$CS-Cipher$

Криптоалгоритм $CS\text{-}Cipher$ (от франц. $"Chiffrement\ Symetrique"$, $Symmetric\ Cipher$) [1] преобразует 64-битовый блок открытых данных $m = m_{63}\dots m_1 m_0$ в 64-битовый блок шифртекста $m' = m'_{63}\dots m'_1 m'_0$, под управлением 128-битового секретного ключа $k = k_{127}\dots k_1 k_0$.

Обозначения. Символ $\|$ обозначает конкатенацию блоков; n-битовый блок $x = x_{n-1} \| \dots \| x_1 \| x_0$ интерпретируется как целое число $x_{n-1}2^{n-1}+\dots+x_1 2^1 + x_0$; биты в блоке нумеруются справа налево, начиная с 0, т.е. x_0 – младший бит в блоке x; $x_{m..n}$ – сокращенная запись для $x_m \| x_{m-1} \|\dots\| x_n$ $(m \geq n)$; для 8-битового блока (байта) x его левый (старший) и правый (младший) полубайты обозначаются как $x.l$ и $x.r$; аналогично, для двухбайтового блока x его левая и правая половины обозначаются как $x.L$ и $x.R$; $\oplus$ и $\&$ – операции побитового сложения по модулю 2 и умножения (коньюнкции) для блоков одинаковой длины; rol_1 – циклический сдвиг байта влево на один бит.

В алгоритме шифрования используются 64-битовые подключи k^0, k^1,…, k^8, генерируемые на основе секретного ключа $k = k^{-1} \| k^{-2}$ по итерационно схеме:

$k^i := k^{i-2} \oplus F(k^{i-1}, c^i)$ для $i = 0, 1,..., 8,$

где c^i – 64-битовые константы:

$$c^0 = 0x290d61409ceb9e8f$$
$$c^1 = 0x1f855f585b013986$$
$$c^2 = 0x972ed7d635ae1716$$
$$c^3 = 0x21b6694ea5728708$$
$$c^4 = 0x3c18e6e7faadb889$$
$$c^5 = 0xb700f76f73841163$$
$$c^6 = 0x3f967f6ebf149dac$$
$$c^7 = 0xa40e7ef6204a6230$$
$$c^8 = 0x03c54b5a46a34465$$

Функция F с 64-битовыми аргументами и значением определена как

$$F(x, c) = T(P_8(x \oplus c)),$$

где P_8 определяется как

$$P_8(x_{63..0}) = P(x_{63..56}) \| P(x_{55..48}) \|\dots\| P(x_{7..0}).$$

P – перестановка (подстановка) на множестве байтов; её значение

$$y.l \| y.r = P(x.l \| x.r)$$

для байта x вычисляется следующим образом:

$$z := x.l \oplus f(x.r);\ y.r := x.r \oplus g(z);\ y.l := z \oplus f(y.r),$$

где f и g – функции, заданные табл. 1. Подстановка P приведена в табл. 2.

Преобразование T – перестановка битов в 64-битовом блоке: бит из позиции $8i + j$ перемещается в позицию $8j + i$, $0 \leq i, j \leq 7$:

$$T(z_{63..0}) = z_{63}z_{55} \|\dots\| z_7 \| z_{62} \| z_{54} \|\dots\| z_6 \|\dots\| z_{56} \| z_{48} \|\dots\| z_0.$$

Отметим, что преобразования P и T инволютивны, т.е. $P^{-1} = P$, $T^{-1} = T$.

Таблица 1

Функции f и g в CS-Cipher

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$f(x)$	f	d	b	b	7	5	7	7	e	d	a	b	e	d	e	f
$g(x)$	a	6	0	2	b	e	1	8	d	4	5	3	f	c	7	9

[1] Авторы шифра: *Jacques Stern* и *Serge Vaudenau* (Франция)

Таблица 2

Подстановка P в CS-Cipher

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

Алгоритм зашифрования

Блок открытых данных m преобразуется в блок шифртекста m′ по правилу:

$$m' = \sigma[k^8] \circ \rho[k^7] \circ \rho[k^6] \circ \ldots \circ \rho[k^1] \circ \rho[k^0](m), = m'_{63} \ldots m'_1 m'_0$$

где $f \circ g(x) \equiv f(g(x))$.

Функция $\sigma[k']$ определяется как $\sigma[k](x) \equiv x \oplus k'$.

Раундовая функция $\rho[k']$ является композицией функций σ, M_4 и R с использованием 64-битовых констант [2]:

$$c = 0\text{x}b7e151628aed2a6a,\ c' = 0\text{x}bf7158809cf4f3c7,$$

а именно:

$$\rho[k'] = \varepsilon \circ \sigma[k],$$

где

$$\varepsilon = R \circ M_4 \circ \sigma[c'] \circ R \circ M_4 \circ \sigma[c] \circ R \circ M_4.$$

Функция M_4 определяется как

$$M_4(z_{63..0}) = M(z_{63..48}) \parallel M(z_{47..32}) \parallel M(z_{31..16}) \parallel M(z_{15..0}),$$

где M – функция от двухбайтового аргумента x, возвращающая двухбайтовое значение $y = y.L \parallel y.R$:

$y.L = P((rol_1(x.L)\&0\text{x}55) \oplus x.L \oplus x.R)$;

$y.R = P(rol_1 1(x.L) \oplus x.R)$.

Функция R – перестановка байтов в 64-битовом (8-байтовом) блоке:

$$R(z_{63..56} \parallel z_{55..48} \parallel z_{47..40} \parallel z_{39..32} \parallel z_{31..24} \parallel z_{23..16} \parallel z_{15..8} \parallel z_{7..0}) =$$
$$z_{63..56} \parallel z_{47..40} \parallel z_{31..24} \parallel z_{15..8} \parallel z_{55..48} \parallel z_{39..32} \parallel z_{23..16} \parallel z_{7..0}.$$

Алгоритм расшифрования

Блок шифртекста m' преобразуется в блок открытых данных m по правилу:

$$m := \rho^{-1}[k_0] \circ \rho^{-1}[k_1] \circ \ldots \circ \rho^{-1}[k_7] \circ \sigma[k_8],$$

где

$$\rho^{-1}[k'] = M_4^{-1} \circ R^{-1} \circ \sigma[c] \circ M_4^{-1} \circ R^{-1} \circ \sigma[c'] \circ M_4^{-1} \circ R^{-1} \circ \sigma[k'],$$

---

[2] Константа $c \parallel c'$ образована первыми 32 цифрами дробной части числа

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 2.\text{b7e251628aed2a6abf7158809cf4f3c762e7160f}_{16} \ldots,$$

в 16-ичном представлении.

а R^{-1} и M_4^{-1} определяются как

$$R^{-1}(z_{63..56} \parallel z_{55..48} \parallel z_{47..40} \parallel z_{39..32} \parallel z_{31..24} \parallel z_{23..16} \parallel z_{15..8} \parallel z_{7..0}) =$$
$$z_{63..56} \parallel z_{31..24} \parallel z_{55..48} \parallel z_{23..16} \parallel z_{47..40} \parallel z_{15..8} \parallel z_{39..32} \parallel z_{7..0};$$
$$\mathrm{M}_4^{-1}(x.L \parallel x.R) = y.L \parallel y.R;$$
$$y.L = (rol_1(P(x.L) \oplus P(x.R))\&0\text{x}aa) \oplus P(x.L) \oplus P(x.R),$$
$$y.R = rol_1(y.L) \oplus P(x.R).$$

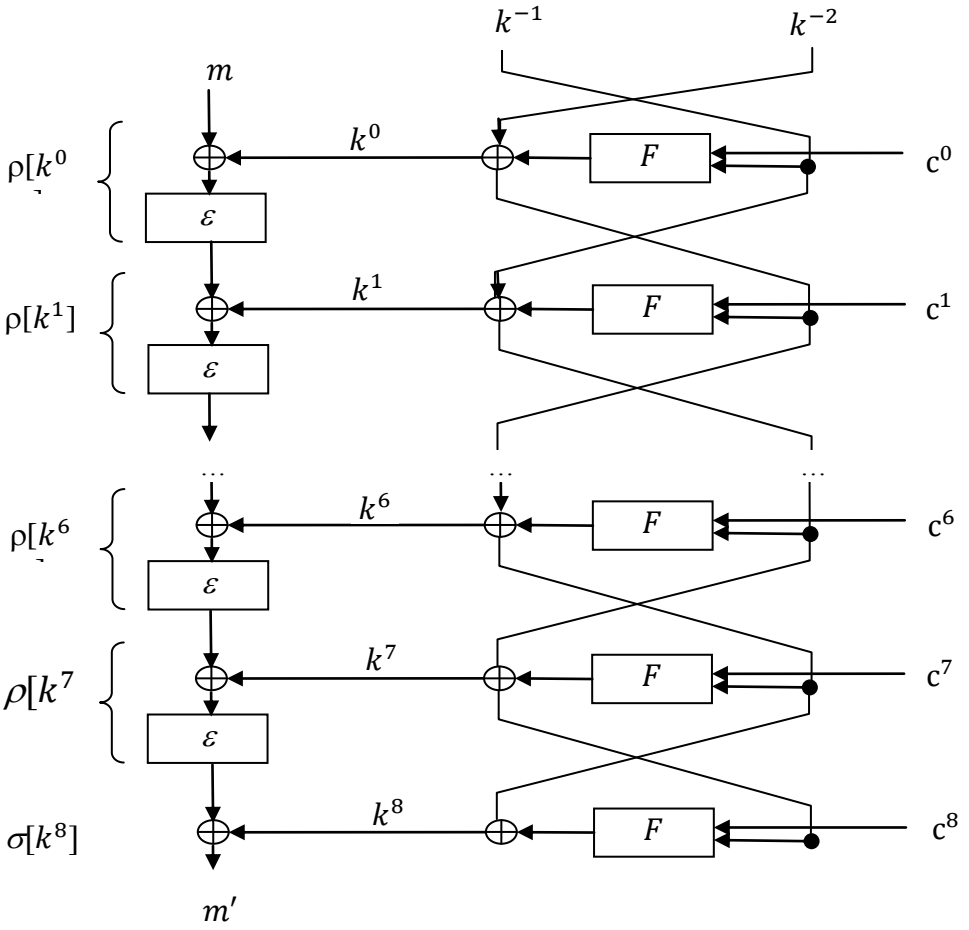

Рис. 1. *Процесс зашифрования в CS-Cipher*