Anubis

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

Каждый 16-байтовый блок $b_0 b_1 \dots b_{15}$, участвующий в криптографическом преобразовании, представляется в виде 4×4-матрицы

$$A = (a_{ij}) = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} b_0 & b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 & b_7 \\ b_8 & b_9 & b_{10} & b_{11} \\ b_{12} & b_{13} & b_{14} & b_{15} \end{pmatrix}.$$

Множество таких матриц обозначим через M. В алгоритме используются следующие функции, аргументами, параметрами и значениями которых являются матрицы из M:

$\tau(A)$ – матрица, полученная из A транспонированием;

$\gamma(A)$ – матрица, полученная из A заменой каждого ее элемента a_{ij} на $S[a_{ij}]$, где S – подстановка на множестве байтов, заданная табл. 1;

$\theta(A) = A \cdot \mathrm{H}$, $\omega(\mathrm{A}) = V \cdot A$,

где

$$H = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \quad V = \begin{pmatrix} 0x01 & 0x01 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x02^2 & 0x02^3 \\ 0x01 & 0x06 & 0x06^2 & 0x06^3 \\ 0x01 & 0x08 & 0x08^2 & 0x08^3 \end{pmatrix}$$

– матрицы, элементы которых (байты) интерпретируются как элементы конечного поля $\mathbb{F}_{256} \cong \mathbb{F}_2[x]/p(x)$, $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ (при вычислении произведений $A \cdot H$ и $V \cdot A$ матрица A также рассматривается над полем $\mathbb{F}_{256}$);

$$\pi(A) = \begin{pmatrix} a_{00} & a_{31} & a_{22} & a_{13} \\ a_{10} & a_{01} & a_{32} & a_{23} \\ a_{20} & a_{11} & a_{02} & a_{33} \\ a_{30} & a_{21} & a_{12} & a_{03} \end{pmatrix}$$

(другими словами, функция π возвращает матрицу, получающуюся из A циклическим сдвигом ее столбцов вниз соответственно на 0, 1, 2 и 3 позиций);

$\sigma[k](A) = A \oplus k$ – добавление к матрице A ключа k – побитовое сложение по модулю 2 элементов матриц A и k;

Раундовая функция $\rho[k]$: $M \to M$ определяется как

$\rho[k](A) = \sigma[k] \circ \theta \circ \tau \circ \gamma\,(\mathrm{A})$,

где $f \circ g(A) \equiv f(g(\mathrm{A}))$.

Отметим следующие свойства введенных функций:

$\tau^{-1} = \tau$, $\gamma^{-1} = \gamma$, $\theta^{-1} = \theta$, $\sigma^{-1}[k] = \sigma[k]$,

т.е. γ, τ, θ и $\sigma[k]$ инволютивны,

$\tau \circ \gamma = \gamma \circ \tau$,

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

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

Шифрующая функция в $Anubis$ определена (при раундовых ключах k_0, k_1, …, k_R) как

$Anubis\,[k_0, k_1, \dots, k_R](\mathrm{A}) = \sigma[k_R] \circ \tau \circ \gamma \circ \rho[k_{R-1}] \circ \dots \circ \rho[k_1] \circ \sigma[k_0](A)$.

Обратная функция имеет вид:

$Anubis^{-1}[k_0, k_1, \dots, k_R](A)$

$= \sigma^{-1}[k_0] \circ \rho^{-1}[k_1] \circ \dots \circ \rho^{-1}[k_{R-1}] \circ \gamma^{-1} \circ \tau^{-1} \circ \sigma^{-1}[k_R](A)$.

С учетом отмеченных свойств функций τ, γ, θ и σ нетрудно показать, что

---

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

$$Anubis^{-1}[k_0, k_1,\ldots, k_R](A) = Anubis\ [k_R, \theta(k_{R-1}),\ldots, \theta(k_1), k_0](A).$$

Другими словами, алгоритм $Anubis$ симметричен, т.е. может быть использован как для зашифрования, так и для расшифрования. Но при этом раундовые подключи расшифрования ke_0, ke_1, …, ke_R и раундовые подключи расшифрования kd_0, kd_1, …, kd_R должны быть связаны соотношениями:

$$ke_0 = kd_R; \quad ke_i = kd_{R-i}, 1 \le i \le R-1; \quad ke_R = kd_0.$$

Раундовые подключи ke_i генерируются, исходя из секретного ключа K, по следующей схеме:

$L := K;$

$ke_0 := \tau \circ \omega \circ \gamma(L);$

for $i := 1$ ***to*** R ***do*** {

$L := \sigma\left[C^i\right] \circ \theta \circ \pi \circ \gamma(L);$

$ke_i := \tau \circ \omega \circ \gamma(L)$

}.

Используемые при этом константы C^i определяются как

$$C^i = \begin{pmatrix} S[4i-4] & S[4i-3] & S[4i-2] & S[4i-1] \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Стандартное число раундов (число использований раундовой функции ρ при шифровании) $R = 12$.

Таблица 1

Подстановка S в $Anubis$ (в 16-ичном представлении)

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

Пояснение к таблице. Для байта $0\text{x}b_1b_2$ значение $S[0\text{x}b_1b_2]$ находятся на пересечении строки b_1 и столбца b_2. Например, $S[0\text{x}5f] = 0\text{x}4e$.