§2. D.E.S (Data Encryptin standard).

Le DES est l'un des cryptosystèmes les plus utilisés pour le B-cryptage (par blocs), malgré son remplacement par l'AES. Son étude permet de comprendre la conceptin des B-cryptosystèmes et les principes sous-jacents (ex. confusin et diffusin de Shannon). Il existe des améliorations tel le 3.DES.

C • Confusin : opératin cryptographique où la relatin entre la clé et le chiffré est obscure.

D • Diffusin : opératin cryptographique où l'influence d'un symbole du clair est étalé sur plusieurs symboles du chiffré (dans le but de cacher les propriétés statistiques du clair).

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

$$x \text{ clair} \longrightarrow \boxed{(P_1, C_1) \xrightarrow[y_1]{} (P_2, C_2) \longrightarrow \cdots \longrightarrow (P_N, C_N)} \rightarrow y_N \text{ chiffré}$$

qui est la structure du DES (et aussi presque de l'AES).