(2.5) Conclusion : sécurité du DES.

- Attaque Exhaustive :

La faiblesse du DES est son petit espace de clés réduite à 56 b

Principe Attaque Exhaustive

Entrée : Au moins deux paires (clair, chiffré) = (x, y).

Sortie : k, telle que $y = DES_k(x)$

Attaque : tester tous les 2^{56} clés possibles jusqu'à :

$$DES^{-1}_{k_i}(y) = x, \quad i = 0, 1, \ldots, 2^{56}-1.$$

1998, Deep-Crack en 56 heures.
($ 250,000). Société Electronic Frontier Foundation.

- Attaque Analytique :

{ cryptanalyse analytique // linéaire } : les S-box résistent.

Départ # paires (clair, chiffré) $\simeq 2^{47}$.

- Amélioration 3-DES.

§ AES : **Projets d'Echanges**