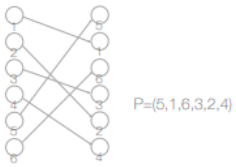
02 - DES

Caratteristiche:

- cifratura simmetrica (secret-key cryptography)
- funziona in blocchi da 64 bit (non è uno stream cipher)
- chiavi a 64 bit, di cui solo 58 sono usati (i rimanenti 8 servono per parity checks)

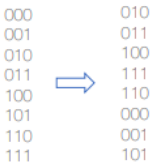
Operazioni

Permutation



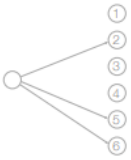
Un bit dell'input determina un bit dell'output

Substitution



Il blocco di bit in input viene convertito in un blocco univoco in output

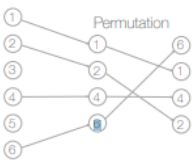
Expansion



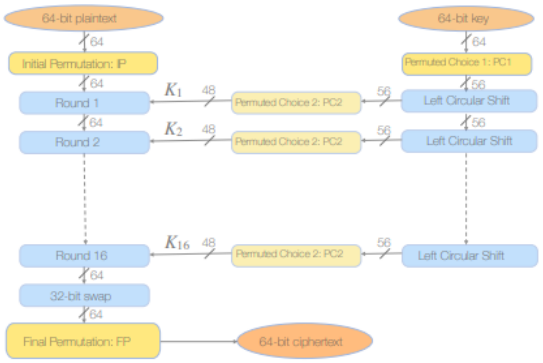
Alcuni bit dell'input vengono ripetuti diverse volte nell'output

Choice (contraction)

Alcuni bit dell'input non appaiono nell'output (vengono ignorati)
Permuted choice:



Generale



IP e FP box

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	23	15	7

IP

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

FP

Sono invertite

PC1 e PC2 box

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

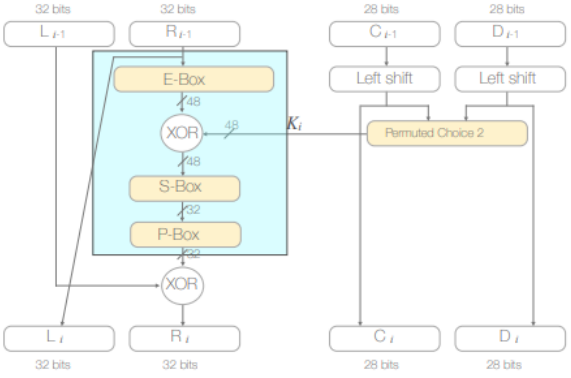
PC1 (64 bits in, 56 bits out)

14	17	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

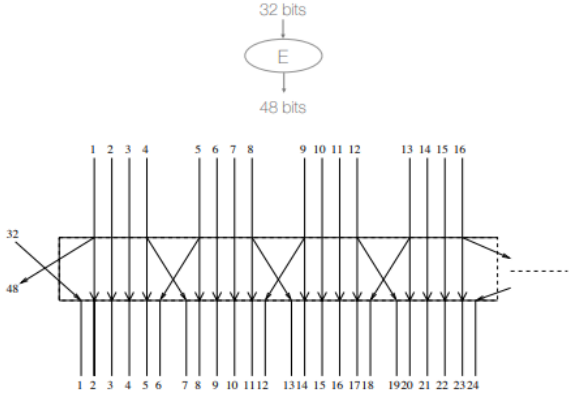
PC2 (56 bits in, 48 bits out)

Alcuni bit sono mancanti (8,16,24, 32, 40, 48, 56, 64) in PC1
Alcuni bit sono mancanti (9,18, 25, 35, 38, 43, 45, 54) in PC2

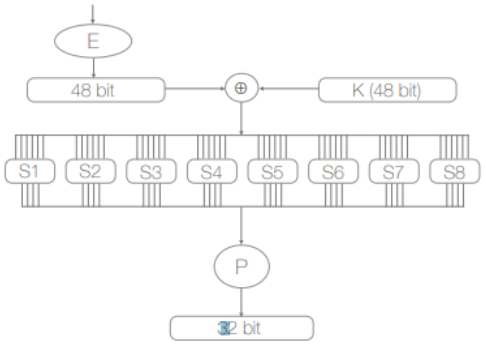
Un round in dettaglio



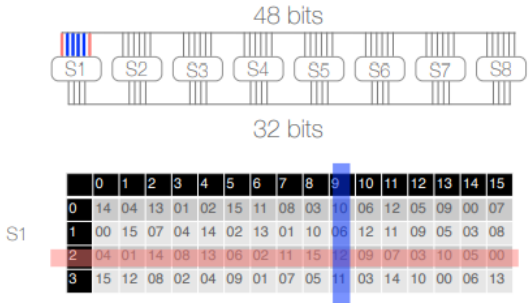
E-box



S-box



I bit 1 e 6 selezionano la riga, i bit 2-5 selezionano la colonna in cui leggere un valore a 4-bit tra une delle 8 possibili mappe



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

P-box

Permutazione di 32-bit

```
16 07 20 21 29 12 28 17
01 15 23 26 05 18 31 10
02 08 24 14 32 27 03 09
19 13 30 06 22 11 04 25
```

Dal 1999 DES è considerata insicura per via della sua chiave troppo corta.

AVG bruteforce:

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years