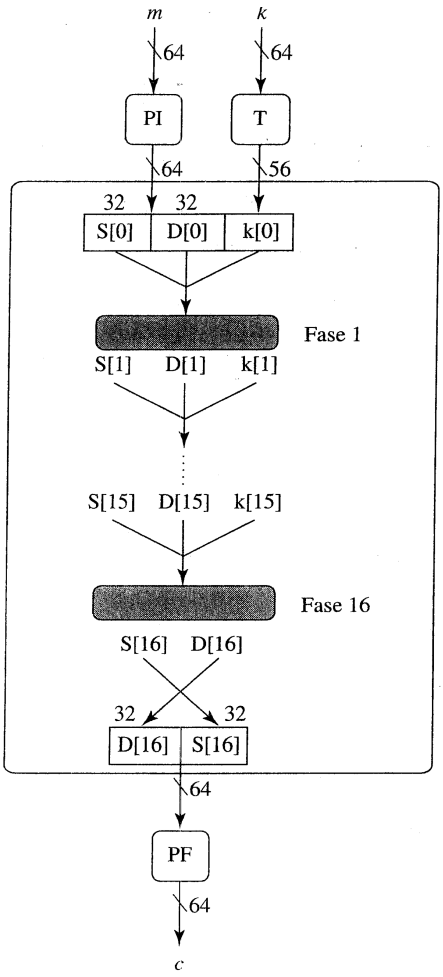


Trasformazione centrale

Struttura del DES

m
blocco del messaggio
c
corrispondente blocco del crittogramma
k
chiave segreta, con i bit di parità

Per ogni i=1,2,...,16

$S[i] = D[i-1]$

$D[i] = S[i-1] \oplus f(D[i-1],k[i-1])$

f : funzione **NON** lineare

Permutazioni

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

Permutazione PI

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

Permutazione PF

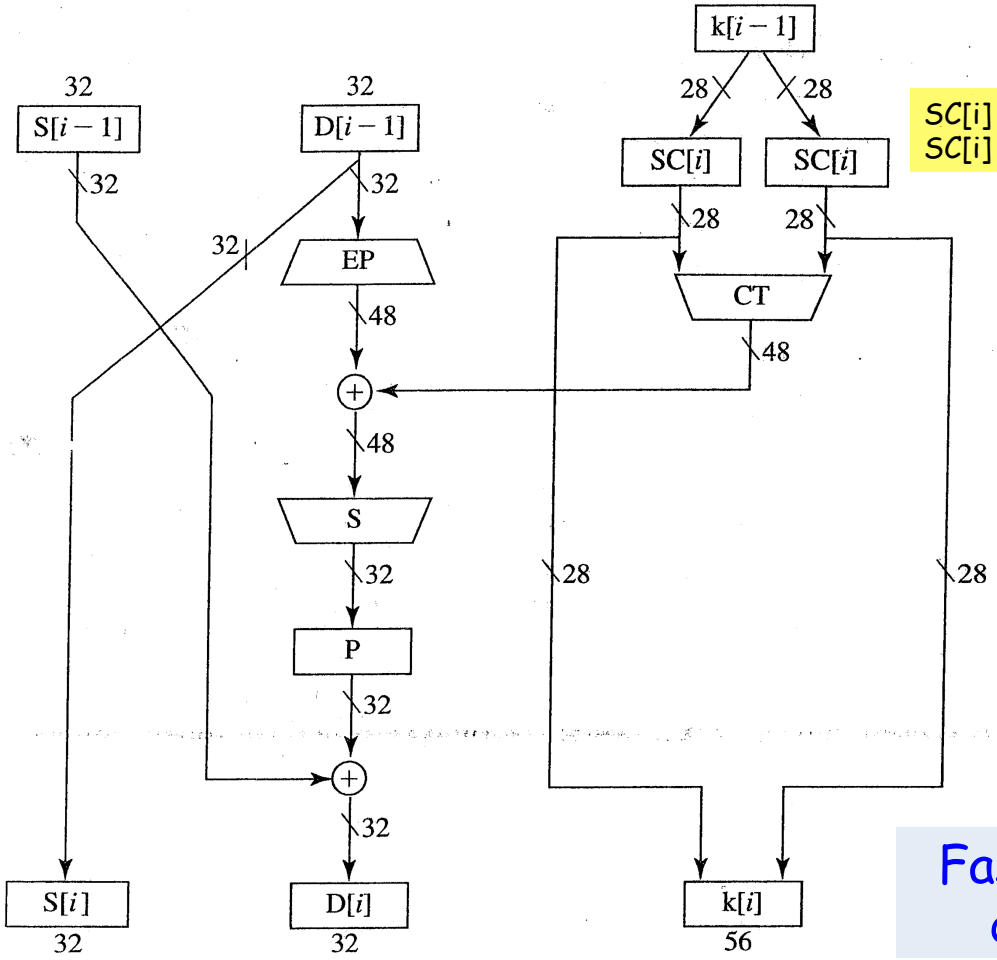
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	52	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Trasposizione T

Le tabelle vanno lette per righe. La permutazione PI riordina i bit del messaggio $m=m_1m_2...m_{64}$ come $m_{58}m_{50}...m_7$. (porta in posizione 40 il bit in posizione 1)

PF è la permutazione inversa di PI, cioè riporta in posizione 1 il bit in posizione 40, etc.

T provvede anche a scartare dalla chiave $k=k_1k_2...k_{64}$ i bit per il controllo di parità k_8, k_{16}, ...,k_{64}, generando una sequenza di 56 bit che costituisce la prima sottochiave k [0].



SC[i] = 1, i = 1, 2, 9, 16
SC[i] = 2, o/w

Fase i-esima del DES

Funzioni CT e EP

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

La funzione CT

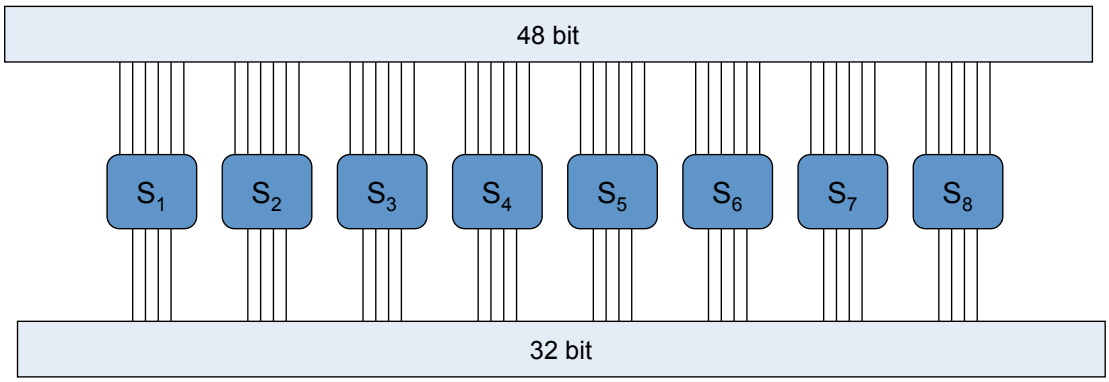
otto bit dell'ingresso (e.g., il bit 09) non sono presenti in uscita.

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

La funzione EP

sedici bit di ingresso sono duplicati (e.g., il bit 32 è copiato nelle posizioni 1 e 47 dell'uscita).

S-box

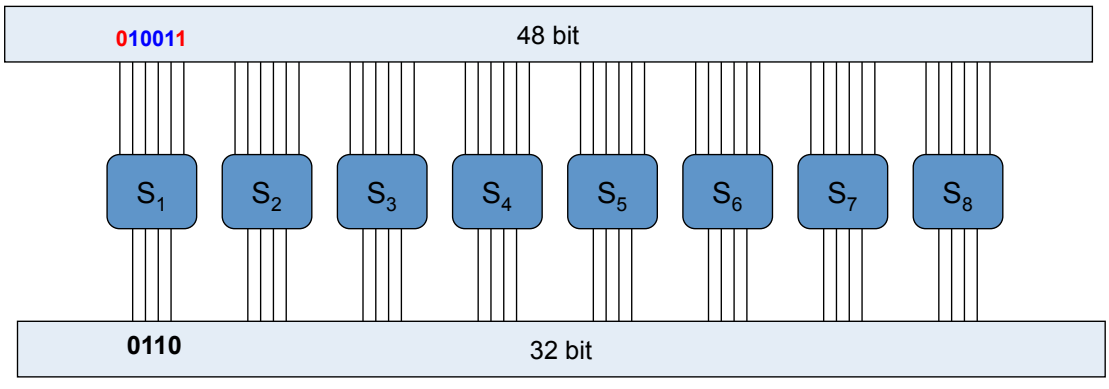


S_1

x \ y	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

Tabella che definisce la sottofunzione S_1.
Le sottofunzioni S_2, S_3, ..., S_8 sono definite in modo simile

S-box



S_1

x \ y	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

Tabella che definisce la sottofunzione S_1.
Le sottofunzioni S_2, S_3, ..., S_8 sono definite in modo simile

Permutazione P

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

Permutazione di 32 bit che genera il blocco finale D[i].

Esercizio

- Siano

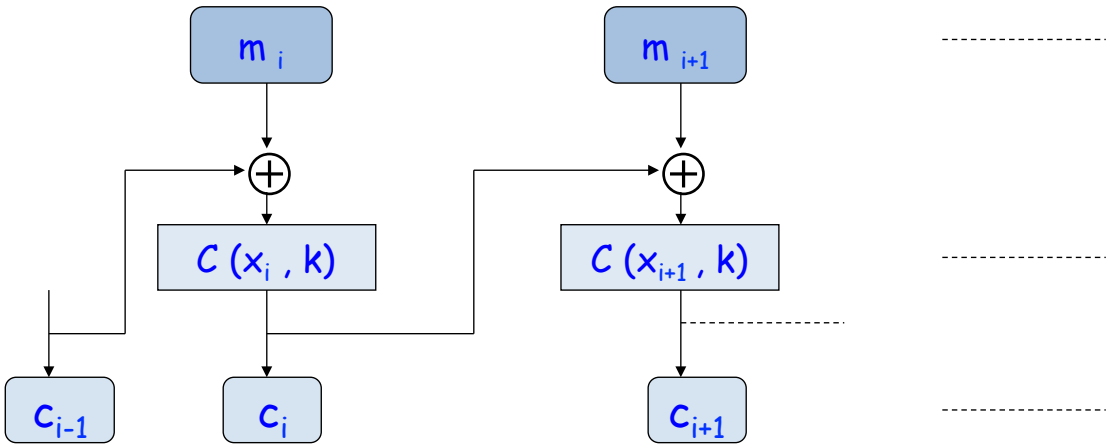
  $c = C_{DES}(m, k)$

  $c^* = C_{DES}(m', k')$

  $c\hat{} = C_{DES}(m, k')$

  dove, m' e k' sono ottenute complementando bit a bit m e k.
- Spiegare se vi è una semplice relazione tra c e c^* e tra c e $c\hat{}$.

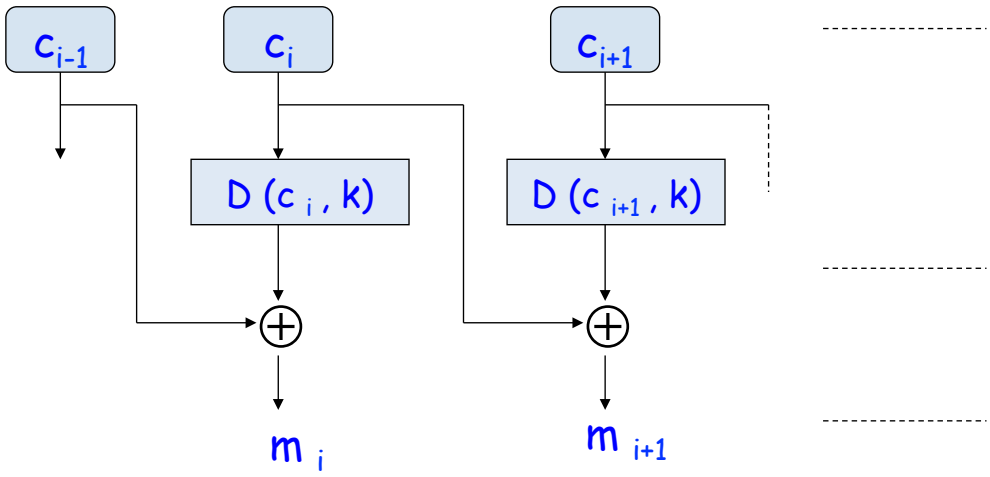
CBC: Cipher Block Chaining



Cifratura

x_i indica il blocco $m_i \oplus c_{i-1}$

CBC: Cipher Block Chaining



Decifrazione

ALTRI CIFRARI A CHIAVE SEGRETA

RC 5 (Ron's Code 5) Ron Rivest

- simile al DES, ne adotta la struttura migliorandone alcune parti
- lascia più libertà all'utente
- blocchi di **64 bit**
- chiave di **c x 32 bit**
- r fasi (valore consigliato: r = 16)
- r e c possono essere scelti a piacere
- usa shift ciclico, XOR, addizione mod 2^{32}
- molto veloce, resiste con successo agli attacchi standard se c e r sono scelti bene
- sicuro e impiegato con una certa frequenza
- SEMPLICITÀ DI REALIZZAZIONE E GRANDE SICUREZZA

IDEA (International Data Encryption Algorithm)

- 1992
- chiave da **128 bit**
- usa shift ciclico, XOR, moltiplicazione mod $(2^{16}+1)$ e addizione mod 2^{16},
- più semplice e più sicuro del DES
- la sicurezza poggia su basi teoriche molto forti
- è rimasto assolutamente inviolato, ma non è diventato il nuovi standard