Introduction à la cryptographie

...

Pourquoi faire?

- Confidentialité
- Authentification
- Intégrité

Confidentialité

- Chiffrement des données
- Beaucoup d'étude (surtout mathématique)
- Évolutif dans le temps
  - Un algorithme peut être suffisant à un instant T...
  - ... et insuffisant à l'instant T+1
  - Selon la puissance de calcul

Fonction de Hashage

- Opération mathématique irréversible (injective, non bijective)
  - md5(“toto”) => f71dbe52628a3f83a77ab494817525c6
  - f(f71dbe52628a3f83a77ab494817525c6) => “toto”
    - f n'existe pas
- Permet de calculer l'empreinte d’une donnée
  - Comme par exemple des mot de passe

Fonction de hashage

- Cas du mot de passe
  - On ne stocke jamais le mot de passe en claire
    - Pour éviter les compromissions
    - On stocke une empreinte du mot de passe
    - A chaque login on calcule l'empreinte que l'on compare à celle stocké
    - Si un utilisateur malveillant récupère l'empreinte il ne pourra rien en faire (non bijective !!!)

Fonction de hashage

- Il existe des attaques sur les fonctions de hashage
  - Ferme de calcul stockant la valeure hashé et représentant une vue partielle de la fonction
    - Il faut donc salé les mot de passe
      - ex : md5(username + password)
  - Attaque par collision
    - Essayer de trouver plusieurs x générant la même emprunte

Fonction de hashage

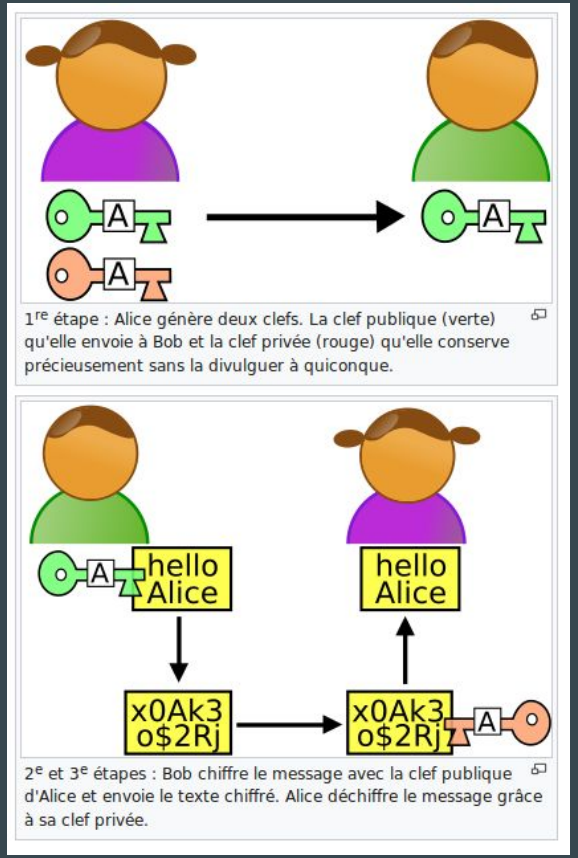
- Etat des algorithmes
  - MD5 -> mort (de nombreuse collision)
  - SHA1 -> déconseillé (Quelque collision cf. Google)
  - SHA2 -> OK (SHA256, SHA512 etc...)

Chiffrement

- Asymétrique
- Symétrique

Asymétrique

- Aucun secret partagé !!!
- RSA
  - Ronald Rivest, Adi Shamir, Leonard Adelman
- Algorithme le plus utilisé sur internet
- Base sur la factorisation de nombre premier
  - Actuellement il n'existe qu'un seul moyen : brute forcer !!!
- Apporte un niveau de sécurité élevé ...
- ... Par contre très lents...

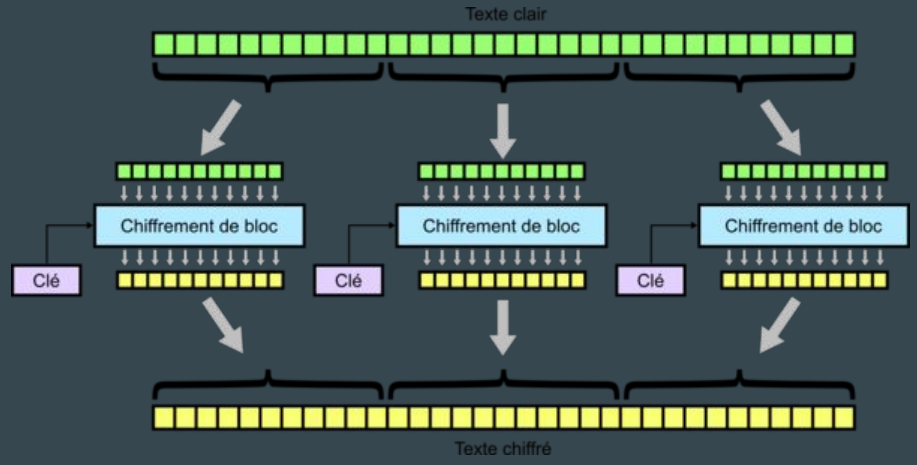


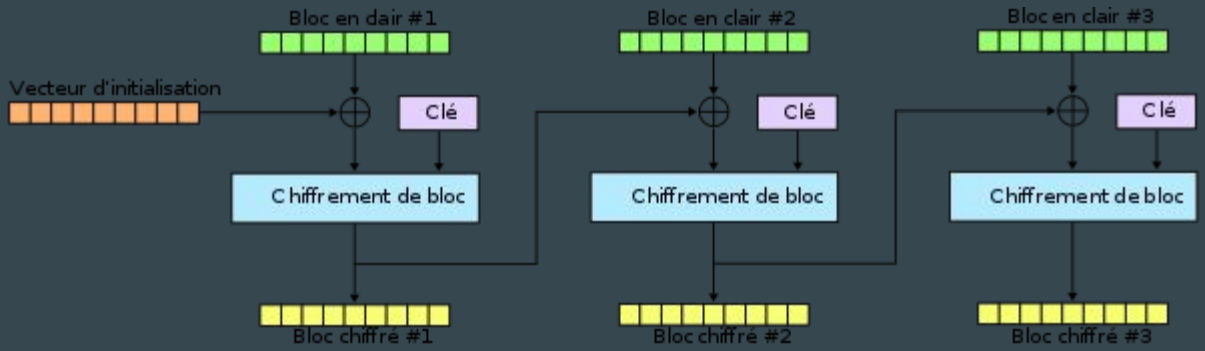
Symétrique

- Secret partagé !!!
- Très performant
- Énormément d’algorithme
  - RC4, DES, 3DES, AES, Blowfish etc...
- Deux mode de chiffrement:
  - Chiffrement par flux (octet par octet)
  - Chiffrement par bloc

Symétrique

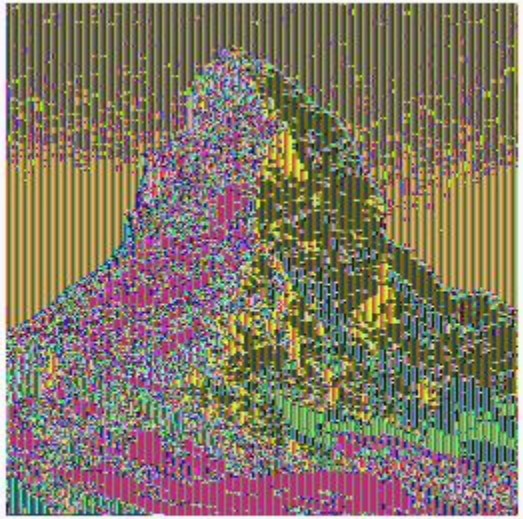
- Chiffrement par bloc (type AES)
  - Plusieur mode d'opération
    - ECB
    - CBC



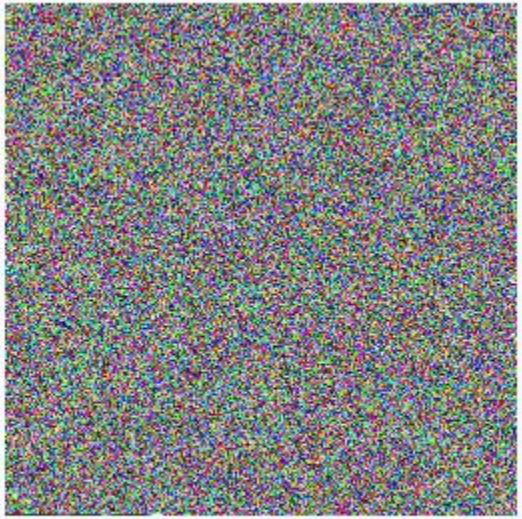


Symétrique

Image originale



Chiffrement en mode ECB



Chiffrement avec un mode sûr (autre que ECB)

Chiffrement Hybride (TLS)

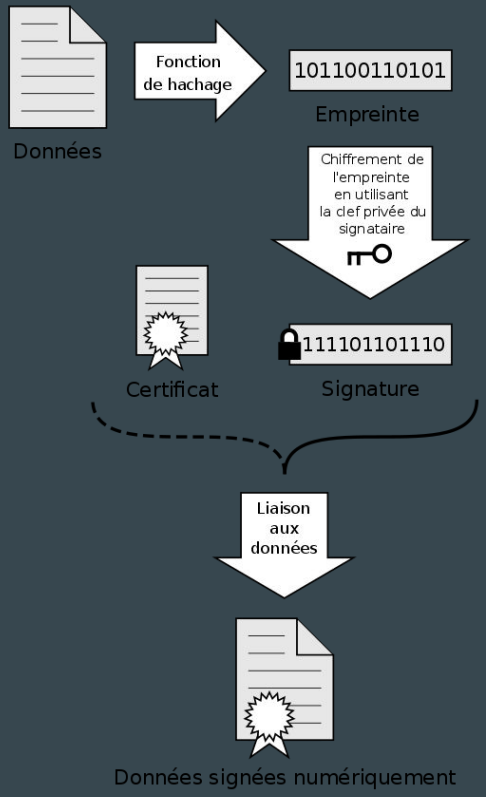
- Utiliser le meilleur des deux mondes
- Le client génère un secret partagé qui va être échangés au moyen d'un chiffrement asymétrique
- Une fois l'échange fait, on poursuit sur un chiffrement symétrique type AES

Authentification

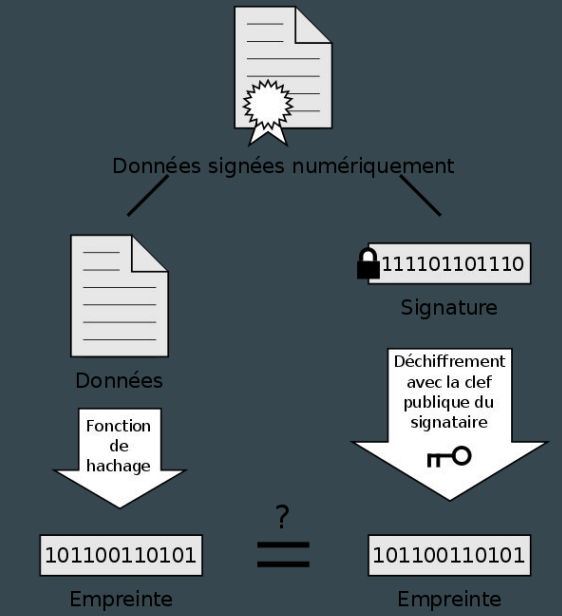
- Deuxième partie fondamentale de la cryptographie
- Basé sur un tiers de confiance
- Basé sur une combinaison d'empreinte signé asymétriquement

Authentification

Signature



Vérification



Si les empreintes sont identiques, la signature est valide