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 \bigoplus 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 одназначными 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 $b_5 \mid\mid b_6 = G_r(b_1 \mid\mid b_2)$ и $b_1 \mid\mid b_2 = G_r^{-1}(b_5 \mid\mid b_6)$ 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

Bxod: W - 64-битовый блок открытых данных.

for r := 1 to 32 do

if $(r \le 8) \lor (17 \le r \le 24)$ then $A_r(W)$ else $B_r(W)$.

Выход: W - 64-битовый блок шифртекста.

Алгоритм расшифрования Skipjack

Вход: W - 64-битовый блок шифртекста.

for r := 32 downto 1 do

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

Bыход: W - 64-битовый блок открытых данных.

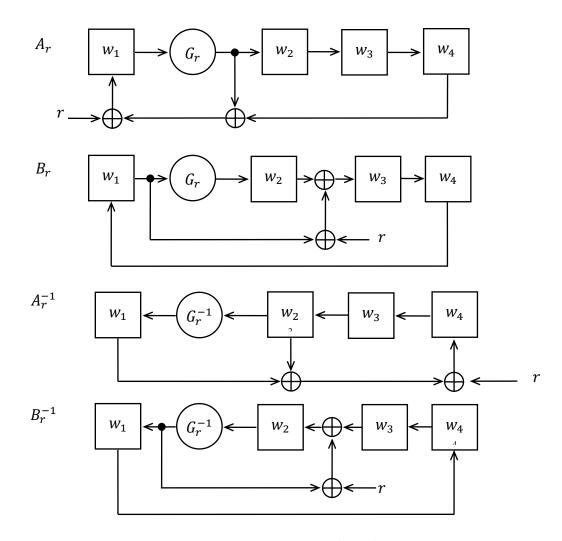


Рис. 1. Преобразования $A_r,\,B_r,\,A_r^{-1},\,B_r^{-1}\varepsilon$ Skipjack

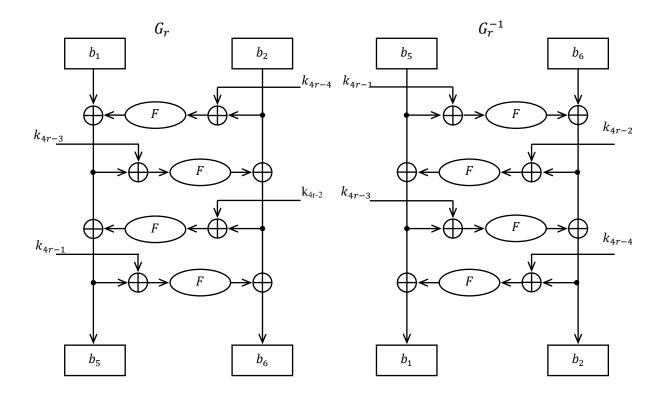


Рис. 2. Подстановки G_r и G_r^{-1} в Skipjack

Таблица 1

		1	T		-	_ ~ .		-							
Подстановка F в $Skipjack$ в 16-ичном представлении															
0	1	2	3	4	5	6	7	8	9	а	b	С	d	e	f
a3	d7	09	83	f8	48	f6	f4	b3	21	15	78	99	b1	af	f9
e7	2d	4d	8a	ce	4c	ca	2e	52	95	d9	1e	4e	38	44	28
0a	df	02	a0	17	f1	60	68	12	b7	7a	с3	e9	fa	3d	53
96	84	6b	ba	f2	63	9a	19	7c	ae	e5	f5	f7	16	6a	a2
39	b6	7b	0f	c1	93	81	1b	ee	b4	1a	ea	d0	91	2f	b8
55	b9	da	85	3f	41	bf	e0	5a	58	80	5f	66	0b	d8	90
35	d5	c0	a7	33	06	65	69	45	00	94	56	6d	98	9b	76
97	fc	b2	c2	b0	fe	db	20	e1	eb	d6	e4	dd	47	4a	1d
42	ed	9e	6e	49	3c	cd	43	27	d2	07	d4	de	c 7	67	18
89	cb	30	1f	8d	с6	8f	aa	c8	74	dc	с9	5d	5c	31	a4
70	88	61	2c	9f	0d	2b	87	50	82	54	64	26	7d	03	40
34	4b	1c	73	d1	c4	fd	3b	СС	fb	7f	ab	e6	3e	5b	a5
ad	04	23	9с	14	51	22	f0	29	79	71	7e	ff	8c	0e	e2
0с	ef	bc	72	75	6f	37	a1	ec	d3	8e	62	8b	86	10	e8
08	77	11	be	92	4f	24	c5	32	36	9d	cf	f3	a6	bb	ac
5e	6c	a9	13	57	25	b5	e3	bd	a8	3a	01	05	59	2a	46
	a3 e7 0a 96 39 55 35 97 42 89 70 34 ad 0c 08	a3 d7 e7 2d 0a df 96 84 39 b6 55 b9 35 d5 97 fc 42 ed 89 cb 70 88 34 4b ad 04 0c ef 08 77	0 1 2 a3 d7 09 e7 2d 4d 0a df 02 96 84 6b 39 b6 7b 55 b9 da 35 d5 c0 97 fc b2 42 ed 9e 89 cb 30 70 88 61 34 4b 1c ad 04 23 0c ef bc 08 77 11	0 1 2 3 a3 d7 09 83 e7 2d 4d 8a 0a df 02 a0 96 84 6b ba 39 b6 7b 0f 55 b9 da 85 35 d5 c0 a7 97 fc b2 c2 42 ed 9e 6e 89 cb 30 1f 70 88 61 2c 34 4b 1c 73 ad 04 23 9c 0c ef bc 72 08 77 11 be	0 1 2 3 4 a3 d7 09 83 f8 e7 2d 4d 8a ce 0a df 02 a0 17 96 84 6b ba f2 39 b6 7b 0f c1 55 b9 da 85 3f 35 d5 c0 a7 33 97 fc b2 c2 b0 42 ed 9e 6e 49 89 cb 30 1f 8d 70 88 61 2c 9f 34 4b 1c 73 d1 ad 04 23 9c 14 0c ef bc 72 75 08 77 11 be 92	0 1 2 3 4 5 a3 d7 09 83 f8 48 e7 2d 4d 8a ce 4c 0a df 02 a0 17 f1 96 84 6b ba f2 63 39 b6 7b 0f c1 93 55 b9 da 85 3f 41 35 d5 c0 a7 33 06 97 fc b2 c2 b0 fe 42 ed 9e 6e 49 3c 89 cb 30 1f 8d c6 70 88 61 2c 9f 0d 34 4b 1c 73 d1 c4 ad 04 23 9c 14 51 0c ef bc 72 75<	0 1 2 3 4 5 6 a3 d7 09 83 f8 48 f6 e7 2d 4d 8a ce 4c ca 0a df 02 a0 17 f1 60 96 84 6b ba f2 63 9a 39 b6 7b 0f c1 93 81 55 b9 da 85 3f 41 bf 35 d5 c0 a7 33 06 65 97 fc b2 c2 b0 fe db 42 ed 9e 6e 49 3c cd 89 cb 30 1f 8d c6 8f 70 88 61 2c 9f 0d 2b 34 4b 1c 73 d1 c4 fd	0 1 2 3 4 5 6 7 a3 d7 09 83 f8 48 f6 f4 e7 2d 4d 8a ce 4c ca 2e 0a df 02 a0 17 f1 60 68 96 84 6b ba f2 63 9a 19 39 b6 7b 0f c1 93 81 1b 55 b9 da 85 3f 41 bf e0 35 d5 c0 a7 33 06 65 69 97 fc b2 c2 b0 fe db 20 42 ed 9e 6e 49 3c cd 43 89 cb 30 1f 8d c6 8f aa 70 88 61 2c	0 1 2 3 4 5 6 7 8 a3 d7 09 83 f8 48 f6 f4 b3 e7 2d 4d 8a ce 4c ca 2e 52 0a df 02 a0 17 f1 60 68 12 96 84 6b ba f2 63 9a 19 7c 39 b6 7b 0f c1 93 81 1b ee 55 b9 da 85 3f 41 bf e0 5a 35 d5 c0 a7 33 06 65 69 45 97 fc b2 c2 b0 fe db 20 e1 42 ed 9e 6e 49 3c cd 43 27 89 cb 30	0 1 2 3 4 5 6 7 8 9 a3 d7 09 83 f8 48 f6 f4 b3 21 e7 2d 4d 8a ce 4c ca 2e 52 95 0a df 02 a0 17 f1 60 68 12 b7 96 84 6b ba f2 63 9a 19 7c ae 39 b6 7b 0f c1 93 81 1b ee b4 55 b9 da 85 3f 41 bf e0 5a 58 35 d5 c0 a7 33 06 65 69 45 00 97 fc b2 c2 b0 fe db 20 e1 eb 42 ed 9e 6e	0 1 2 3 4 5 6 7 8 9 a a3 d7 09 83 f8 48 f6 f4 b3 21 15 e7 2d 4d 8a ce 4c ca 2e 52 95 d9 0a df 02 a0 17 f1 60 68 12 b7 7a 96 84 6b ba f2 63 9a 19 7c ae e5 39 b6 7b 0f c1 93 81 1b ee b4 1a 55 b9 da 85 3f 41 bf e0 5a 58 80 35 d5 c0 a7 33 06 65 69 45 00 94 97 fc b2 c2 b0 fe db	0 1 2 3 4 5 6 7 8 9 a b a3 d7 09 83 f8 48 f6 f4 b3 21 15 78 e7 2d 4d 8a ce 4c ca 2e 52 95 d9 1e 0a df 02 a0 17 f1 60 68 12 b7 7a c3 96 84 6b ba f2 63 9a 19 7c ae e5 f5 39 b6 7b 0f c1 93 81 1b ee b4 1a ea 55 b9 da 85 3f 41 bf e0 5a 58 80 5f 35 d5 c0 a7 33 06 65 69 45 00 94 56	0 1 2 3 4 5 6 7 8 9 a b c a3 d7 09 83 f8 48 f6 f4 b3 21 15 78 99 e7 2d 4d 8a ce 4c ca 2e 52 95 d9 1e 4e 0a df 02 a0 17 f1 60 68 12 b7 7a c3 e9 96 84 6b ba f2 63 9a 19 7c ae e5 f5 f7 39 b6 7b 0f c1 93 81 1b ee b4 1a ea d0 55 b9 da 85 3f 41 bf e0 5a 58 80 5f 66 35 d5 c0 a7 33<	0 1 2 3 4 5 6 7 8 9 a b c d a3 d7 09 83 f8 48 f6 f4 b3 21 15 78 99 b1 e7 2d 4d 8a ce 4c ca 2e 52 95 d9 1e 4e 38 0a df 02 a0 17 f1 60 68 12 b7 7a c3 e9 fa 96 84 6b ba f2 63 9a 19 7c ae e5 f5 f7 16 39 b6 7b off c1 93 81 1b ee b4 1a ea d0 91 55 b9 da 85 3f 41 bf e0 5a 58 80 5f 66	0 1 2 3 4 5 6 7 8 9 a b c d e a3 d7 09 83 f8 48 f6 f4 b3 21 15 78 99 b1 af e7 2d 4d 8a ce 4c ca 2e 52 95 d9 1e 4e 38 44 0a df 02 a0 17 f1 60 68 12 b7 7a c3 e9 fa 3d 96 84 6b ba f2 63 9a 19 7c ae e5 f5 f7 16 6a 39 b6 7b 0f c1 93 81 1b ee b4 1a ea d0 91 2f 55 b9 da 85 3f 41 bf </td

Пояснение к табл. 1. Для байта $0xb_1b_2$ значение $F(b_1b_2)$ находится на пересечении строки с номером b_1 и столбцом с номером b_2 . Например, F(0x8b) = 0xd4.