Confidentialité

Définition

Seules les entitées authorisées peuvent accèder à l'information

Cryptographie

Classification

Ancienne

- Substitution
  - Mono-alphabétique
  - Poly-alphabétique

  Changer un caractère par un autre dans le même alphabet ou dans un autre
- Transposition

  Changement de position des caractères suivant un ordre ou non pour avoir un nouveau message ayant ou non un sens

Modèrne

- Symétrique
  1. Une seule et même clé pour le chiffrement et le déchiffrement.
  2. Rapide
  3. Si N est le nbr d'entités alors N(N-1)/2 est le nbr de clé nécessaire dans un groupe
     - Plus le nbr augment plus ça devient difficile à gérer
- Asymétrique
  1. Deux clés: Une pour le chiffrement (clé publique) et l'autre pour le déchiffrement (clé privée aussi dite secrète)
  2. Gourmand en termes de temps car basé sur des opération mathématiques (factorisation des grands nombres par exp)
  3. Si N est le nbr d'entités alors N est le nbr de paires de clé nécessaire dans un groupe
     - Pas de problème de distibution ni de gestion des clés.
- Hybride