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
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 :
  - 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

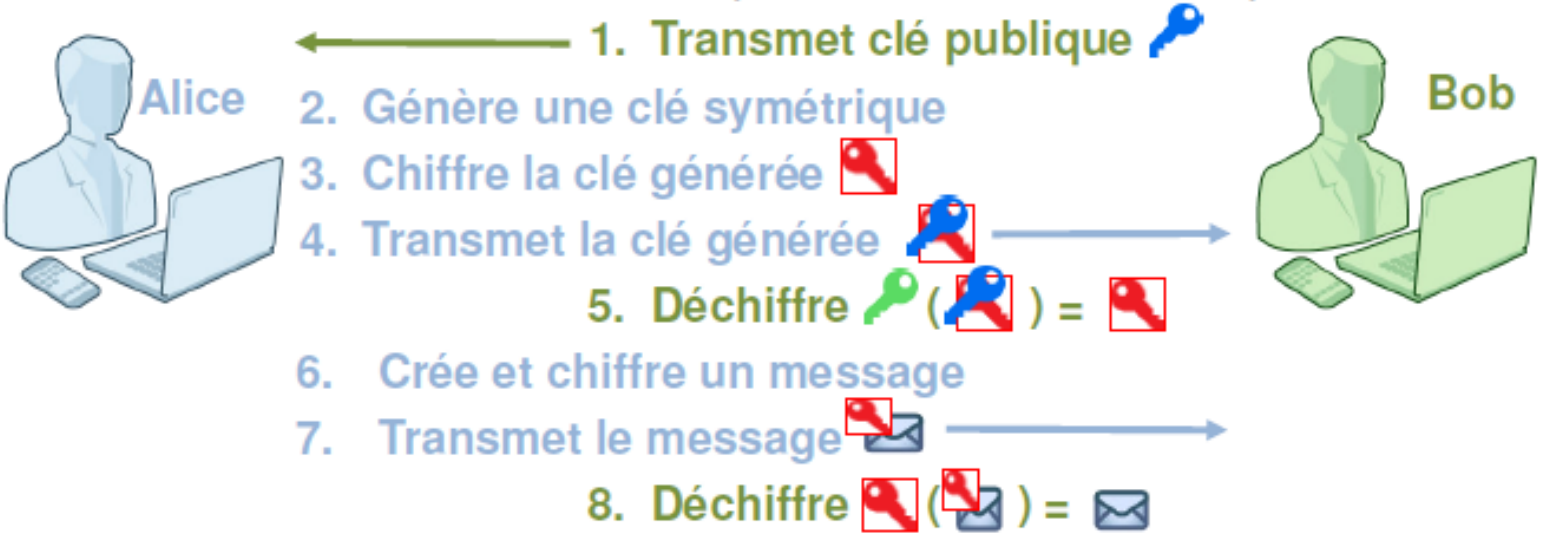
CEJMA

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 **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

CEJMA

Sécuriser les communications et les documents

- Fonction hachage
  - fonction unidirectionnelle -> irréversible
  - lie un code « **unique »** de taille fixe = empreinte électronique, haché (condensat, empreinte, hash, message digest)
  - à un message de **longueur quelconque**.
  - > impossible de retrouver le message depuis le haché
  - Modification minime du message -> haché différent
  - Algorithmes de hachage : MD5 ; SHA1 ; SHA2

CEJMA

Sécuriser les communications et les documents

- Fonction hachage
  - Site https://emn178.github.io/online-tools/sha256.html

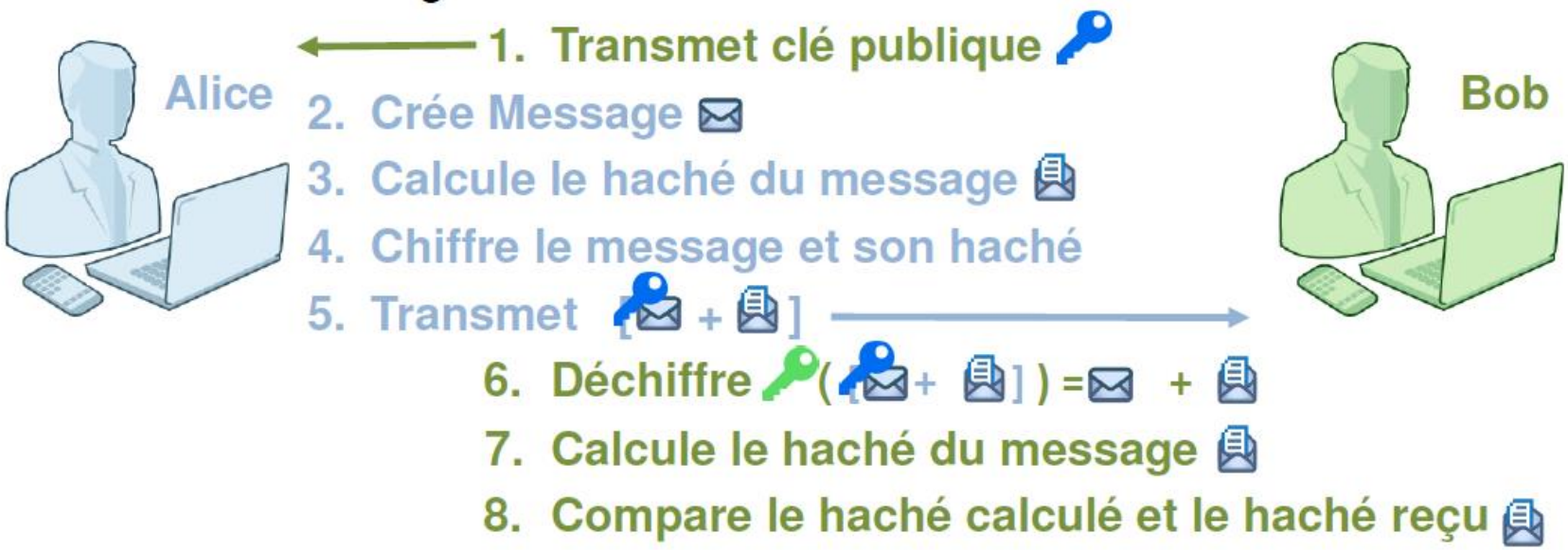
CEJMA

Sécuriser les communications et les documents

- Contrôle d'intégrité
  - Chiffrement asymétrique et intégrité

CEJMA

- Contrôle d'intégrité



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

CEJMA

Sécuriser les communications et les documents

- Signature numérique
  - Chiffrer le haché d'un message
  - Avec sa clé privée
  - -> authentification et intégrité du message

CEJMA

- Signature numérique

1. Transmet clé publique →
2. Crée Message et son haché
3. Chiffre haché (clé privée Alice)
4. Transmet + →

Alice

5. Déchiffre haché ( ) =
6. Compare le haché calculé et le haché reçu

Bob

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

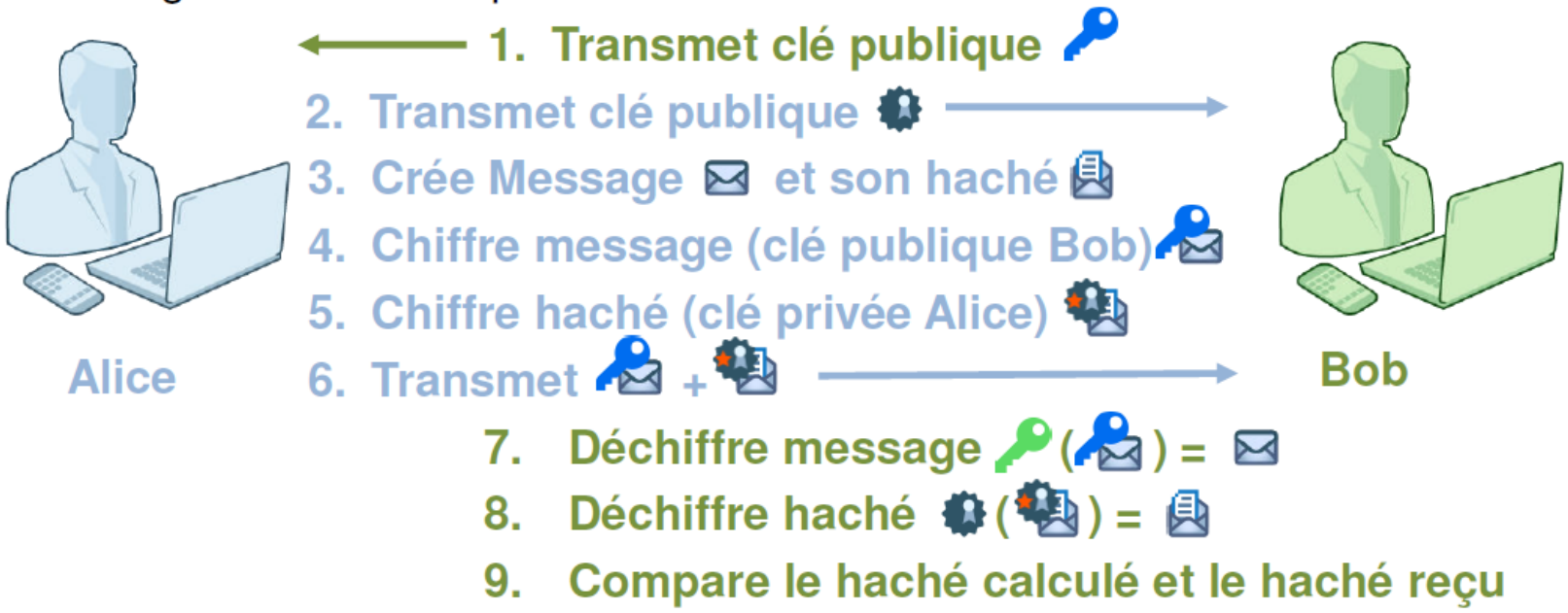
CEJMA

Sécuriser les communications et les documents

- Signature numérique et chiffrement
  - Chiffrer le haché d'un message
  - Avec sa clé privée
  - -> authentification et intégrité du message

CEJMA

- Signature numérique et chiffrement



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

CEJMA

Sécuriser les communications et les documents

- Signature numérique et chiffrement
  - Authentification émetteur :
    - Déchiffrement du haché avec la clé publique de l'émetteur
  - Confidentialité :
    - Chiffrement du message avec la clé publique du destinataire
  - Intégrité :
    - Comparaison haché reçu et haché calculé
  - Authentification du destinataire :
    - Déchiffrement du message avec la clé privée du destinataire

CEJMA

Sécuriser les communications et les documents

- Autorité de certification de confiance
  - Tiers de confiance dans un domaine défini (entreprise, Agence, continent, etc.)
  - Gère les certificats et les identités numériques
  - Signe les certificats émis -> garant de leur authenticité

CEJMA

Sécuriser les communications et les documents

- Création identité numérique
  - Création bi-clé asymétrique
  - Renseignement de l'identité de l'utilisateur
  - Création de l'identité numérique :
    - Identité + clé publique + clé privée
  - Création du certificat public signé et limité dans le temps:
    - identité + clé publique

CEJMA

Sécuriser les communications et les documents

- Vérifications :
  - Deux conditions pour la preuve électronique :
    - Signataire identifié : nom, adresse, etc.
    - Lien entre le document et l'identité
    - -> non-répudiation par le signataire du document signé

CEJMA

Sécuriser les communications et les documents

- Vérifications :
  - Certificat électronique délivré par une CA de confiance
    - -> vérifier l'identité de l'auteur du document
  - Clé publique :
    - -> vérifier la signature électronique
  - Empreinte électronique :
    - -> Intégrité