Sécurisation des communications : La cryptologie

La **cryptologie**, étymologiquement est la "science du secret"
Elle englobe :

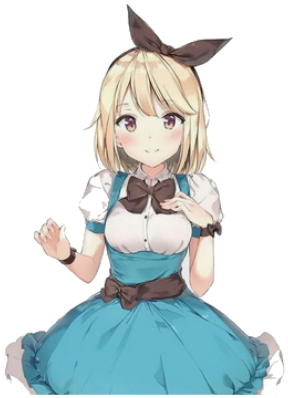
- la **cryptographie** : c'est la science du chiffrement et du déchiffrement
- la **cryptanalyse** : c'est l'analyse de la cryptographie. On utilise alors le verbe décrypter.

◊ La cryptographie s'intéresse à la protection des données.

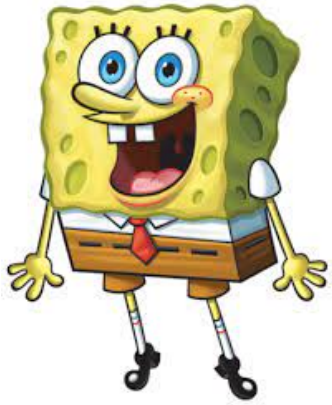
◊ la cryptanalyse a pour objectif de corrompre les propriétés apportées par la cryptographie. On parle couramment d'attaque sur un cryptosystème.

Remarque: On parle de codage et décodage quand la syntaxe d'écriture et de lecture est connue de tous les intervenants. Elle est publique (ex : python, ASCII, UTF8...)

Sécurisation des communications



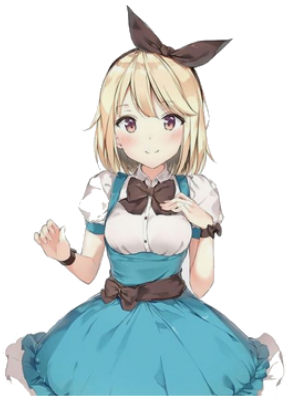
Alice et Bob communiquent
en chiffrant les échanges



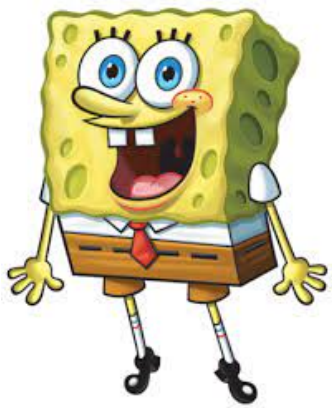
Deux méthodes :

- Le chiffrement symétrique.
- Le chiffrement asymétrique.

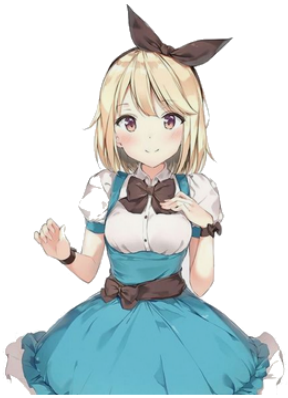
Chiffrement symétrique



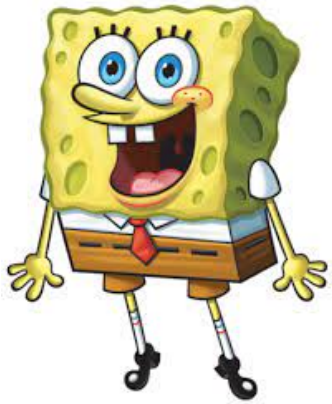
Alice et Bob communiquent
en chiffrant les échanges
avec la même clef K



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)
- Vigenére (Chiffrement par bloc)
- Chiffrement par substitution (Enigma)
- DES (chiffrement moderne obsoléte)
- 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.

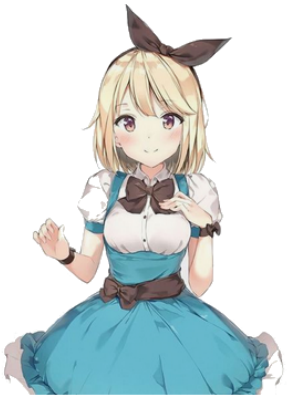
La boîte aux lettres :

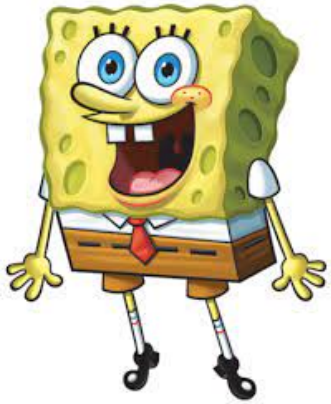
- La clef publique : une boîte aux lettres. N'importe qui peut y déposer un message.
- La clef privée : la clef "secrète" détenue uniquement par le possesseur de la boîte aux lettres.

Clef Publique

Clef Privé

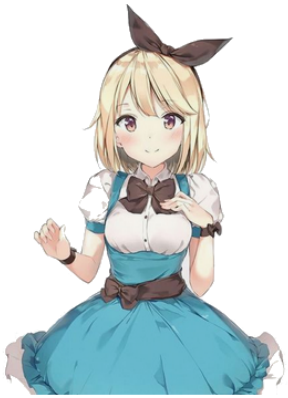
Chiffrement Asymétrique



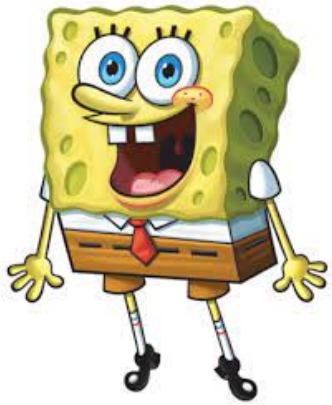


Alice génére un couple de clef asymétrique (K_{prive}, K_{public})

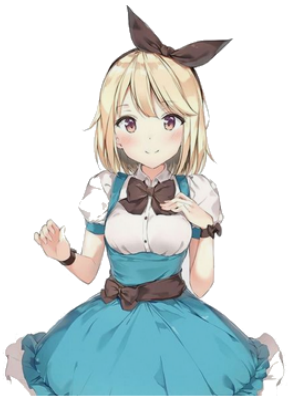
Chiffrement Asymétrique

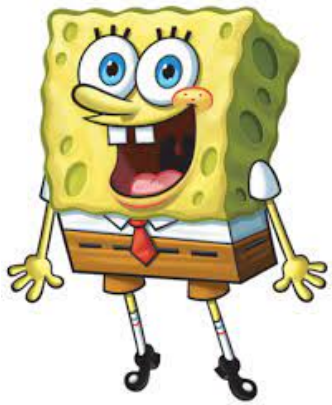


Alice envoie K_{public}



Chiffrement Asymétrique



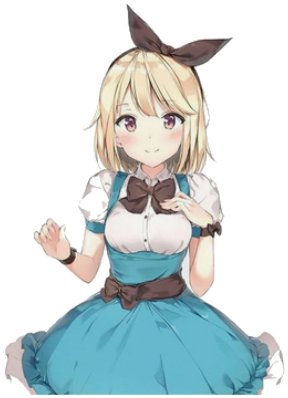


Bob chiffre le message

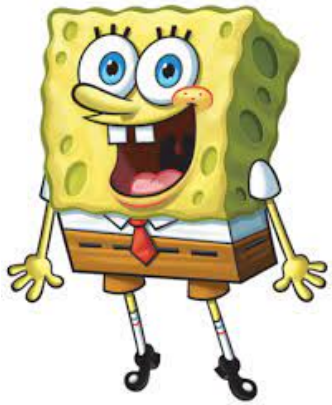
M_{clair} avec K_{public} :

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

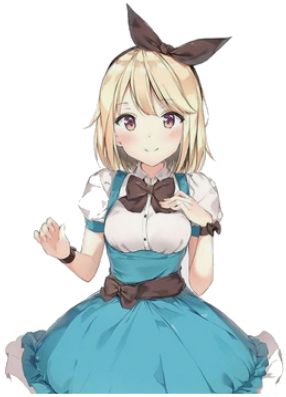
Chiffrement Asymétrique

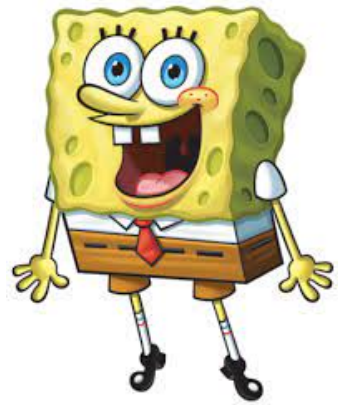


Bob envoie $M_{chiffre}$



Chiffrement Asymétrique





Alice déchiffre avec K_{prive}

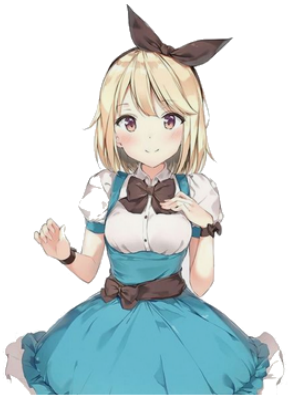
$$M_{clair} = F_{dechiffre}(M_{chiffre}, K_{prive})$$

Protocol HTTPS

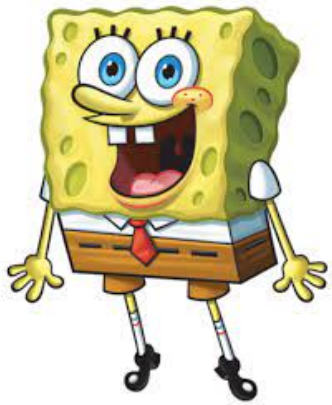
Le chiffrement asymétrique est trés gourmand en calcul.
On l'utilise surtout pour les échanges de clés.
Il est trés peu utilisé pour les échanges standards.

Protocole HTTPS

Utilisation des deux méthodes de chiffrement (symétrique et asymétriques) .

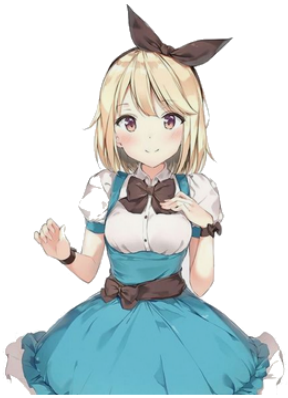


Alice Demande une connexion HTTPS avec Bob

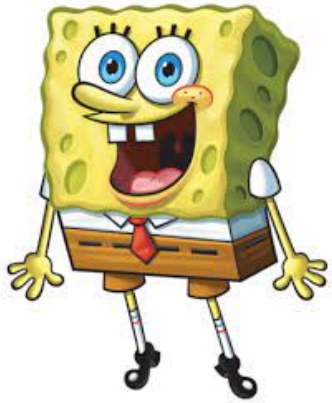


Bob génére un couple de clef asymétrique (K_{prive}, K_{public})

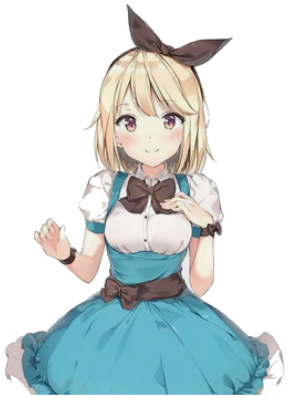
Protocole HTTPS



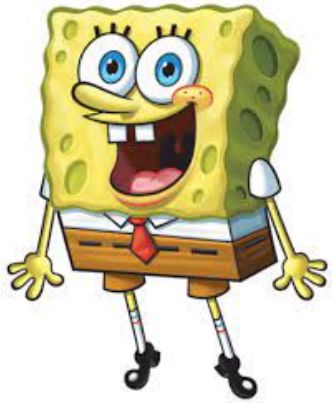
Bob envoie la clef K_{public}



Protocole HTTPS



Bob envoie la clef K_{public}



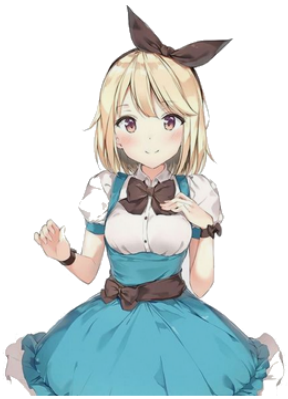
Probleme :
Qu'est ce qui garantit que Alice reçoit bien une clef publique générée par Bob ?

Protocole HTTPS : Authentification

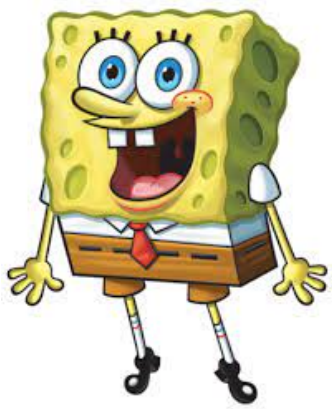
- Un inconvénient : la clef est public
- Alice ne peut pas vérifier avec certitude la provenance de ces données (Bob ou Carole)

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

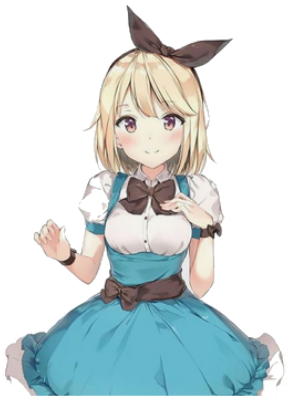
Protocole HTTPS et certificat



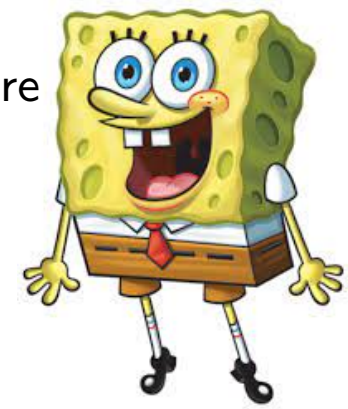
Bob envoie la clef K_{public} et
un certificat qui assure
qu'elle est bien à Bob



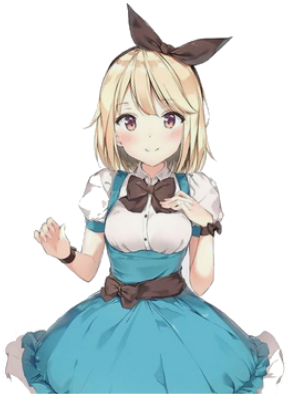
Protocole HTTPS et authentification par clef privée

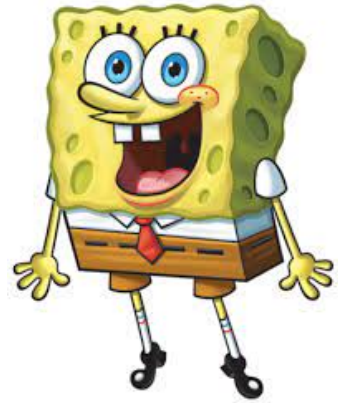


Bob envoie la clef K_{public} et authentification par clef privée qui assure que c'est Bob qui l'envoie.



Protocole HTTPS





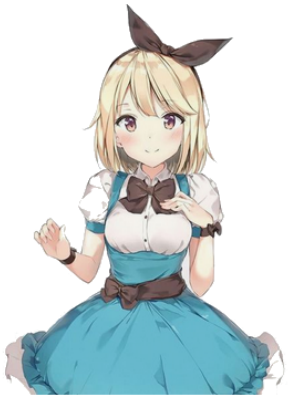
Alice génére une

clef **symétrique** K_{sym}

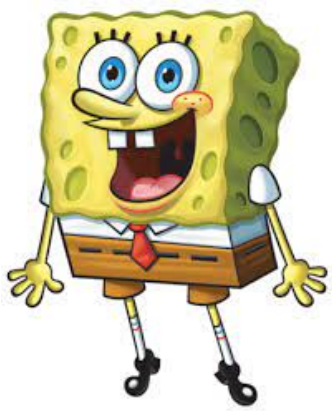
et la chiffre avec K_{public}

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

Protocole HTTPS



Alice envoie la clef $\overset{chiffre}{K_{sym}}$

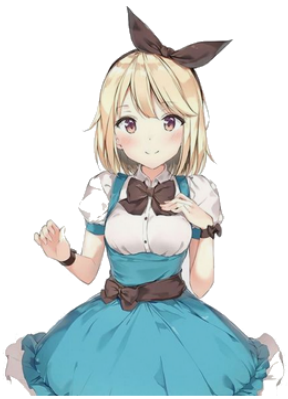


Bob déchiffre $\overset{chiffre}{K_{sym}}$

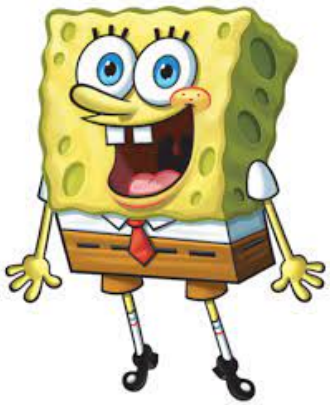
avec sa clef privée

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

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.

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.

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 aprés RSA.

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 aprés RSA.
- Cryptographie à base de codes
  Basé sur les codes correcteurs d'erreurs.

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 aprés 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.

Évolution de la factorisation par un ordinateur quantique :
21 (5 bits) en 2012, 143(8bits) en 2015, 56 153 (16bits) en 2017.
1005973 (20bits) en 2019.
On estime que les ordinateurs quantiques seront opérationnels au alentour de 2030.