

# Cryptographie

## Les bases

# Introduction

- Échange d'information sensibles
  - cette problématique n'est pas nouvelle
  - un contrat entre deux parties
    - authenticité : signatures, paraphes
    - intégrité du contenu : conservation d'une copie par les deux parties
  - informations confidentielles transmises à un notaire, avocat, médecin, ...
  - données militaires
  - ...

# Introduction

- Objectifs de la cryptographie
  - confidentialité
    - seul le destinataire peut connaître le contenu du message qui lui est envoyé
  - authenticité
    - le destinataire du message doit pouvoir s'assurer de son origine
  - intégrité
    - le destinataire doit pouvoir s'assurer que le message n'a pas été modifié
  - non répudiation
    - l'émetteur et le destinataire ne peuvent nier d'avoir émis et reçu le message

# Introduction

- Cryptographie
  - ensemble des techniques permettant de chiffrer des messages
    - techniques basées sur des calculs
  - un message est protégé à l'aide de clés (ou secrets)
    - le but est d'assurer la confidentialité, l'authenticité et l'intégrité du message émis
  - chiffrement
    - action de transformation d'un message en clair (plaintext) en un message chiffré (ciphertext, cryptogramme)
  - déchiffrement
    - action inverse au chiffrement

# Introduction

- Décrypter : action de casser un code pour récupérer le plaintext
- Le chiffrement est effectué à l'aide d'une clé de chiffrement
  - clé symétrique : la même clé est utilisée pour le chiffrement et le déchiffrement
    - chiffrement à clé secrète
  - clés asymétriques : les clés utilisées sont différentes
    - chiffrement à clé publique

# Vocabulaire

- **digest** : permet de s'assurer de l'intégrité du message
- **chiffrement par clé symétrique** : permet de s'assurer de la confidentialité du message
- **chiffrement par clé publique** : permet à deux parties de partager un secret, sans échange préalable de clé
- **signature numérique** : authentifie l'auteur du message
- **certificat numérique** : technologie permettant à de sécuriser les signatures numériques par une partie tiers (CA)
- **signature du code** : permet de s'assurer que le code est livré par une entité de confiance
- **SSL/TLS** : protocole de communication sécurisé
  - Transport Layer Security est le successeur de Secure Socket Layer

# Cryptographie

- Ensemble de techniques pour protéger un message en le transformant en un autre message
  - l'information transmise devient non compréhensible
  - à l'inverse des méthodes de cryptanalyse sont utilisées pour intercepter les messages

# Cryptographie

- Fonction de chiffrement
  - permet de chiffrer un message  $m$  avec une clé  $k$
  - utilise une fonction  $C_k$

$m \rightarrow$  fonction de chiffrement + clé  $\rightarrow C_k(m)$




- La fonction de déchiffrement  $D_k(c)$  permet de retrouver le message originel

$c \rightarrow$  fonction de déchiffrement + clé  $\rightarrow D_k(c)$

- Les fonctions vérifient l'équation

$$D_k(C_k(m)) = m$$

# Cryptographie

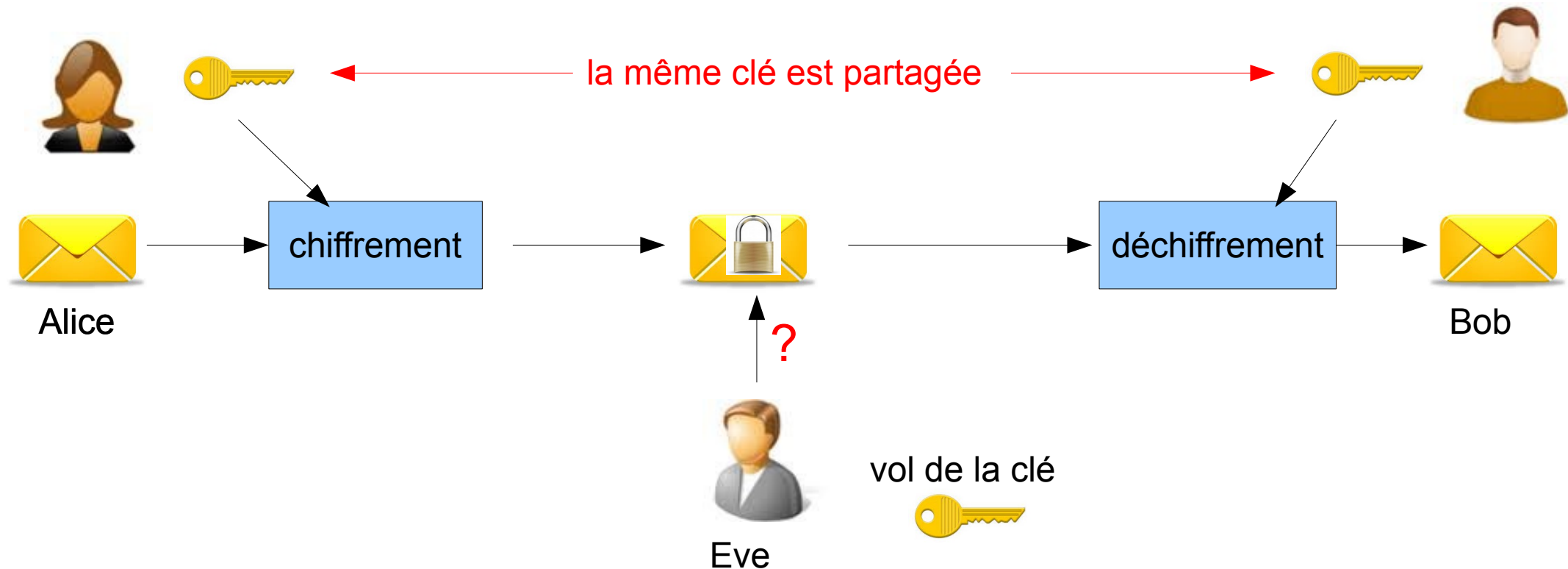
- Deux catégories de chiffrement
  - chiffrement symétrique
    - même clé pour chiffrer et déchiffrer 
  - chiffrement asymétrique
    - nommé aussi chiffrement à clef publique
    - utilise
      - une clé publique pour chiffrer 
      - une clé privée pour déchiffrer 

# Cryptographie

- Plutôt que d'utiliser des lettres A, B, C, ... les protagonistes des échanges de messages sont nommés, avec leurs rôles
  - utilisateurs légitimes
    - Alice et Bob: Alice tente d'envoyer un message à Bob
    - Carol et Dave sont deux autres participants
  - adversaires
    - Eve : écoute les échanges entre Alice et Bob
    - Mallory : peut modifier, substituer des messages lors des échanges entre Alice et Bob
  - liste complète : [https://fr.wikipedia.org/wiki/Alice\\_et\\_Bob](https://fr.wikipedia.org/wiki/Alice_et_Bob)

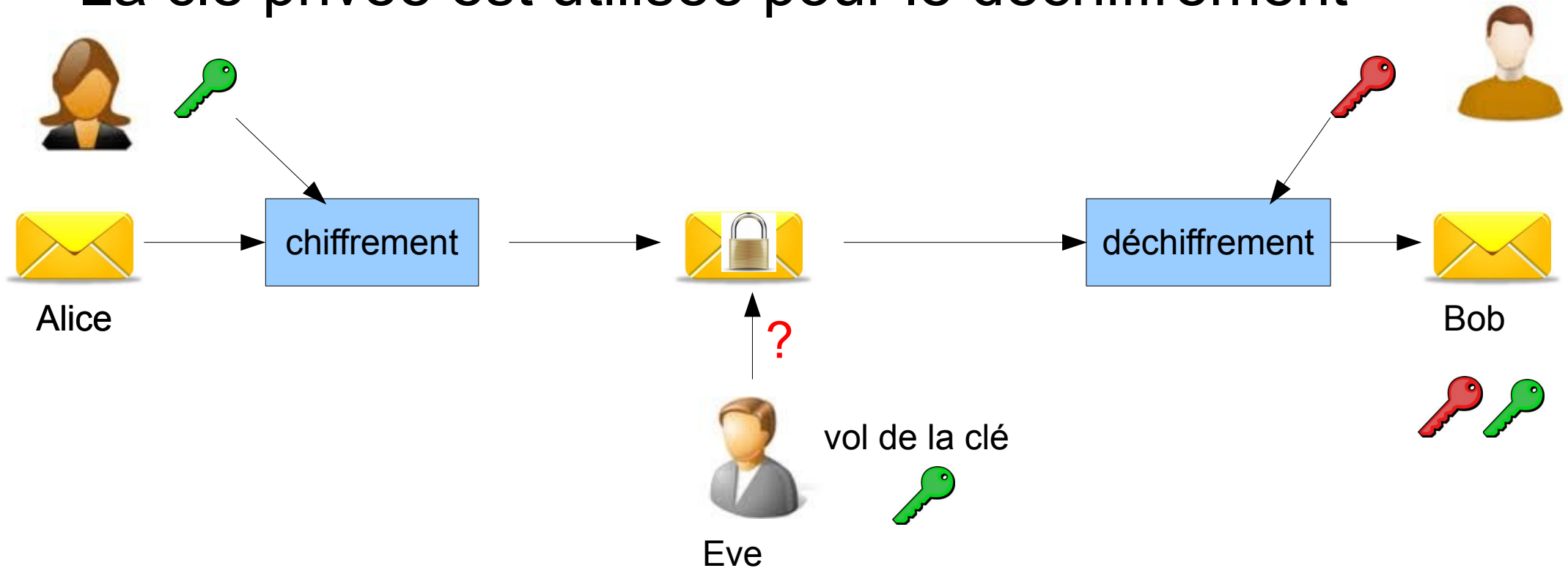
# Chiffrement symétrique

- La même clé est utilisée pour le chiffrement et le déchiffrement



# Chiffrement asymétrique

- La clé publique est diffusée, et est utilisée pour le chiffrement
- La clé privée est utilisée pour le déchiffrement



# Hachage

- L'intégrité du message est assurée par une fonction
  - converti un message de taille quelconque en une chaîne de caractères de taille unique
    - digest, hash, condensé, résumé, empreinte, ...
  - fonction rapide à exécuter
  - fonction à sens unique
    - il est impossible de retrouver le message en clair à partir du digest
      - collisions possibles en fonction des algorithmes

# Hachage

- Principaux algorithmes utilisés
  - cf. : [https://fr.wikipedia.org/wiki/Cat%C3%A9gorie:Algorithme\\_de\\_hachage](https://fr.wikipedia.org/wiki/Cat%C3%A9gorie:Algorithme_de_hachage)
  - MD5
    - Message Digest 5
    - impropre à toute utilisation en sécurité
  - SHA
    - Secure Hash Algorithm
    - SHA3
  - algorithmes insécures
    - MD5, SHA-0, SHA-1

# Hachage

- Les fonctions de hachage sont employées pour stocker les mots de passe des utilisateurs

motdepasse → sha256 → f82d4ae82779aeea53bc7bb14fbe5d877f27b968185c28b58acddc748d4d1165

- ce sont les résumés qui sont alors comparés
- si un attaquant récupère la base de données, connaissant la fonction de hachage il peut récupérer le mot de passe
  - attaque par dictionnaire
  - attaque par force brute
  - attaque par rainbow tables

# Hachage

- Attaque par dictionnaire
  - un dictionnaire de mots de passe usuels existe
    - prénom, nom, mots courant, ...
    - 75% des utilisateurs utilisent 500 mots de passe les plus courant
  - chaque entrée du dictionnaire est hachée
  - comparaison avec le hash de la base récupérée
- Attaque par force brute
  - hachage de toutes les combinaisons
  - long mais utilisable sur des mot-de-passes courts
    - moins d'une minute pour un PC avec max 6 caractères et SHA1

# Hachage

- Attaque par rainbow table
  - la table contient toutes les combinaisons possibles des mots de passe avec une correspondance directe sur le hash
    - tables très volumineuses, plusieurs Téraoctets
  - site accessible pour les mots de passes classiques
    - recherchez sur internet le mot de passe pour

5ed25af7b1ed23fb00122e13d7f74c4d8262acd8

# Hachage

- Salage
  - complique la tâche de l'attaquant
  - une donnée (le sel) est ajoutée pour régénérer le hash
    - donnée aléatoire, générée pour chaque entrée
    - cette donnée est sauvegardée en base
      - pas dans la table des utilisateurs et des mot de passes hachés

sel : 123ac456bf789

motdepasse+sel → SHA256 → 8cdc4982e5330f9d8badd045abd3fbe7319be7d98f74bfe883fc54adc6d25e07

- si l'attaquant ne possède pas les sels il devient très complexe de mener une attaque

# Signature numérique

- Permet de garantir l'intégrité d'un message et d'authentifier son auteur
- Doit être
  - authentique : l'identité du signataire doit être retrouvée
  - infalsifiable : la signature ne peut pas être falsifiée
  - non réutilisable : la signature fait partie du document et ne peut pas être copiée dans un autre
  - inaltérable : une fois le document signé il n'est plus modifiable
  - irrévocable : le signataire ne peut pas nier le document

# Signature numérique

- Utilise la cryptographie asymétrique
  - le sens chiffrement/déchiffrement est inversé par rapport au chiffrement asymétrique
- Signature
  - Alice crée un hash du document  $m$  à signer
$$h = H(m)$$
  - Alice chiffre le résumé avec sa clé privée
$$s = C_{k_{priv}}(h)$$
  - le document en clair  $m$  et  $s$  sont mis dans un conteneur et envoyés à Bob

# Signature numérique

- Réception du message
  - Bob doit prouver l'authenticité du message
    - il récupère le message  $m$  en clair et crée un résumé
      - le même qu'Alice
$$h = H(m)$$
    - Bob déchiffre la signature avec la clé publique d'Alice
$$h' = D_{k_{pub}}(s)$$
    - il compare  $h$  et  $h'$ , qui doivent être égaux
      - car  $h' = D_{k_{pub}}(C_{k_{priv}}(H(m)))$