 0\ \boldsymbol{to}\ R\ \boldsymbol{do}\ \ ke^r := c^r \oplus \theta\big(\gamma(ke^{r-1})\big) \oplus ke^{r-2}$.

Используемые при этом 8-байтовые раундовые константы $c^r = (c_0^r, c_1^r,\ldots, c_7^r)$, $0 \le r \le R$, определяются как

$$c_i^r = S[byte(8r + i)]\ ,\ 0 \le i \le 7,$$

где $byte(m)$ – числовое значение байта $m$.

Таблица 1

*Подстановка $S$ в $Khazad$ (в 16-ичном представлении)*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | ba | 54 | 2f | 74 | 53 | d3 | d2 | 4d | 50 | ac | 8d | bf | 70 | 52 | 9a | 4c |
| 1 | ea | d5 | 97 | d1 | 33 | 51 | 5b | a6 | de | 48 | a8 | 99 | db | 32 | b7 | fc |
| 2 | e3 | 9e | 91 | 9b | e2 | bb | 41 | 6e | a5 | cb | 6b | 95 | a1 | f3 | b1 | 02 |
| 3 | cc | c4 | 1d | 14 | c3 | 63 | da | 5d | 5f | dc | 7d | cd | 7f | 5a | 6c | 5c |
| 4 | f7 | 26 | ff | ed | e8 | 9d | 6f | 8e | 19 | a0 | f0 | 89 | 0f | 07 | af | fb |
| 5 | 08 | 15 | 0d | 04 | 01 | 64 | df | 76 | 79 | dd | 3d | 16 | 3f | 37 | 6d | 38 |
| 6 | b9 | 73 | e9 | 35 | 55 | 71 | 7b | 8c | 72 | 88 | f6 | 2a | 3e | 5e | 27 | 46 |
| 7 | 0c | 65 | 68 | 61 | 03 | c1 | 57 | d6 | d9 | 58 | d8 | 66 | d7 | 3a | c8 | 3c |
| 8 | fa | 96 | a7 | 98 | ec | b8 | c7 | ae | 69 | 4b | ab | a9 | 67 | 0a | 47 | f2 |
| 9 | b5 | 22 | e5 | ee | be | 2b | 81 | 12 | 83 | 1b | 0e | 23 | f5 | 45 | 21 | ce |
| a | 49 | 2c | f9 | e6 | b6 | 28 | 17 | 82 | 1a | 8b | fe | 8a | 09 | c9 | 87 | 4e |
| b | e1 | 2e | e4 | e0 | eb | 90 | a4 | 1e | 85 | 60 | 00 | 25 | f4 | f1 | 94 | 0b |
| c | e7 | 75 | ef | 34 | 31 | d4 | d0 | 86 | 7e | ad | fd | 29 | 30 | 3b | 9f | f8 |
| d | c6 | 13 | 06 | 05 | c5 | 11 | 77 | 7c | 7a | 78 | 36 | 1c | 39 | 59 | 18 | 56 |
| e | b3 | b0 | 24 | 20 | b2 | 92 | a3 | c0 | 44 | 62 | 10 | b4 | 84 | 43 | 93 | c2 |
| f | 4a | bd | 8f | 2d | bc | 9c | 6a | 40 | cf | a2 | 80 | 4f | 1f | ca | aa | 42 |

Например: $S[0\text{x}7a] = 0\text{x}d8$.