Varianti al DES

Sottochiavi indipendenti

Sottochiavi non estratte dalla stessa chiave: $48 \cdot 16 = 768$ bit, ma solo 61 di sicurezza con crittoanalisi differenziale.

Cifratura multipla

Possibile perché non è lineare:

$$\forall k_1, k_2, k_3, m \; . \quad C(C(m, k_1), k_2) \neq C(m, k_3)$$

$56 \cdot 2 = 112$ bit di chiave, ma solo 57 bit di sicurezza con attacco *meet-in-the-middle*: data una coppia m, c,

- per ogni k_1 si memorizza $C(m, k_1)$ in una tabella;
- per ogni k_2 si cerca nella tabella $D(c, k_2)$, se è presente alla posizione k_1 allora (k_1, k_2) è probabilmente la chiave.

Costo: $O(2^{56} + 2^{56}) = O(2^{57})$.