INTRODUCTION À LA CRYPTOGRAPHIE

OLFA BESBES

olfa.besbes@isitc.u-sousse.tn

3ÈME LICENCE A.U. 2022-2023

1

Plan

- Terminologie de la cryptographie
- Primitives cryptographiques
- Chiffrement et déchiffrement
- Chiffrement à clé publique / secrète
- Fonction de hachage
- Signature numérique
- Certificat numérique
- Protocoles cryptographiques

2

Terminologie de la cryptographie

- *Cruptos* = Caché et *Graphein* = Écrire
- **Cryptologie** = Science du secret = {Cryptographie, Cryptanalyse} ⊂ **Sécurité**
- **Cryptographie** : Ensemble de techniques permettant de **protéger** des informations et des communications de quiconque n'est pas autorisé.
- **Cryptanalyse** : Ensemble de procédés d'**attaques** des systèmes cryptographiques afin de trouver des failles et de décrypter les informations chiffrées sans connaître la clé de déchiffrement.

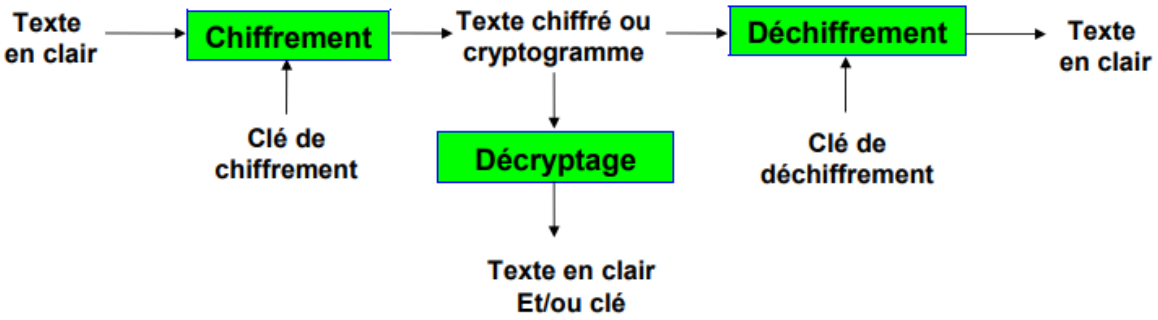
3

Terminologie de la cryptographie

- **Crypto-système** = Système cryptographique
- **Chiffrement** : Opération de chiffrer un message en clair pour rendre une information incompréhensible en absence de la clé de déchiffrement.
- **Déchiffrement** : Action inverse du chiffrement qui s'effectue uniquement en possession de la clé secrète.
- **Décryptage** : Déchiffrement du message chiffré sans la clé secrète.
- **Protocole** : Ensemble de règles qui régissent les échanges de données.

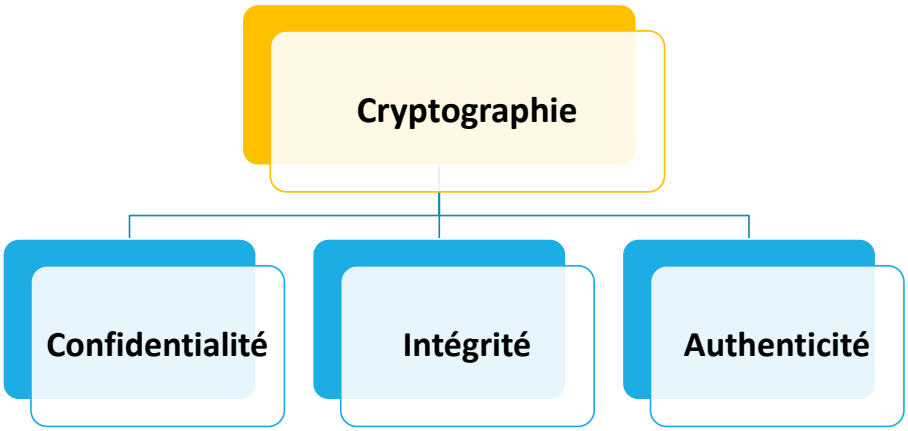
4

Crypto-sytème et décryptage



5

Primitives cryptographiques

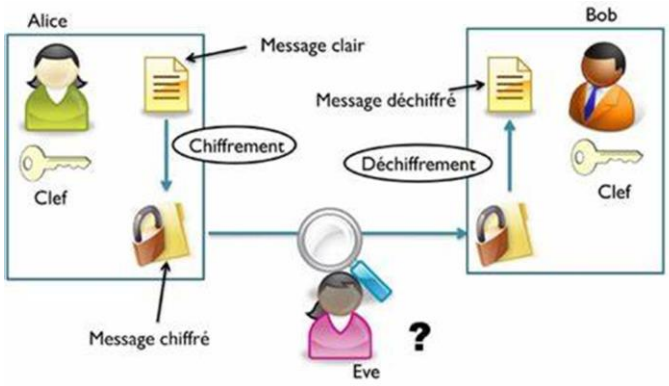


6

Confidentialité

- L'information n'est seulement **accessible** qu' aux *personnes autorisées*.
- Ou bien assurer **un stockage sécurisé** localement ou sur un serveur distant.

➡ **Chiffrement de l'information**



7

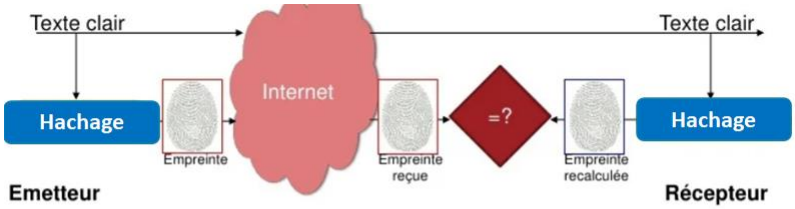
Confidentialité des communications

- **Domaine militaire** : Transmission de documents, de stratégies, de plans secret défense.
- **Domaine médical** : Confidentialité des dossiers de patients.
- **Domaine commercial** : Transmission des informations bancaires lors d'achats en ligne.
- **Domaine industriel** : Transmission d'informations internes à l'entreprise à l'abris des concurrents.

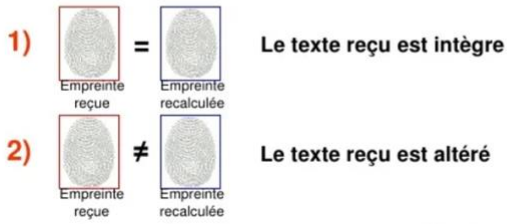
8

Intégrité

- L'information ne peut être **modifiée** / **détruite** que par les personnes autorisées.



➡ **Fonction de hachage**



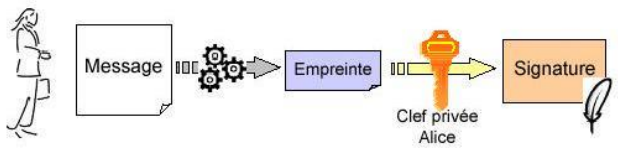
9

Authenticité

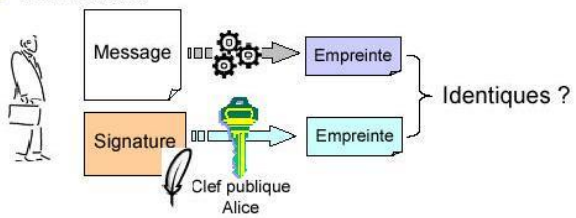
- L'expéditeur est bien celui qu'il prétend être.

➡ **Signature numérique**

- Signature



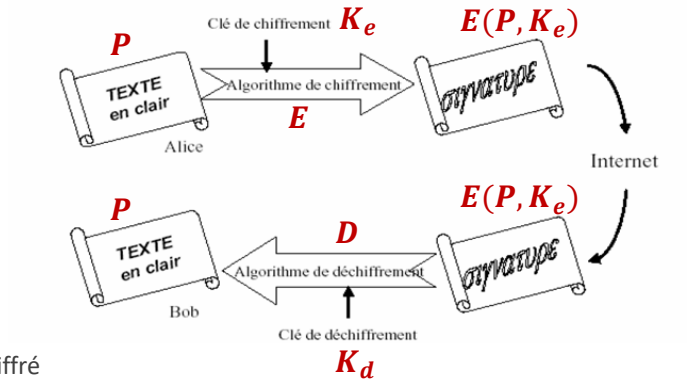
- Vérification



10

Chiffrement et déchiffrement

- P : Message en clair
- E : Algorithme de chiffrement
- D : Algorithme de déchiffrement
- K_e : Clé de chiffrement
- K_d : Clé de déchiffrement
- $E(P, K_e)$: Message chiffré
- $P = D(E(P, K_e), K_d)$: Message déchiffré



11

Chiffrement à clé secrète / publique

Chiffrement symétrique ou à clé secrète

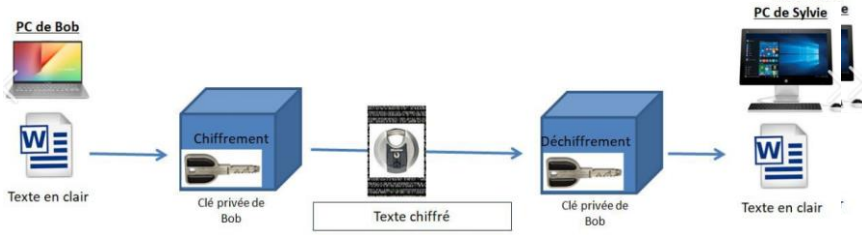
- $K_e = K_d$: Clé privée / secrète de **l'émetteur**.
- L'échange de la clé secrète est nécessaire entre l'émetteur et le récepteur.

Chiffrement asymétrique ou à clé publique

- $K_e \neq K_d$
- K_e : Clé publique du **récepteur** envoyée à l'émetteur pour le chiffrement.
- K_d : Clé privée / secrète du **récepteur**.

12

Chiffrement à clé secrète



++ Avantages ++

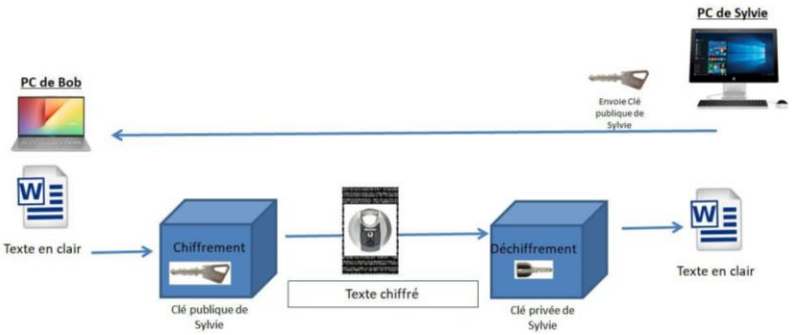
- Cryptosystème rapide
- Clés relativement courtes (128 ou 256 bis)

-- Inconvénients --

- Gestion difficile de plusieurs clés
- Echange de la clé secrète (point faible)

13

Chiffrement à clé publique



++ Avantages ++

- Clé privée n'est pas échangée
- Gestion facile des clés

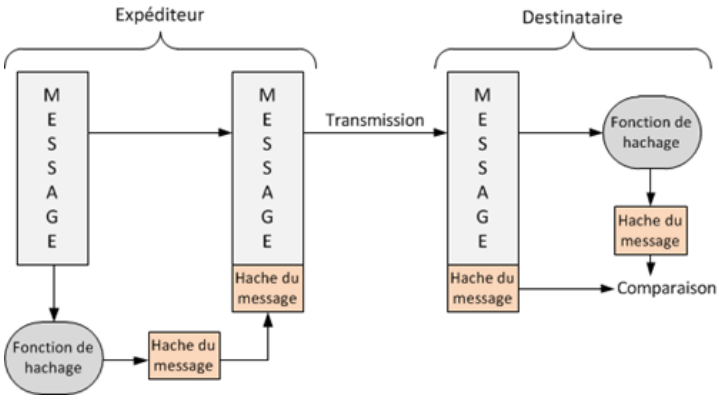
-- Inconvénients --

- Clés plus longues
- Crypto-systèmes plus lents
- Gestion de certificats de clés publiques

14

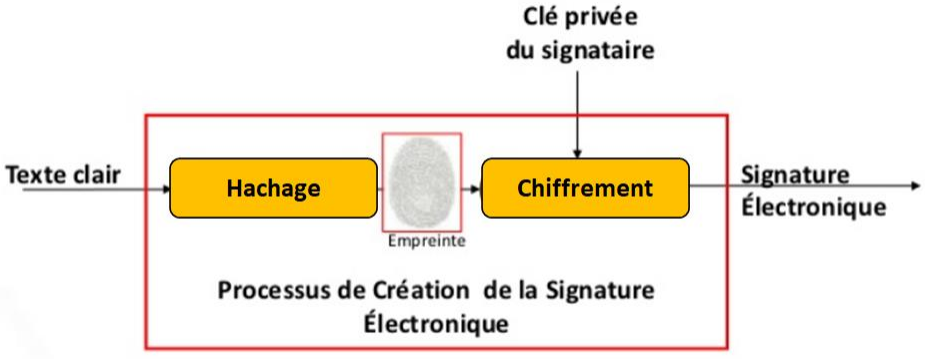
Propriétés d'une fonction de hachage

- Calcul **simple** et **rapide**
- **Taille fixe** de l'empreinte
- **Irréversible**
- **Unicité**
- **Intégrité**



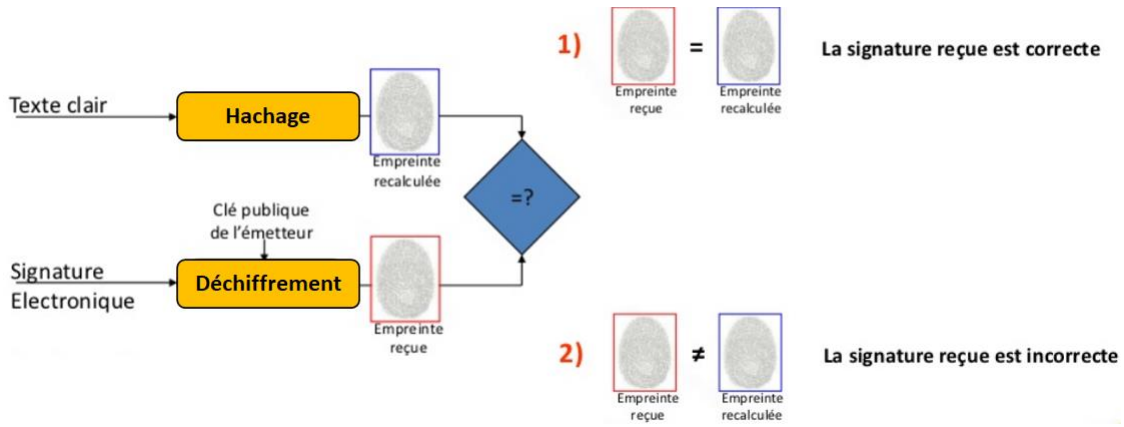
15

Création de la signature électronique



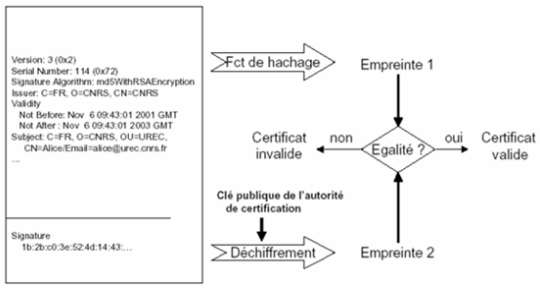
16

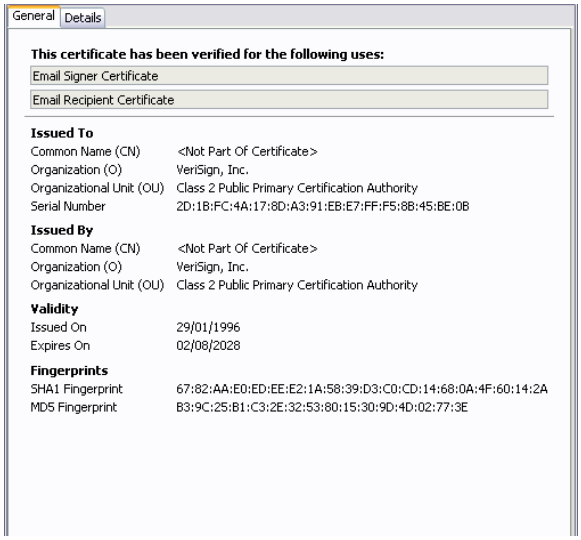
Vérification de la signature électronique



Certificat numérique

- Tout certificat numérique est délivré par une **autorité de certification** (CA).
- Un certificat électronique est une **identité numérique** (d'une personne, d'un organisme, d'un site Web, etc.) qui se compose de trois éléments :
  - Une clé publique.
  - Des informations sur le certificat (l'identité de l'utilisateur, son nom, son ID, etc.)
  - Une ou plusieurs signatures numériques.
- Le certificat est signé par le CA en créant une empreinte avec une fonction de hachage qui est ensuite cryptée avec la **clé privée de la CA**.
- La vérification s'effectue avec la **clé publique de la CA**.





Certificat numérique

19

Protocoles Cryptographiques

- Un protocole cryptographique ou un **protocole de sécurité** est un ensemble d'opérations cryptographiques à réaliser, leur séquence, afin de sécuriser la communication.
- Il assure les **services de sécurité** : la confidentialité, l'intégrité et l'authentification.
- Il utilise les **mécanismes de sécurité** : chiffrement, signature, hachage, certificat, etc.
- Exemples :
  - **SSH (Secure Shell)** : Accès sécurisé sur des machines distantes à travers un réseau ouvert.
  - **Secure Socket Layer (SSL)** : Sécurisation des échanges entre clients et serveurs sur internet. Il se situe en position intermédiaire entre la couche de transport assurée par TCP et la couche application correspondant aux protocoles SMTP, HTTP ou FTP.
  - **Secure Electronic Transaction (SET)** : Sécurisation des transactions de paiement utilisant la carte bancaire.
  - **S/MIME (Secure/Multipurpose Internal Mail Extensions)** : Envoi de messages chiffrés et signés numériquement.

20