DES

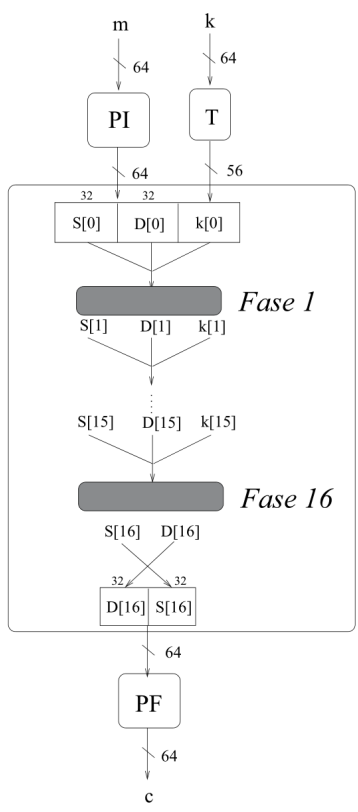
Data Encryption Standard: cifrario simmetrico a blocchi di 64 bit.

Struttura:

- cifratura e decifrazione in $r = 16$ fasi (round) in cui si ripetono le stesse operazioni;
- chiave k di $b = 8$ byte, ma in ogni byte l'ottavo bit è di parità (solo 56 bit casuali);
- da k vengono estratte 16 sottochiavi $k[0], \ldots, k[15]$, una per ogni fase;
- ciascun blocco viene diviso nella metà sinistra $S[0]$ e destra $D[0]$ da 32 bit;
- alla fase i:

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

  dove f è una funzione non lineare ($f(a \oplus b) \neq f(a) \oplus f(b)$);
- per decifrare si ripete il processo con le chiavi in ordine inverso.

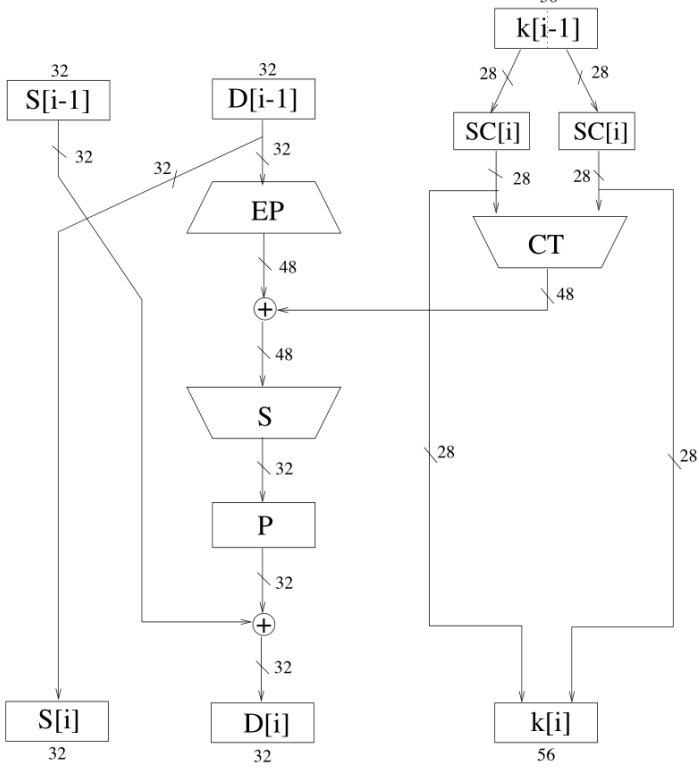


PI permutazione iniziale di m;

T trasposizione, elimina i bit di parità di k e permuta i restanti;

PF permutazione finale di m, inversa di PI.

PI e PF sono escluse in molte implementazioni, non sono fondamentali per la sicurezza del cifrario.



SC shift ciclico verso sinistra di 1 o 2 posizioni (in base alla fase) su ciascuna metà di $k[i-1]$;

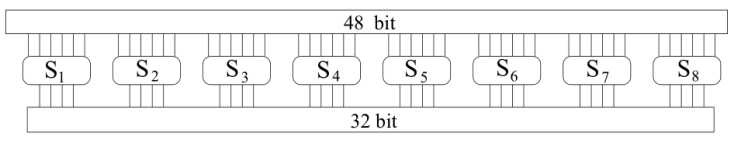
CT compressione e trasposizione dei risultati degli SC, che viene permutato con l'esclusione di 8 bit (da 56 a 48);

chiave successiva ottenuta ricomponendo i risultati degli SC;

EP espansione e permutazione di $D[i-1]$ da 32 a 48 bit, duplicandone 16;

S-box trasformazione non lineare da 48 a 32 bit, composta da 8 sottofunzioni definite tramite tabelle (no forma algebrica). Ciascuna prende 6 bit e ne restituisce 4. Con il primo e ultimo bit in input si seleziona la riga, con i 4 interni la colonna. Ogni riga è una permutazione dei primi 16 interi. Tutti i bit di $D[i-1]$ influenzano il risultato, altrimenti non sarebbe invertibile;

P permutazione.



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

Le operazioni eseguite garantiscono che ogni bit del crittogramma dipende da tutti i bit della chiave e del messaggio, quindi sono rispettati i principi di diffusione e confusione.

La generazione delle sottochiavi è tale che ogni bit di k viene usato in circa 14 delle 16 fasi.