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

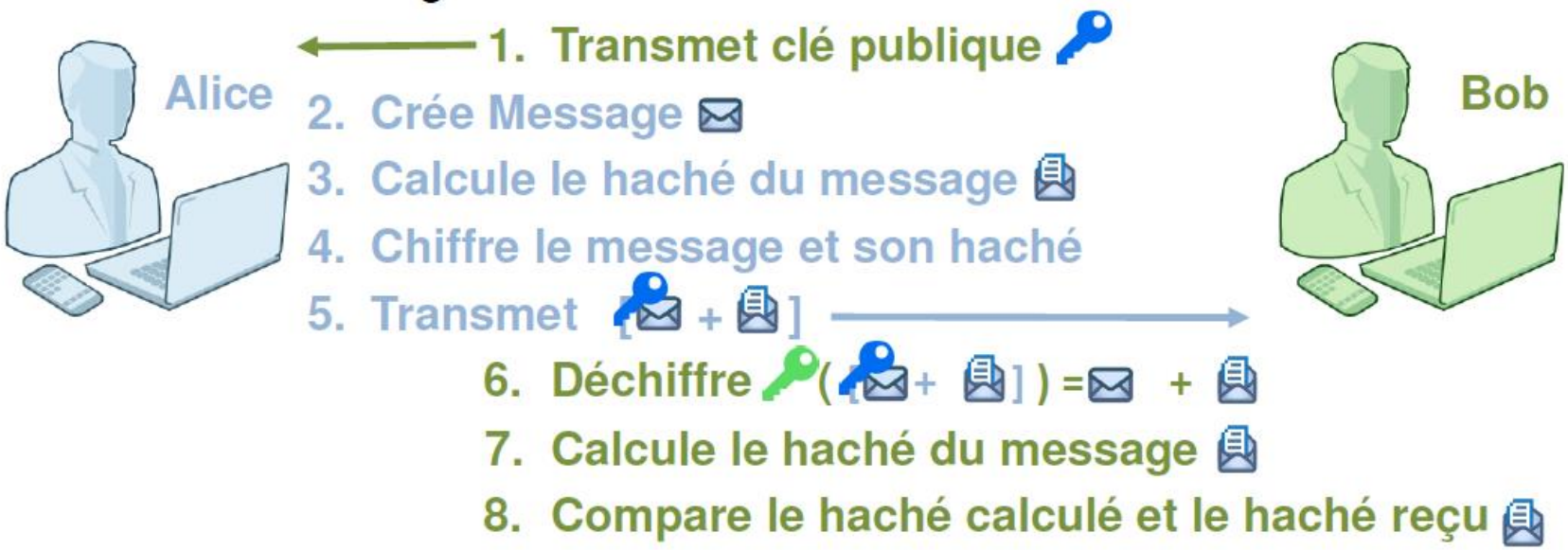
CEJMA

Sécuriser les communications et les documents

- 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
✓	✗	✓	✗	✗

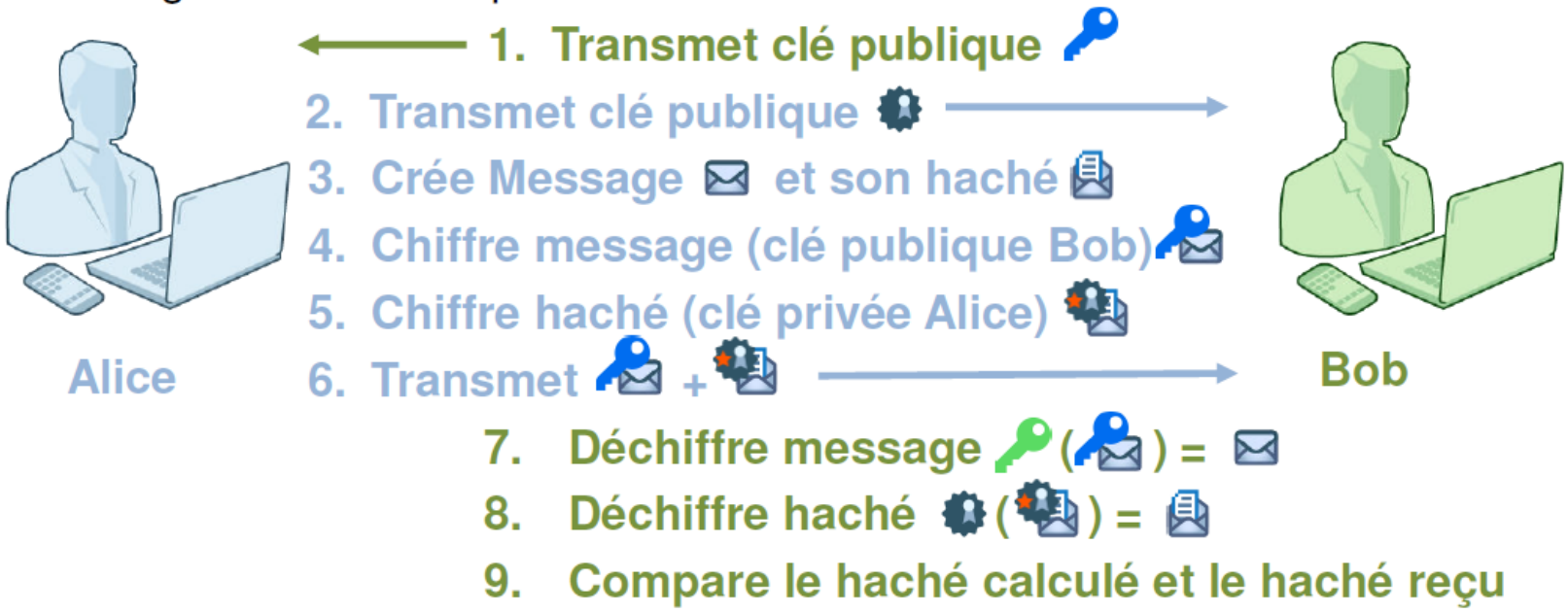
CEJMA

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