CEJMA

Sécuriser les communications et les documents

- La cryptographie se base sur des opérations mathématiques généralement (algorithmes)
- Objectif : transmettre de manière sécurisée des messages

CEJMA

Sécuriser les communications et les documents

- Principe du chiffrement :
  - appliquer un algorithme sur le message en clair
  - qui utilise comme paramètre d'entrée une clé de chiffrement.
- Principe du déchiffrement :
  - appliquer un algorithme sur le message chiffré
  - qui utilise comme paramètre d'entrée une clé de déchiffrement.

- Cryptographie symétrique :

Avantage : Rapidité des opérations de chiffrement et déchiffrement

Inconvénient : Transmission de la clé secrète de chiffrement (la procédure doit être sécurisée)

Algorithmes de chiffrement symétrique : AES, DES, Blowfish

CEJMA

Sécuriser les communications et les documents

- Chiffrement symétrique (à clé secrète)
  - Algorithmes de chiffrement avec opérations mathématiques simples
  - Connaître clé de chiffrement + algorithme de chiffrement utilisé permet de calculer la clé de déchiffrement -> inconvénient majeur
  - clé secrète assimilée à une clé identique pour chiffrer et déchiffrer -> **la clé doit rester secrète**
  - **Procédure sécurisée pour transmettre la clé**

CEJMA

Sécuriser les communications et les documents

- Chiffrement symétrique (à clé secrète)
  - Avantage : rapidité des opérations cryptographiques rapidement.
  - Algorithme AES, DES / triple DES, Blowsfish
  - AES est l'un des plus sûr
  - Robustesse du procédé :
    - Les algorithmes symétriques sont connus
    - Tentative de déchiffrement = découvrir la clé
    - -> importance du choix de la **longueur de la clé**

CEJMA

Sécuriser les communications et les documents

- Activité sur l'algorithme AES
  - https://www.securiteinfo.com/cryptographie/aes.shtml
  - https://www.keylength.com/fr/5/
  - Caractéristiques de l'algorithme AESP
  - Quels critères déterminent le niveau de sécurité ?
  - Recommandation de l'ANSSI
  - Exemples de mise en œuvre de AES

CEJMA
Cryptographie

- Cryptographie asymétrique

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

Inconvénient : Nécessite 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

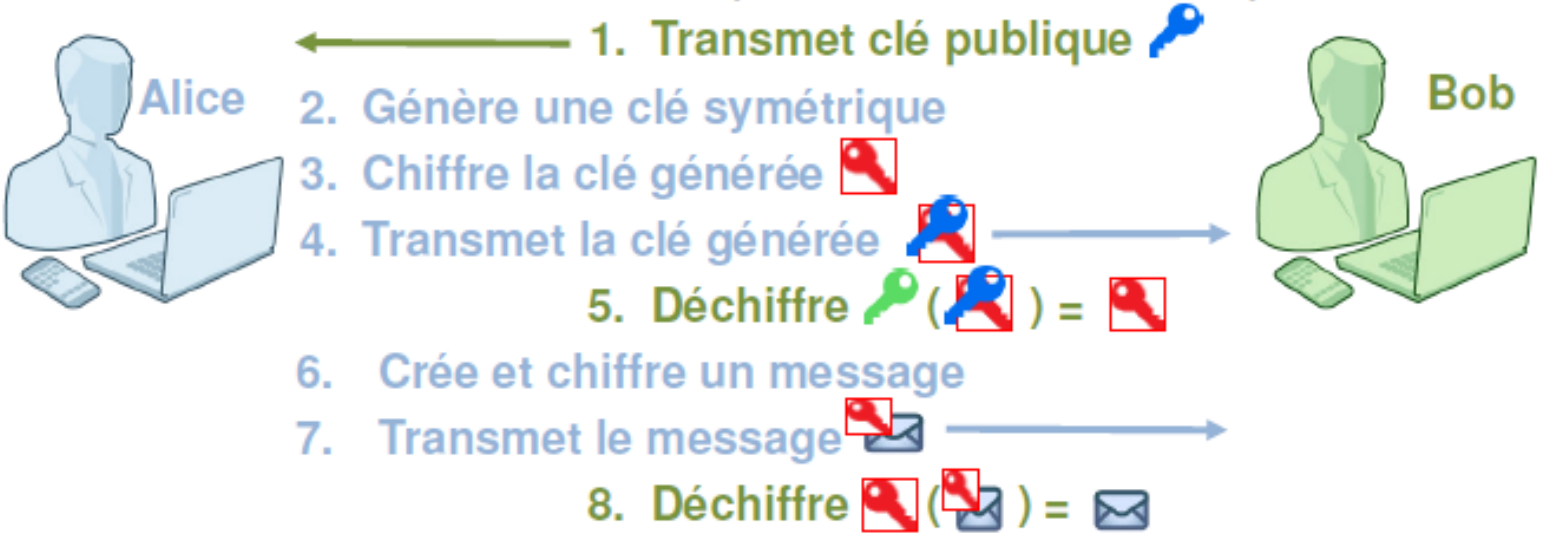
CEJMA

Sécuriser les communications et les documents

- Chiffrement asymétrique : 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 pub
    - -> **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 **consomment 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