Lecture: concetti base di crittografia

Riccardo Torre

29 novembre 2025

1 Lecture 13/05/2025

Le reti di sostituzione-permutazione di Calude Shannon Nel 1949 Claude Shannon introdusse l'idea di reti di permutazione-sostituzione (S-P) che sono basate su due operazioni crittografiche primitive ossia le sostituzioni con le S-box che sostituiscono i simboli di input confondendo il contenuto del messaggio e le permutazioni con el P-box che permettono di diffondere i bit tra le S-box dissipando la struttura statistica del contenuto del messaggio. I cifrari che hanno questa struttura si dicono **cifrari a prodotto**.

Feistel Nel 1973 Feistel crea il cifrario omonimo che si basa sull'idea di rete S-P proposta da Shannon. Ad ogni **round** si prende un blocco, lo si divide a metà. La parte di destra viene passata ad una funzione di round (funzione di Feistel) che prende in input oltre alla parte destra una chiave . La parte di sinistra viene messa in XOR con il risultato della funzione di Feistel. Successivamente la parte sinistra e destra vengono scambiate. Vengono fatti 16 round. Dopo il 16 esimo round (17°esimo passaggio) vengono scambiate le due metà. Se nell'operazione di cifratura vengono usate le chiavi nell'ordine $\mathrm{K}_1, \ldots, \mathrm{K}_{16}$, e al 17°esimo passaggio viene fatto lo scambio delle due metà del blocco, nella decifratura i passaggi devono essere svolti nell'ordine inverso, ovvero, si scambiano le due metà, si applicano i round usando le chiavi nell'ordine $\mathrm{K}_{16}, \ldots, \mathrm{K}_1$.

DES È l'implementazione del cifrario di Feistel, Data Encryption Standard. È stato attaccato per il rapido avanzamento tecnologico, non perché non fosse sicuro. Si decise di utilizzare una chiave da 56 bit perché la computazione con chiavi più lunghe per la tecnologia dell'epoca era abbastanza onerosa. Nel 1999 DES è stato attaccato con un brute force attack. Ci sono dei sospetti che il NSA avesse modificato le S-box introducendo una backdoor.

DDES È suscettibile ad attacco Meet-In-the-Middle. È un attacco **chosen plaintext**:

$$X = E_{Ki}(P) \xrightarrow{M} E_{Kj}(M) = C = E_{Kj}(E_{Ki}(P)) \qquad \text{con } \begin{cases} 0 \leq i \leq 2^{56} - 1 \\ 0 \leq j \leq 2^{56} - 1 \end{cases}$$

1. Scegli un plaintext P, e applica l'algoritmo DDES per ottenere il relativo ciphertext C. Crea una tabella ordinata per X.
2. Decifra C con tutte le 2^{56} possibili chiavi k_j e verifica se $X = E_{Ki}(P) = D_{Kj}(C)$ (condizione Meet in the Middle).
3. Ciascuna corrispondenza della suddetta condizione è una soluzione candidata. Usare la stessa coppia di chiavi $(\mathrm{K}_i, \mathrm{K}_j)$ con altre coppie (P, C).

L'attacco ha una complessità spaziale e temporale di $O(2^{56})$. Quindi la chiave non ha una dimensione doppia di 112 bit.