

Cryptographie

Chiffrement asymétrique

- Cryptographie asymétrique



Avantage : Robustesse du chiffrement liée à l'usage d'une paire de clés

Inconvénient : Nécessité des ressources de calcul plus importantes

Algorithmes de chiffrement asymétrique : DSA, RSA

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique (à clé publique)
 - Algorithmes de chiffrement avec opérations mathématiques complexes
 - Connaître clé de chiffrement + algorithme de chiffrement utilisé **ne permet pas de calculer** la clé de déchiffrement -> avantage majeur
 - Pas d'échange de la clé de chiffrement

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique (à clé publique)
 - Taille de clé plus grande
 - Clé publique en libre accès
 - Clé privée est secrète et déployée sur un seul système

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique (à clé publique)
 - Usages :
 - Authentifier une communication
 - Echanger la clé secrète d'un chiffrement symétrique
 - Signature numérique

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : principe de base

CEJMA

- Chiffrement asymétrique



OBJECTIFS				
Authentification émetteur	Confidentialité	Intégrité	Authentification destinataire	Vitesse de traitement
✗	✓	✗	✓	✗

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : principe de base
 - Le destinataire du message :
 - Création d' une **bi-clé asymétrique** :
 - Clé publique ; Clé privée
 - Communique sa clé publique
 - L'émetteur du message (personne quelconque) :
 - Crée un message,
 - Le chiffre avec la clé publique du destinataire
 - Clé publique comparée à un **cadenas**
 - -> **confidentialité du message**

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : principe de base
 - Le destinataire du message :
 - Est **seul capable de déchiffrer** le message avec sa clé privée
 - Clé privée comparée à la **clé du cadenas**
 - -> **authentification** du destinataire assurée
 - Calculs consommateur de ressources

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique :
 - création de la bi-clé asymétrique

```
$ ssh-keygen
```

```
$ ls .ssh
```

```
id_rsa id_rsa.pub
```

Lien : <https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/debian/clessh>

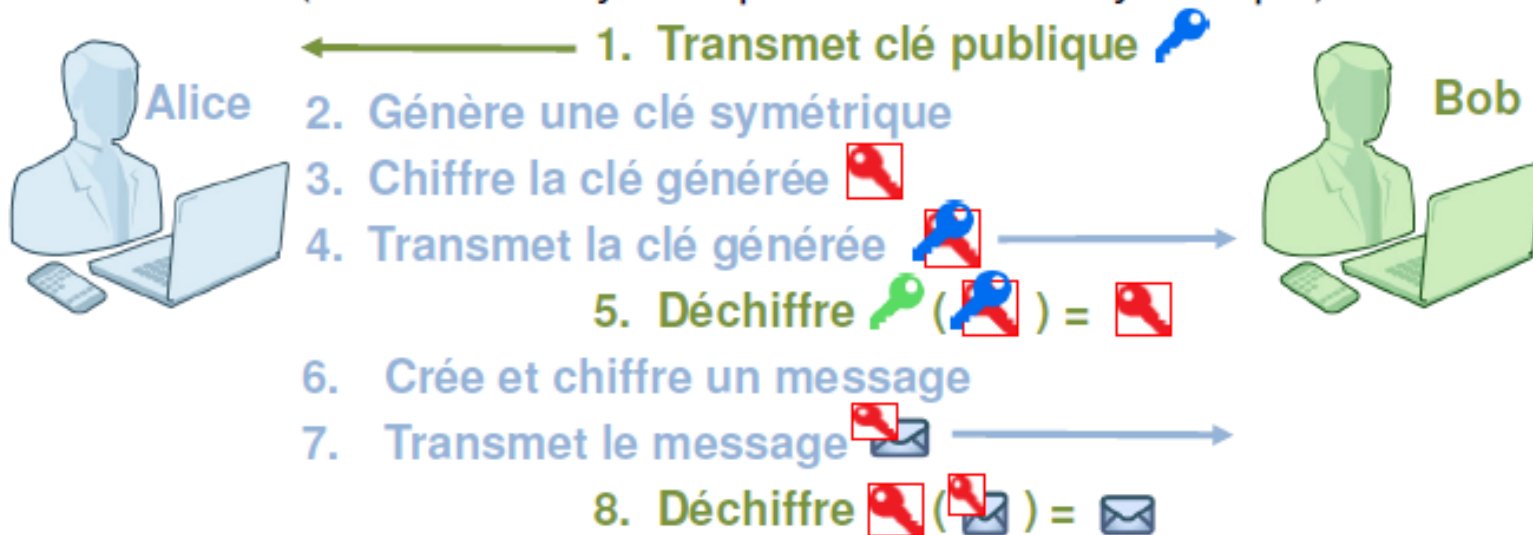
CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : clé de session

CEJMA

- Session (chiffrement asymétrique + chiffrement symétrique)



OBJECTIFS				
Authentification émetteur	Confidentialité	Intégrité	Authentification destinataire	Vitesse de traitement

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : clé de session
 - Le destinataire des échanges :
 - Création d' une **bi-clé asymétrique** :
 - Clé publique ; Clé privée
 - Communique sa clé publique
 - L'émetteur du message (personne quelconque) :
 - Génère une clé symétrique pour le destinataire permettant de chiffrer les messages = **clé de session**
 - Chiffre la clé symétrique avec la clé publique
 - -> **confidentialité** de la **clé symétrique**
 - -> **échange sécurisé** de la **clé symétrique**

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : clé de session
 - L'émetteur du message (personne quelconque) :
 - Envoi de la **clé symétrique chiffrée**
 - Le destinataire des échanges :
 - **Déchiffre** la clé symétrique
 - -> **authentification** du destinataire assurée
 - émetteur chiffre ses messages avec la clé symétrique
 - destinataire déchiffre avec la clé symétrique
 - -> calculs **consommement peu** de ressources
 - Plus **grande vitesse** de traitement

CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : clé de session
 - Durée de vie limitée de la clé de session
 - Usages :
 - https
 - sftp
 - ssh