Attacchi al DES

Chiavi deboli

Ci sono 64 chiavi che compromettono la sicurezza, tra cui quella con tutti 1, tutti 0, o 28 1 seguiti da 28 0 o viceversa.

Forza bruta

Spazio delle chiavi $\{0,1\}^{56}$, forzato con architetture ad-hoc o parallele.

Attacco chosen plain text

Conoscendo due coppie (m, c_1) e $(\overline{m}, c_2)$, si possono ridurre i bit di sicurezza da 56 a 55 sfruttando il fatto che:

$$C(m,k) = \overline{C(\overline{m}, \overline{k})}.$$

Infatti, le uniche operazioni influenzate dal complemento sono XOR e S-box: il primo XOR è tra due valori complementati, quindi il suo risultato è uguale a quello originale, ed è usato come input per la S-box. Il secondo è tra un valore complementato e il risultato della permutazione dell'output della S-box, quindi otteniamo il complemento dell'uscita originale della fase (complementando solo la chiave non c'è relazione significativa perché la S-box non è lineare e il suo input viene complementato).

Per ogni chiave k:

- se $C(m,k) = c_1$, probabilmente k è la chiave;
- se $C(m,k) = \overline{c}_2$ allora probabilmente è $\overline{k}$;
- altrimenti posso escludere sia k che $\overline{k}$ con la stessa operazione di cifratura.

Crittoanalisi differenziale

Chosen plain text, richiede 2^{47} coppie (m,k) con m scelto dal crittoanalista. Studia come variazioni nel messaggio si ripercuotono nei crittogrammi. Ha costo circa $O(2^{55.1})$, quindi non ancora forzato (forza bruta più efficiente), per via del numero di fasi (probabilmente i progettisti conoscevano la crittoanalisi differenziale).

Crittoanalisi lineare

Known plain text, richiede 2^{43} coppie. Permette di stimare alcuni bit della chiave approssimando la funzione di cifratura con una funzione lineare. Meno costoso del brute force.