

## §2. D.E.S (Data Encryption standard).

2.9

Le DES est l'un des cryptosystèmes les plus utilisés par.

le B-cryptage (par blocs), malgré son remplacement par.

l'AES. Sa étude permet de comprendre la conception des

B-cryptosystèmes et les principes sous-jacents (ex.

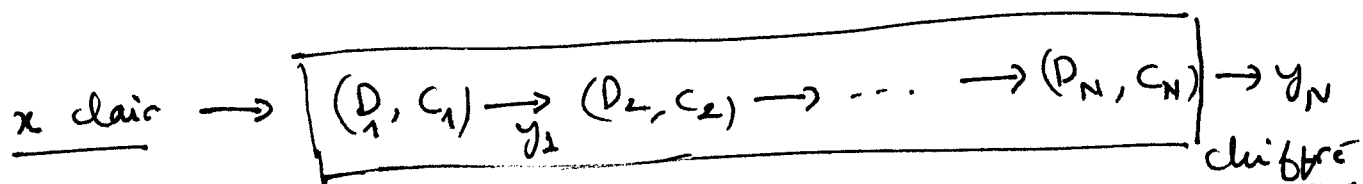
Confusion et diffusion de Shannon). Il existe des améliorations

tel le 3-DES.

C • Confusion : opération cryptographique où la relation entre la clé et le chiffre est obscur.

D • Diffusion : opération cryptographique où l'influence d'un symbole du clair est étalée sur plusieurs symboles du chiffre (dans le but de cacher les propriétés statistiques du clair).

Pour renforcer cette idée, on concatène les opérations primitives en utilisant un chiffrement produit :



qui est la structure du DES (et aussi presque des AES).