DES

Стандарт шифрования данных DES ($Data\ Encryption\ Standard$) опубликован в США в 1977 году, а в 1980 году DES принят Национальным институтом стандартов и технологий США ($NIST$) в качестве стандарта шифрования данных для защиты от несанкционированного доступа несекретной информации государственного и коммерческого характера.

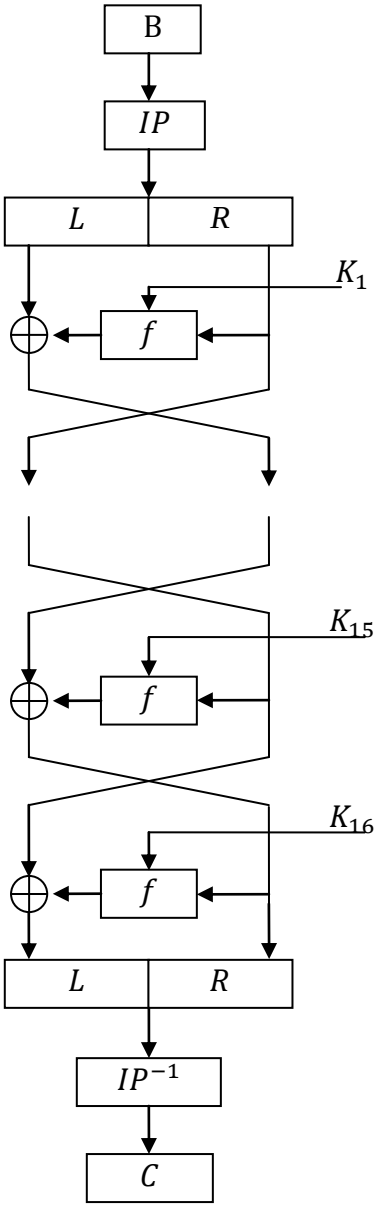


Рис. 1. *Алгоритм DES* (DEA)

Криптоалгоритм DEA (Data Encryption Algorithm), реализующий DES, шифрует 64-битовые блоки открытых данных под управлением 56-битового секретного ключа.

Замечание. Ключ обычно представляется в виде 64-битового блока KS, но каждый восьмой бит отбрасывается. Пользователь выбирает ключ K, содержащий 56 случайных битов, но затем к каждым семи битам добавляется восьмой бит так, чтобы в каждом получающемся байте было нечетное число битовых единиц. Это используется для обнаружения ошибок в ключе при обмене и хранении ключей.

DES построен в соответствии со схемой Фейстеля (см. рис. 1). Для зашифрования и расшифрования применяется один и тот же алгоритм. Различие состоит лишь в том, что при расшифровании раундовые подключи используются в обратном порядке.

Алгоритм зашифрования

Вход : $B = L \parallel R$ – 64-битовый блок открытых данных, представленных в виде конкатенации 32-битовых подблоков L и R, в которой R следует за L.

Шаг 1. (Начальная подстановка.)

$$B := IP(B);$$

Шаг 2. (16 раундов шифрования под управлением 16 48-битовых раундовых подключей.)

for $i := 1$ ***to*** 15 ***do*** {

$L := L \oplus f(R, K_i)$;

LR

};

$L := L \oplus f(R, K_{16})$;

$B := L \parallel R$;

Шаг 3. (Заключительная подстановка.)

$C := IP^{-1}(P)$.

Выход: C – 64-битовый блок шифртекста.

Биты в блоках нумеруются слева направо, начиная с 1. Начальная перестановка IP задаётся таблицей 1: бит 58 блока открытых данных B перемещается в позицию 1, бит 50 – в позицию 2,…, бит 7 – в позицию 64.

Таблица 1

Начальная перестановка IP в DES

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	33	15	7

Заключительная перестановка IP^{-1}, заданная табл. 2, является обратной перестановкой по отношению к IP.

Таблица 2

Заключительная перестановка IP^{-1} в DES

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Раундовая функция f называется *функцией шифрования*. Её аргументами являются 32-битовый блок R и 48-битовый раундовый подключ k. Схема вычисления 32-битового значения $f(R,k)$ представлена на рис. 2.

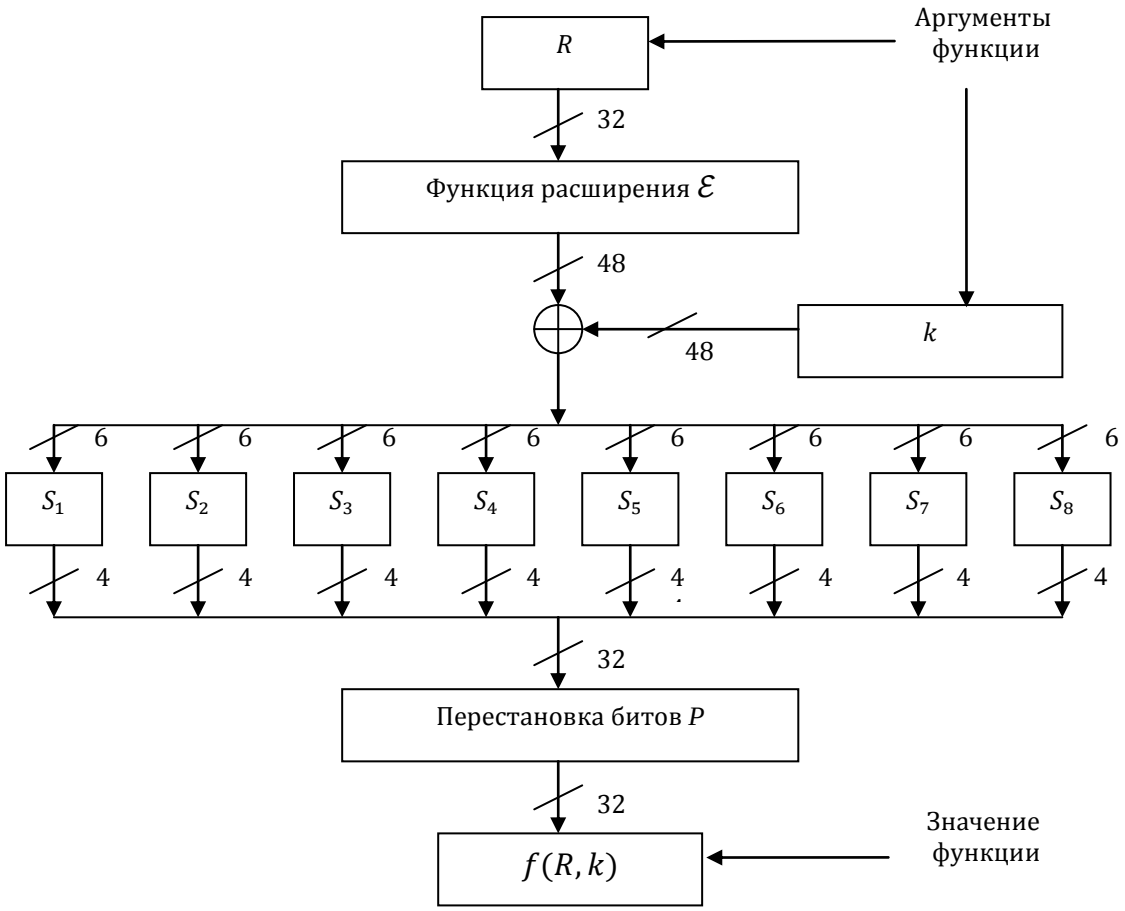


Рис.2. *Функция шифрования f в DES*

Функция f является композицией четырёх функций: $f(R,k) = P(S(\mathcal{E}(R) \oplus k)))$.

Функция $\mathcal{E}$ ″расширяет″ 32-битовый блок R до 48-битового блока $\mathcal{E}(R)$ путём дублирования некоторых битов блока R (см. рис. 3). Операция расширения выполняется следующим образом: подблок R разбивается на восемь 4-битовых подблоков; затем каждому подблоку слева и справа присоединяется по одному биту, в качестве которых берутся ближайшие биты соседних подблоков (для первого подблока соседним слева считается восьмой подблок, а для восьмого подблока соседним справа считается первый подблок).

Значение $\mathcal{E}(R)$ складывается побитно по модулю 2 с раундовым подключом k, результат представляется в виде восьми 6-битовых подблоков B_j:

$$E(\mathrm{R}) \oplus k = B_1B_2B_3B_4B_5B_6B_7B_8.$$

Функция S ″сжимает″ каждый 6-битовый подблок B_j, заменяя его на 4-битовый подблок $S_j(B_j)$, $j = 1, 2,\ldots, 8$. Подстановки замены, называемые -блоками, заданы табл. 4. Каждый из блоков S_j состоит из 4 строк и 16 столбцов, занумерованных соответственно как 0, 1, 2, 3, и 0, 1, …, 15.

Пусть подблок B_j образован битами b_1, b_2, b_3, b_4, b_5, b_6. Биты b_1 и b_6 образуют число $a = 2b_1 + b_6$ со значением от 0 до 3, а средние 4 бита b_2, b_3, b_4 и b_5 образуют число $d = 8b_2 + 4b_3 + 2b_4 + b_5$ со значением от 0 до 15. В таблице S_i на пересечении -ой строки и d-го столбца находится число m со значением от 0 до 15. 4-битовое представление $B' = b_1'b_2'b_3'b_4'$ числа m даёт выходное значение $S_j(B_j)$. Например, если $B_2 = 110110$, то $a = (10)_2 = 2_{10}$, $d = (1011)_2 = (11)_{10}$ и $B_2' = S_2(B_2) = (0110)_2$.

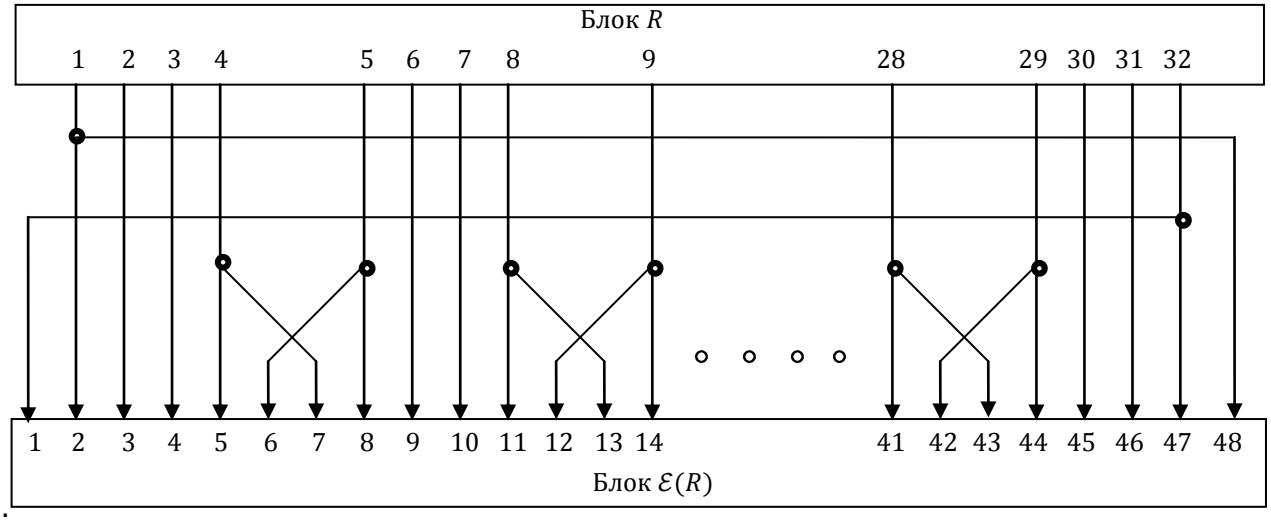
Функция P преобразует 32-битовый блок $B' = B_1'B_2'B_3'B_4'B_5'B_6'B_7'B_8'$, полученный после операции сжатия, в 32-битовый блок $P(B')$ путём перестановки битов в блоке B'. Соответствующая перестановка задаётся таблицей 5: бит 16 перемещается в позицию 1, бит 7 – в позицию 2, …, бит 25 − в позицию 32.

Раундовые подключи k_1, k_2, …, k_{16} формируются на основе 64-битового секретного ключа KS. Сначала ключ KS уменьшается до 56-битового ключа k путём отбрасывания каждого восьмого бита, при этом биты переставляются. Соответствующее преобразование, обозначаемое как PS-1, описывается таблицей 6: биты из позиций 57, 49, 41, …, 20, 12, 4 ключа KS перемещаются в позиции 1, 2, 3, …, 54, 55, 56 ключа k.

После извлечения 56-битового ключа для каждого из 16 раундов генерируются 48-битовые подключи k_i. Эти подключи определяются следующим образом. Сначала ключ k делится на две 28-битовые половины C и D, затем половины циклически сдвигаются влево на один или два бита в зависимости от номера раунда. Величины сдвигов показаны в табл.7. После сдвига выбираются 48 из 56 битов. Соответствующее преобразование, получившее название *перестановка со сжатием* и обозначаемое как PC-2, описывается табл. 8: бит 14 ключа $K = C \parallel D$ помещается в позицию 1 ключа k_i, бит 7 – в позицию 2 и т.д. Циклический процесс получения раундовых подключений иллюстрируется на рис. 4.

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

(*а*)



(*б*)

Рис. 3. *Перестановка с расширением в DES*: (*а*) *Е-блок;* (*б*) *схема перестановки*

Таблица 4

S-блоки DES

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	12	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	12	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Таблица 5

Перестановка P в DES

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Таблица 6

Преобразование PS-1 – выбор ключа в DES

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Таблица 7

Сдвиги ключа в DES *в зависимости от номера раунда*

Номер раунда	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг (бит)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Таблица 8

Преобразование PC-2 – перестановка со сжатием в DES

14	7	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

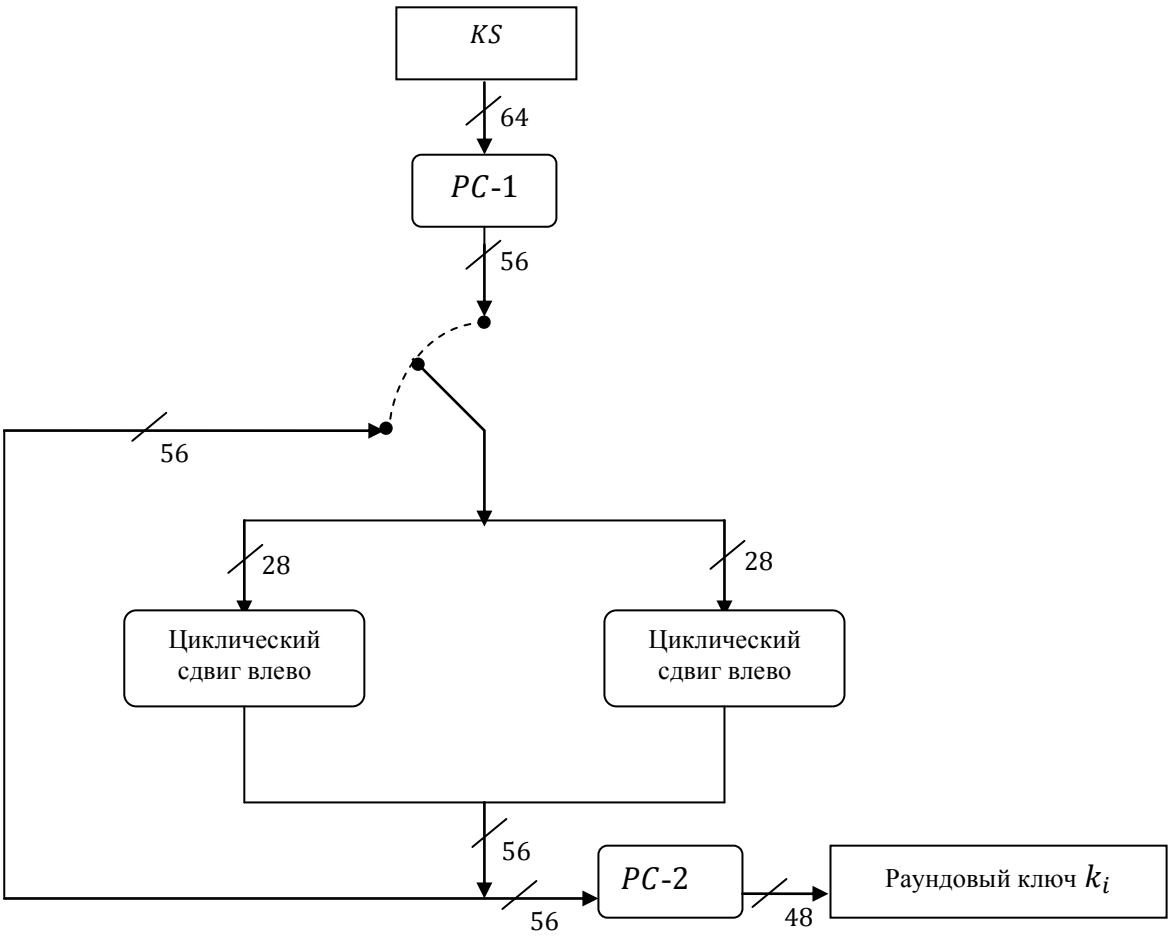


Рис. 4. *Циклический процесс получения раундовых подключей в* DES