Cifrari simmetrici per le comunicazioni di massa

Cifrari per le comunicazioni di massa

Offrono **sicurezza computazionale**

- nascondono l'informazione se il crittoanalista ha accesso a risorse computazionali limitate (polinomiali) e se $P \neq NP$

Cifrari per le comunicazioni di massa

Advanced Encryption Standard (AES)

- ➔ Standard per le comunicazioni riservate ma “non classificate”
- ➔ Pubblicamente noto e realizzabile in hardware su computer di ogni tipo
- ➔ Chiavi brevi (qualche decina di caratteri, 128 o 256 bit)
- ➔ Cifrario **simmetrico**, **a blocchi**

  la stessa chiave è usata per cifrare e decifrare

  il messaggio è diviso in blocchi lunghi come la chiave

  la chiave è utilizzata per trasformare un blocco del messaggio in un blocco del crittogramma

Principi di Shannon

La sicurezza è basata su due principi (Claude Shannon)

DIFFUSIONE

il testo in chiaro si deve distribuire su tutto il crittogramma

- ➔ *ogni carattere del crittogramma deve dipendere da tutti i caratteri del blocco di messaggio*

CONFUSIONE

messaggio e chiave sono combinati tra loro in modo complesso per non permettere al crittoanalista di separare le due sequenze tramite l’analisi statistica del crittogramma

- ➔ *la chiave deve essere ben distribuita sul testo cifrato*
- ➔ *ogni bit del crittogramma deve dipendere da tutti i bit della chiave*

Data Encryption Standard (DES)

Cifrario anni ‘70 (prodotto IBM)

Primo cifrario ufficialmente certificato (NIST) per la protezione delle comunicazioni non classificate, fino al 1999

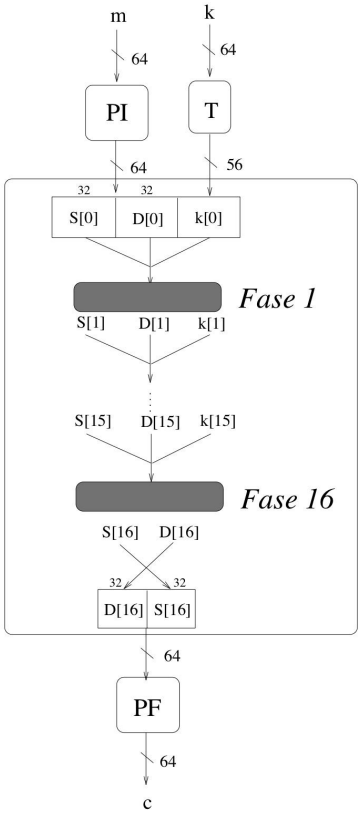
STRUTTURA

- Il messaggio è suddiviso in blocchi, ciascuno cifrato e decifrato indipendentemente dagli altri
- Nel DES ogni blocco contiene 64 bit
- Cifratura e decifrazione procedono attraverso r fasi (o round) in cui si ripetono le stesse operazioni. Nel DES si ha r = 16
- La chiave segreta k è composta di 8 byte. In ciascun byte i primi sette bit sono scelti arbitrariamente e l’ottavo è aggiunto per il controllo di parità

  → chiave di 64 bit di cui 56 arbitrari e 8 di parità

  → dalla chiave k vengono create le r sottochiavi di fase

Data Encryption Standard (DES)



Trasformazione Centrale

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] ⊕ **f** (D[i-1],k[i-1])

f : funzione **NON** lineare

Feistel Network

Data Encryption Standard (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	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

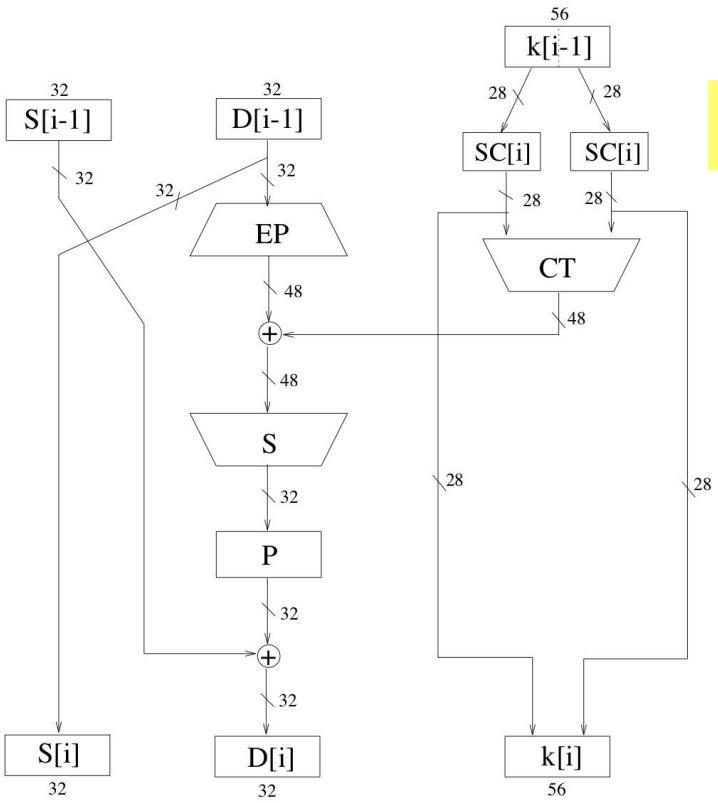
Le tabelle vanno lette per righe

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]

Fase i-esima del DES



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

Blocchi CT ed 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

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

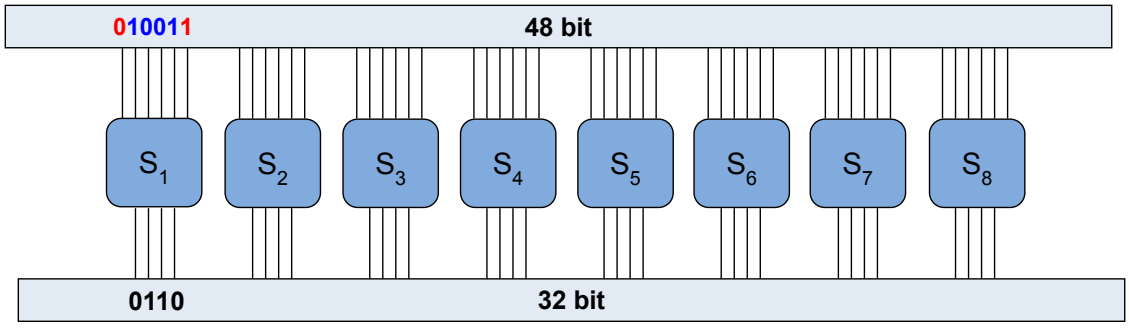
La funzione CT

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

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

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 $c\hat{}$.

DES: sicurezza e attacchi

- Spazio delle chiavi: $\{0,1\}^{56}$
- bit di sicurezza?

  un cifrario ha una sicurezza di b bit se il costo del miglior attacco è di ordine $O(2^b)$ operazioni di decifrazione, i.e., richiede di esplorare uno spazio delle chiavi di cardinalità 2^b
- 56 → 55

  si sfrutta il fatto che $C_{DES}(m,k) = c$ implica $C_{DES}(m',k')=c'$

  k e il suo complemento k' si controllano "simultaneamente"
- crittoanalisi differenziale (1990)

  costa come un attacco esauriente sulle chiavi con 16 fasi
- crittoanalisi lineare (1993)

  meno costoso di un attacco esauriente
- architetture costruite appositamente per attaccare il cifrario

Alternative al DES: cifratura multipla

Idea: concatenare più copie del DES, con chiavi diverse

Date due arbitrarie chiavi k_1 e k_2

$$C_{DES}(C_{DES}(m, k_1), k_2) \neq C_{DES}(m, k_3)$$

per qualsiasi messaggio m e qualsiasi chiave k_3

Due chiavi di 56 bit → una chiave di ~~112~~ **57** bit

Attacchi "meet in the middle"

$c = C_{DES}(C_{DES}(m, k_1), k_2)$ $\quad D_{DES}(c, k_2) = C_{DES}(m, k_1)$

Data una coppia <m,c>

1. per ogni k_1, si calcola e si salva $C_{DES}(m, k_1)$ in una tabella
2. per ogni k_2, si calcola $D_{DES}(c, k_2)$ e si cerca nella tabella

Costo: $O(2^b + 2^b)$ op. = $O(2^{b+1})$ op., b = bit della chiave

doppia enumerazione delle di chiavi → 2^{57}