

Sécurisation des communications : La cryptologie

La **cryptologie**, étymologiquement est la "science du secret"

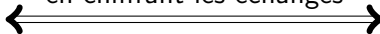
Elle englobe :

- la **cryptographie** : c'est la science du chiffrement et du déchiffrement
- la **cryptanalyse** : c'est l'analyse de la cryptographie. On utilise alors le verbe décrypter.
- ◇ La cryptographie s'intéresse à la protection des données.
- ◇ la cryptanalyse a pour objectif de corrompre les propriétés apportées par la cryptographie. décrypter. On parle couramment d'attaque sur un cryptosystème.

Sécurisation des communications



Alice et Bob communiquent
en chiffrant les échanges



Deux méthodes :

- Le chiffrement symétrique.
- Le chiffrement asymétrique.

Chiffrement symétrique



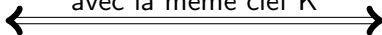
Alice et Bob communiquent
en chiffrant les échanges
avec la même clef K



Chiffrement symétrique



Alice et Bob communiquent
en chiffrant les échanges
avec la même clef K



- Le chiffrement de César (Décalage dans l'alphabet)
- Le masque jetable (Utilisation de XOR)
- Vigenère (Chiffrement par bloc)
- DES (chiffrement moderne obsolète)
- AES (chiffrement symétrique le plus utilisé)

Principe du chiffrement asymétrique

Le chiffrement asymétrique repose sur le principe qu'une personne génère deux clefs qui sont liées entre elles.

- Cette relation doit être difficile à retrouver du point de vue calculatoire.
- Une des clefs est secrète, c'est-à-dire connue de la seule personne qui veut déchiffrer le message.
- L'autre clef est publique et peut être utilisée par n'importe qui.

Principe du chiffrement asymétrique

L'analogie classique pour se représenter le chiffrement asymétrique est le principe de la boîte aux lettres. La clef publique est une boîte aux lettres et n'importe qui peut y déposer un message. Cette boîte ne peut être ouverte que par la clef "secrète" détenue uniquement par le possesseur de la boîte aux lettres.



Clef Publique



Clef Privé

Chiffrement Asymétrique

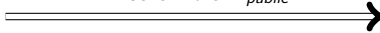


Alice génère un couple
de clef asymétrique
(K_{prive} , K_{public})

Chiffrement Asymétrique



Alice envoie K_{public}



Chiffrement Asymétrique



Bob chiffre le message

M_{clair} avec K_{public} :

$$M_{chiffre} = F_{chiffre}(M_{clair}, K_{public})$$

Chiffrement Asymétrique



Bob envoie $M_{chiffre}$



Chiffrement Asymétrique



Alice déchiffre avec $K_{\text{privé}}$

$$M_{\text{clair}} = F_{\text{dechiffre}}(M_{\text{chiffre}}, K_{\text{privé}})$$

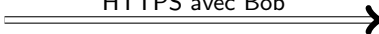
Le chiffrement asymétrique est très gourmand en calcul.
On l'utilise surtout pour les échanges de clés.
Il est très peu utilisé pour les échanges standards.

Protocole HTTPS

Les deux méthodes de chiffrement (symétrique et asymétriques) sont utilisées lorsqu'un navigateur demande une page web avec le protocole HTTPS. Dans le schéma ci-dessous, on a représenté les échanges de communications entre un client (A) et un serveur (B) avec le protocole HTTPS.



Alice Demande une connexion
HTTPS avec Bob



Bob génère un couple
de clef asymétrique
(K_{prive} , K_{public})

Protocole HTTPS



Bob envoie la clef K_{public}



Alice génère une
clef **symétrique** K_{sym}

et la chiffre avec K_{public}

$$K_{sym}^{chiffre} = F_{chiffre}(K_{sym}, K_{public})$$



Bob envoie la clef K_{public}



Alice génère une
clef **symétrique** K_{sym}

et la chiffre avec K_{public}

$$K_{sym}^{chiffre} = F_{chiffre}(K_{sym}, K_{public})$$

Probleme :

**Qu'est ce qui garantit que Alice reçoit bien une clef publique
générée par Bob ?**

Un inconvénient majeur de l'utilisation des mécanismes de chiffrement asymétriques est le fait que la clef publique est distribuée à toutes les personnes.

Bob et Alice souhaitant échanger des données de façon confidentielle.

De ce fait, lorsque la personne possédant la clef privée, Alice, déchiffre les données chiffrées, elle n'a aucun moyen de vérifier avec certitude la provenance de ces données (Bob ou Carole)

On parle de **problèmes d'authentification**.

Protocole HTTPS



Bob envoie la clef K_{public} et
un certificat qui assure
qu'il est bien Bob



Alice génère une
clef **symétrique** K_{sym}

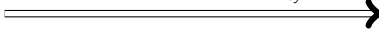
et la chiffre avec K_{public}

$$K_{sym}^{chiffre} = F_{chiffre}(K_{sym}, K_{public})$$

Protocole HTTPS



Alice envoie la clef $K_{sym}^{chiffre}$



Bob déchiffre $K_{sym}^{chiffre}$
avec sa clef privée

$$K_{sym} = F_{dechiffre} \left(K_{sym}^{chiffre}, K_{prive} \right)$$

Protocole HTTPS



Alice et Bob communiquent
en chiffrant les échanges
avec la même clef K_{sym}



Chiffrement asymétrique, les méthodes pratiques

- Chiffrement RSA (Rivest-Shamir-Adleman).
Le plus utilisé actuellement basé sur l'arithmétique des entiers et le petit théorème de Fermat.
- Cryptosystème de Chor-Rivest
Basé sur le problème du sac à dos.
- Cryptographie sur les courbes elliptiques et hyperelliptiques.
Très utilisé après RSA.
- Cryptographie à base de codes
Basé sur les codes correcteurs d'erreurs.
- Cryptographie multivariée
Basé sur les polynômes multivariés. Très en vogue dans le développement de la cryptographie post-quantique.