



One
Round
of
DES

DES Expansion Permutation

□ Input 32 bits

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

□ Output 48 bits

31	0	1	2	3	4	3	4	5	6	7	8
7	8	9	10	11	12	11	12	13	14	15	16
15	16	17	18	19	20	19	20	21	22	23	24
23	24	25	26	27	28	27	28	29	30	31	0

DES S-box

- ❑ 8 “substitution boxes” or S-boxes
- ❑ Each S-box maps 6 bits to 4 bits
- ❑ S-box number 1

input bits (0,5)

↓

input bits (1,2,3,4)

| 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110
1111

00		1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01		0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10		0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11		1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

DES P-box

□ Input 32 bits

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

□ Output 32 bits

15	6	19	20	28	11	27	16	0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8	18	12	29	5	21	10	3	24

DES Subkey

- 56 bit DES key, numbered 0,1,2,...,55
- Left half key bits, LK

49	42	35	28	21	14	7
0	50	43	36	29	22	15
8	1	51	44	37	30	23
16	9	2	52	45	38	31

- Right half key bits, RK

55	48	41	34	27	20	13
6	54	47	40	33	26	19
12	5	53	46	39	32	25
18	11	4	24	17	10	3

DES Subkey

- For rounds $i=1, 2, \dots, 16$
 - Let $LK = (LK \text{ circular shift left by } r_i)$
 - Let $RK = (RK \text{ circular shift left by } r_i)$
 - Left half of subkey K_i is of LK bits

13 16 10 23 0 4 2 27 14 5 20 9
22 18 11 3 25 7 15 6 26 19 12 1

- Right half of subkey K_i is RK bits

12 23 2 8 18 26 1 11 22 16 4 19
15 20 10 27 5 24 17 13 21 7 0 3

DES Subkey

- For rounds 1, 2, 9 and 16 the shift r_i is 1, and in all other rounds r_i is 2
- Bits 8,17,21,24 of LK omitted each round
- Bits 6,9,14,25 of RK omitted each round
- **Compression permutation** yields 48 bit subkey K_i from 56 bits of LK and RK
- **Key schedule** generates subkey

DES Last Word (Almost)

- ❑ An initial perm P before round 1
- ❑ Halves are swapped after last round
- ❑ A final permutation (inverse of P) is applied to (R_{16}, L_{16}) to yield ciphertext
- ❑ None of these serve any security purpose