

Figure 3.5 Single Round of DES Algorithm

The round key K_i is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits (Table 3.2c). The resulting 48 bits are XORed with K_i . This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted as defined by Table 3.2d.

The role of the S-boxes in the function F is illustrated in Figure 3.6. The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. These transformations are defined in Table 3.3, which is interpreted as follows: The first and last bits of the input to box S_i form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i . The middle four bits select one of the sixteen columns. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example, in S_1 , for input 011001, the row is 01 (row 1) and the column is 1100 (column 12). The value in row 1, column 12 is 9, so the output is 1001.

Each row of an S-box defines a general reversible substitution. Figure 3.1 may be useful in understanding the mapping. The figure shows the substitution for row 0 of box S_1 .

The operation of the S-boxes is worth further comment. Ignore for the moment the contribution of the key (K_i) . If you examine the expansion table, you

of of

30.5c	计编辑器 法基督教 细胞体 實際 化对抗原因 医电子 医二甲基甲基 医二甲基甲基 医二甲基甲基 医二甲基甲基
1. C. S.	
200	14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
Chi.	- PP: 大學學 的复数 學 表 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是 是
707	
Gan .	
S ₁	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
170	
26	
73	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
Œ.	1. 4 1. 14 8 13 6 9 14 15 99 6 6 6 6 6
200	
300 m	
T	
72	- Participal Particip
7. ·	
() .	15^{1} 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13
¥	。

(m)	CACCEND 188 ACCENT TO 188 ACCENT 18 1 (2014) 2014 CO. A.
,C	[5] 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
11.	
	TRACON ROLL SOCIETY OF
Control of	- 1983年1989年1989年1989年1989年1989年1988年1989年1989年1989年1981年1983年1982年1982年1982年1982年1982年1982年1982年1982
V -	
	【2007年11日 11日 11日 11日 11日 11日 11日 11日 11日 11日
	PARTY AND EXPERIENCE AND AND ADDRESS OF A STATE OF A ST
	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 2 15
5	
	T 18 24 TEXT CONTROL OF THE CONTROL
•	
	I STATE OF THE STA
	13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$
--

2 + 12 + 4 + 1 = 7 + 10 + 11 + 6 + 8 + 5 + 3 + 15 + 13 + 0 + 14 + 9
$\begin{bmatrix} 14 & 11 & 2 & 12 & 4 & 7 & 13 & 1 & 5 & 0 & 15 & 10 & 3 & 9 & 8 & 6 \end{bmatrix}$
4 2 1 1 10 13 7 8 15 9 12 5 6 3 0 14
$\begin{bmatrix} 11 & 8 & 12 & 7 & 1 & 14 & 2 & 13 & 6 & 15 & 0 & 9 & 10 & 4 & 5 & 3 \end{bmatrix}$
Part I Provide the Control of the Co
Programme Visit and Control of the C

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 1 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6 4 3 2 12 9 5 15 10 41 14 1 7 6 0 9
	4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

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 6 6 11
----------------	---

Table 3.2 Permutation Tables for DES

(a) Initial Permutation (IP)

		(42)			Section of the Sens		att de day
58	50	42	34	⊤26	18	10	2
	52	44	36	28	20	12	4
60 62	54	46	38	30	22	14	6
25.7	t and	48	40	32	24.	16	8
64.	56	41	33	25	. 17	9	1
57	49	43	35	27	19	. 11	7 in 3
59	51	阿斯斯斯斯斯	37	- 29	21	13	5
61	53	45	39	31	23	15	7
63	- 55	47	29	***	<u> </u>	多类学家 零	<u> </u>

(b) Inverse Initial Permutation (IP^{-1})

(~)		San Share But	Jack and September 1992	na Than Sell Street		32
40 8 8	18	16	56	24	64	
	17	15	55	23	63	31
1 27	46	14	54	22	62.	30
20	45	13	53	21	61	- 29
F-7"	44	12	52	△20	60	28
1.79	43	11	51	19	59 -	27
200	42	10	50	18	58	26
77	41	9	49	- 17	57	25
33 1	HT.	A		媒體演 澳和企	alcordo esta con sta	731 1 NRS1 # 112

(c) Expansion Permutation (E)

27	44	2	3 .	4	
75.4		6	7	- 8	
4			11	12	1
- 8	9	10		16	1
12	13	14	. 15	PER DESIGNATION OF THE PER PER PER PER PER PER PER PER PER PE	4.0
16	17	. 18	19	20	2
20	21	22	23	24	2
24	25	26	27	28	2
	20	30	31	32	
I 28 ·	4.7		S. P. As Ex	類。多層的概念	A

(d) Permutation Function (P)

(4) 2	20,000,000
100 Later and the Control of the Con	
· · · · · · · · · · · · · · · · · · ·	70
16 7 20 21 29 12	40
1 16 20 24	
1.0	21
$\frac{16}{3}$ $\frac{15}{15}$ $\frac{26}{73}$ $\frac{5}{26}$ $\frac{18}{5}$	
1 10 42 49	
200	7
2. 50 54" 14 32 ² .	
1 2 8 44	
	Δ ∠ ∠ Δ
10 40 6 22	
1 19 15	Pull Section Section Committee Commi
是他们的是一个人,我们就是一个人的,我们就是一个人的。 第一个人的,我们就是一个人的,我们就是一个人的,我们就是一个人的。	

labeled L (left) and R (right). As in any classic Feistel cipher, the overall processing a each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \times F(R_{i-1}, K_i)$$

Table 3.4 DES Key Schedule Calculation

4

(a) Input Key

	- Area of Secondario	AND DESCRIPTION OF THE OWNER, WHEN THE OWNER,	AND DESCRIPTION	100	
3 9 3	4	5	6	7	- 8
1 2 3					16
6 10 11.	12	. 13	14	. 15	-
			22	23	24
17 18 19	20	21	- 10 to		
25 26 27	28	29	30	31	32
25 26 27	20				40
33 34 35	36	* 37	38	. 39	. TV
34			46	47	48
41 42 43	44	45			
	52	53	54	- 55	56
49 50 51	- PE			100	64
58 59:	60	61	62 ^	63	04
57 58 59.				100 to	

(b) Permuted Choice One (PC-1)

(A STATE OF THE STA		an are districted that		* X (1) (1)	
57	49	41	33	25	17	- 9
			42		26	18
±1**	58	50	42	34		
and the fig.	2	49	51	43	35	27.
10.	1		200	Alternative to		92
19	41	3	60	52	44	36
		47	39	31	23	15
63	55	(:		a line		here is
	62	54	46	38	30	22
	100			45	37	29
14	- 6	61	53	*3		- V. V.
41	13	- 5	28	20	. 12	4
Z1						ALTO ALTO A

(c) Permuted Choice Two (PC-2)

(6)		
	11 24 11	5 3 28
14	24 10 23	19 12 4
A CONTRACTOR OF THE SECOND		20 13 2
		55 30 40
	31 37 47	49 39 56
51 45	33 48 4 4	
34 53	46 42 50	36 29 32
The second second second	(C)	

(d) Schedule of Left Shifts

	16 1	
the distribution of 12 3 4 5 6 7 8 9 10 11 12 13 14 15		
Round number 1 2 3 4 5 6 7 8 9 10 11 12 2 2 2		
Round number 1 2 3 4 5 9 1 5 7 7 2 2 2 2		
Riscretated 1 1 2 2 2 2 2 1 2 2 2 2 2 2 2 2 2 2 2	27.7	
Round number 1 2 3 4 5 6 7 8 9 10 11 2 2 2 2 2 2 8 1 2 2 2 2 2 2 2 2 8 1 2 2 2 2	-<4	٠

DES Decryption

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.

The Avalanche Effect

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in