Skipjack

Криптоалгоритм $Skipjack$[1] шифрует 64-битовые блоки открытых данных под управлением 80-битового секретного ключа. Секретный ключ K представляется в виде массива из 10 байтов:

$$K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9,),$$

а 64-битовый блок открытых данных W, над которым осуществляется криптографическое преобразование, в виде массива из четырех двухбайтовых слов: $W = (w_1, w_2, w_3, w_4,)$ (в словах левый байт, расположенный в младшей адресной позиции, считается старшим). В алгоритме шифрования, состоящем из 32 раундов, используются преобразования $A_r(W)$ и $B_r(W)$ и обратные к ним преобразования $A_r^{-1}(W)$ и $B_r^{-1}(W)$, $1 \le r \le 32$ (см. рис. 1):

$A_r(W)$	$B_r(W)$
$z := w_4;$	$z := w_4;$
$w_4 := w_3;$	$w_4 := w_3;$
$w_3 := w_2;$	$w_3 := w_1 \oplus w_2 \oplus word(r);$
$w_2 := G_r(w_1);$	$w_2 := G_r(w_1);$
$w_1 := w_2 \oplus z \oplus word(r).$	$w_1 := z.$

$A_r^{-1}(W)$	$B_r^{-1}(W)$
$z := w_4;$	$z := w_1;$
$w_4 := w_1 \oplus w_2 \oplus word(r);$	$w_1 := G_r^{-1}(w_2);$
$w_1 := G_r^{-1}(w_2);$	$w_2 := w_1 \oplus w_3 \oplus word(r);$
$w_2 := w_3;$	$w_3 := w_4;$
$w_3 := z.$	$w_4 := z.$

Здесь $word(r)$ – двухбайтовое слово с числовым значением r (младший байт со значением r расположен справа, в старшей адресной позиции); символ $\oplus$ обозначает побитовое сложение по модулю 2.

Преобразования G_r (в A_r и B_r) и обратное к нему G_r^{-1} (в A_r^{-1} и B_r^{-1}) являются подстановками (т.е. взаимно однозначными отображениями) на множестве двухбайтовых слов. Они построены в соответствии с четырехраундовой схемой Фейстеля (см.рис. 2). Используемая при этом раундовая функция F является таблично заданной подстановкой на множестве байтов (см. табл. 1). Значения $b_5 \,||\, b_6 = G_r(b_1 \,||\, b_2)$ и $b_1 \,||\, b_2 = G_r^{-1}(b_5 \,||\, b_6)$ вычисляются следующим образом:

G_r	G_r^{-1}
$b_3 := F(b_2 \oplus k_{4r-4}) \oplus b_1;$	$b_4 := F(b_5 \oplus k_{4r-1}) \oplus b_6;$
$b_4 := F(b_3 \oplus k_{4r-3}) \oplus b_2;$	$b_3 := F(b_4 \oplus k_{4r-3}) \oplus b_5;$
$b_5 := F(b_4 \oplus k_{4r-2}) \oplus b_3;$	$b_2 := F(b_3 \oplus k_{4r-3}) \oplus b_4;$
$b_6 := F(b_5 \oplus k_{4r-1}) \oplus b_4.$	$b_1 := F(b_2 \oplus k_{4r-4}) \oplus b_3.$

Индексы у k_i приводят по модулю 10, так что $k_{10} \equiv k_0$, $k_{11} \equiv k_1$ и т.д.

[1] Шифр разработан *Агенством Национальной Безопасности* США

Алгоритм зашифрования *Skipjack*

Вход: W – 64-битовый блок открытых данных.

$\boldsymbol{for}\ r := 1\ \boldsymbol{to}\ 32\ \boldsymbol{do}$

$\boldsymbol{if}\ (r \le 8) \vee (17 \le r \le 24)\ \boldsymbol{then}\ A_r(W)\ \boldsymbol{else}\ B_r(W)\ \boldsymbol{.}$

Выход: W – 64-битовый блок шифртекста.

Алгоритм расшифрования *Skipjack*

Вход: W – 64-битовый блок шифртекста.

$\boldsymbol{for}\ r := 32\ \boldsymbol{downto}\ 1\ \boldsymbol{do}$

$\boldsymbol{if}\ (r \le 8) \vee (17 \le r \le 24) \boldsymbol{then}\ A_r^{-1}(W) \boldsymbol{else}\ B_r^{-1}(W)\ \boldsymbol{.}$

Выход: W – 64-битовый блок открытых данных.

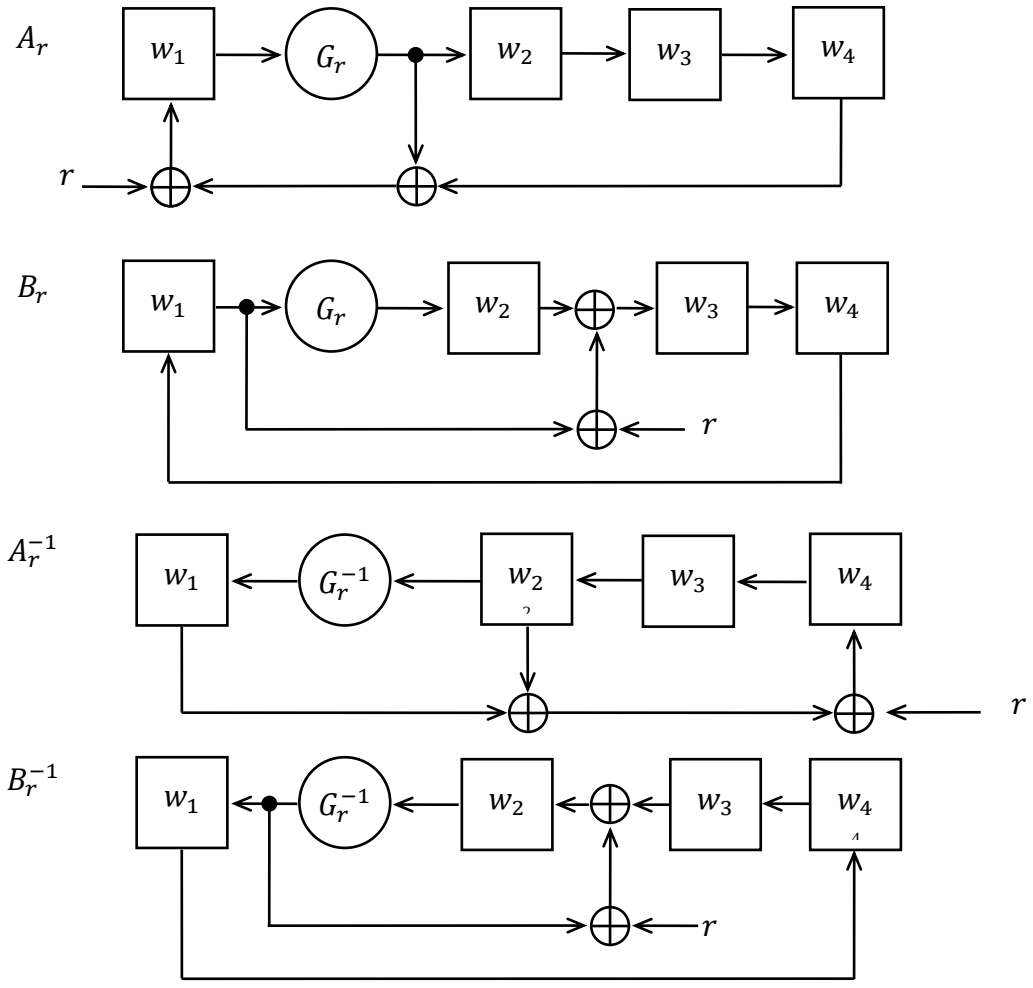

Рис. 1. *Преобразования* A_r, B_r, A_r^{-1}, B_r^{-1} *в Skipjack*

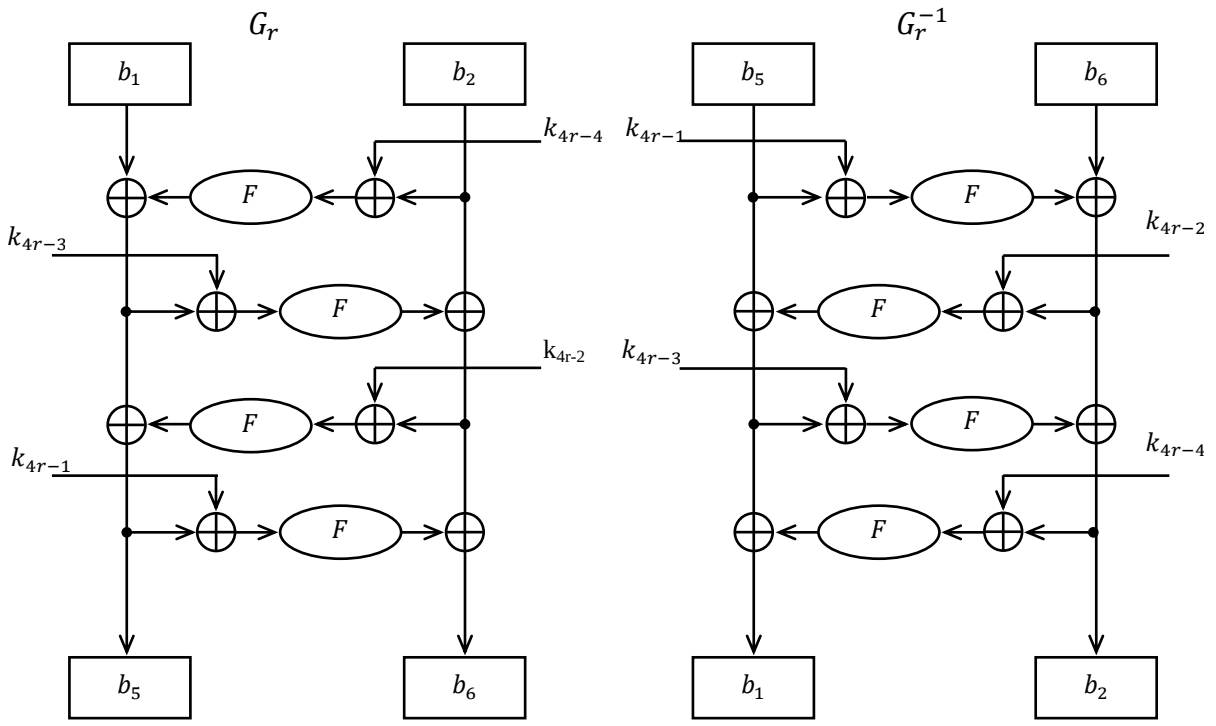

Рис. 2. Подстановки G_r и G_r^{-1} в $Skipjack$

Таблица 1

Подстановка F в $Skipjack$ в 16-ичном представлении

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

Пояснение к табл.1. Для байта $0\text{x}b_1b_2$ значение $F(b_1b_2)$ находится на пересечении строки с номером b_1 и столбцом с номером b_2. Например, $F(0\text{x}8b) = 0\text{x}d4$.