Sécurité et contrôle d'accès aux big data

MALEK REKIK LABIDI

1

Objectifs de la sécurité informatique

- Authentification
- Confidentialité
- Intégrité
- Non-répudiation
- Disponibilité
- Contrôle d'accès
- Autorisation

2

Objectifs de la sécurité informatique

- Confidentialité: Protection des données transmises contre les attaques passives, et protection des flux de données contre l'analyse.
  - Préservation du secret des données transmises. Seulement les entités communicantes sont capable d'observer les données.
  - Protection des adresses source et destination, fréquence et longueur des messages, etc.
- Mécanismes utilisés: Cryptage, techniques d'anonymisation, contrôle d'accès.

3

Objectifs de la sécurité informatique

- Authentification: S'assurer que l'origine du message soit correctement identifié:
  - Assurer le receveur que le message émane de la source qui prétend avoir envoyé ce message.
  - Assurer l'authenticité des entités participantes: chacune des entités est celle qui prétende l'être.
  - Empêcher la perturbation de la connexion par une tierce partie qui se fait passer pour une entité légitime (émission ou réception non autorisée).
- Techniques utilisées:
  - *Some Thing you Know* : mot de passe
  - *Some Thing you Have* : carte à puce
  - *Some Thing you Are* : empreinte digitale
  - Signature numérique

4

Objectifs de la sécurité informatique

- Intégrité:
  - Détecter si les données ont été modifiées depuis la source vers la destination
  - Techniques utilisées: cryptage, signature numérique, contrôle d'accès
- Non répudiation:
  - Empêche l'émetteur ou le receveur de nier avoir transmis ou reçu un message.
  - Techniques utilisées: signature numérique

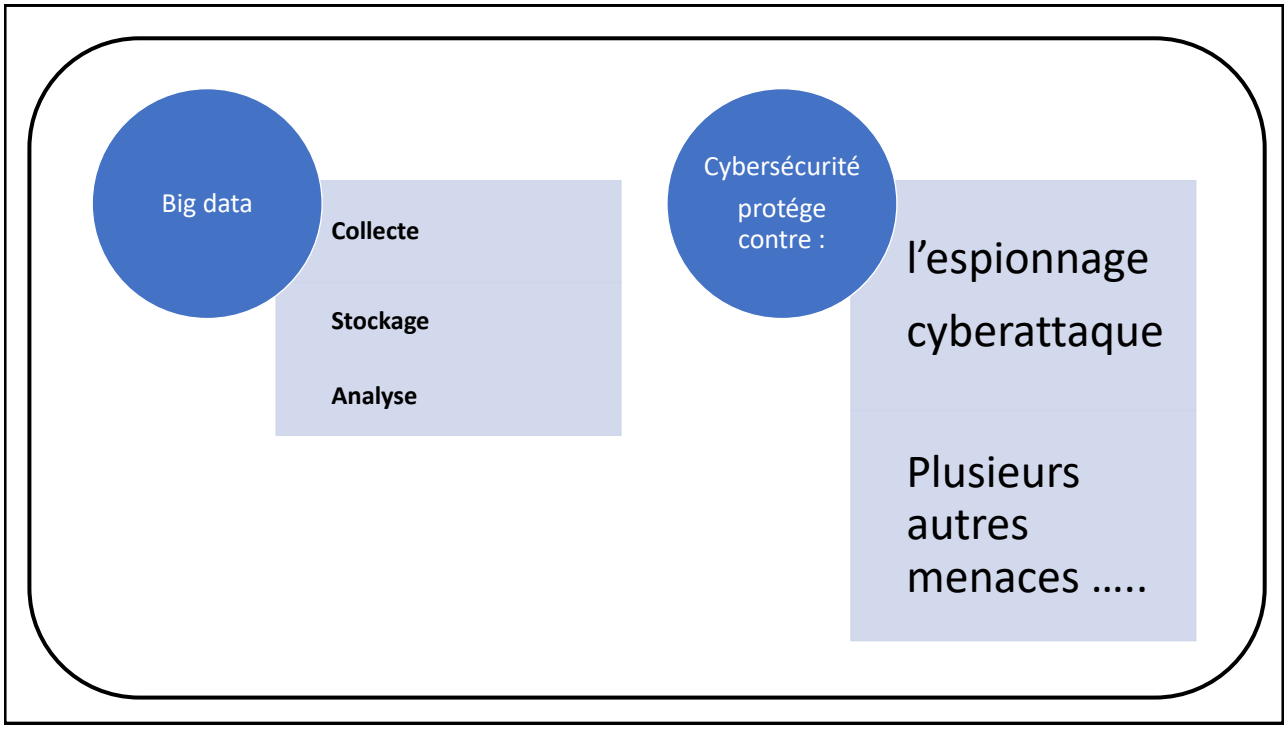
5

Objectifs de la sécurité informatique

- Contrôle d'accès: Empêcher l'utilisation non autorisée d'une ressource
  - Définir qui a le droit d'accéder aux ressources ?
  - Déterminer sous qu'elles conditions ceci peut avoir lieu ?
  - Définir ce qu'il est alloué de faire ?
- Disponibilité : Concept permettant de s'assurer que l'information et les services sont accessibles lorsqu'ils sont demandés.
  - Mécanismes utilisés :
    - Redondance
    - Sauvegardes
    - Partage de charge « load balancing »

15

6



7

Mécanismes de sécurité

- Cryptage
  - Utilisation d'algorithmes mathématiques pour transformer les messages en une forme non intelligible.
  - La transformation dépend d'un algorithme et de clés.
- Signature numérique
  - Ajout de données, ou transformation cryptographique irréversible, à une unité de données afin de prouver la source et l'intégrité de cette unité de données.
- Échange d'authentification
  - Mécanisme assurant l'identité d'une entité à travers un échange d'information.

56

8

Mécanismes de sécurité

- Notarization:
  - Utilisation d'une tierce partie afin d'assurer certaines propriétés liées à un échange de données.
- Horodatage (Timestamping)
  - Inclusion d'une date et d'un temps correct dans un message.
- Mécanismes non cryptographiques:
  - Détection d'intrusions
  - Implémentation de Firewalls
  - Traçabilité (garder un historique des événements)

57

9

La cryptographie

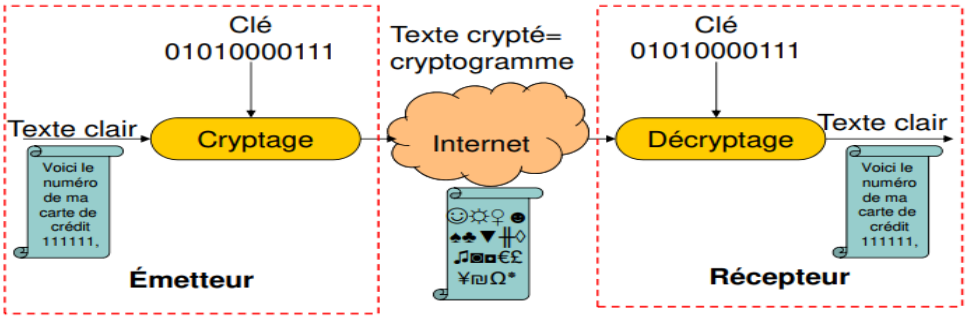
Un crypto-système est décrit par cinq uplets (P,C,K,E,D), satisfaisant ces conditions:

- «P» est un ensemble fini de textes clairs (plain text)
- «C» est un ensemble fini de textes cryptés (cypher text)
- «K» est l'espace de clés (*key space*), représente un ensemble fini de clés possibles.
- Pour chaque k € K, il existe une fonction cryptage e_k € E, et une fonction de décryptage correspondante d_k € D
  - Les fonctions e_k : P→C et d_k : C→P doivent satisfaire: $d_k(e_k(x))=x$ pour chaque x € P
- Crypto-système
  - Les crypto-systèmes symétriques
  - Les crypto-systèmes asymétriques
  - Les fonctions de hashage

10

La cryptographie symétrique

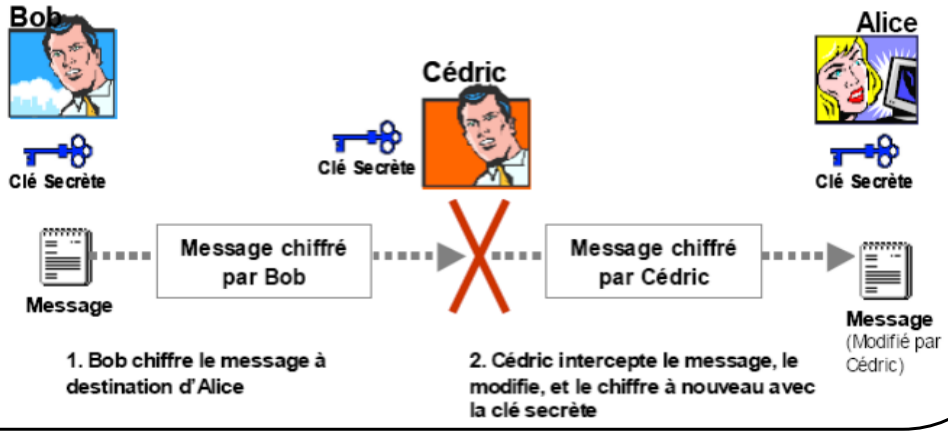
- Les deux parties communicantes utilisent un algorithme symétrique et une même clé pour crypter et décrypter les données
- Une ***clé symétrique*** appelée aussi ***clé de session*** est une séquence binaire aléatoire dont la longueur dépend de l'algorithme
- Un algorithme est une séquence de transformations sur les données et la clé



11

Le cryptage symétrique

- Limitation: Pas d'intégrité et d'identification de l'auteur
- Si Alice, Bob et Cédric partage le même lien de communication alors ils partagent la même clé de chiffrement symétrique.



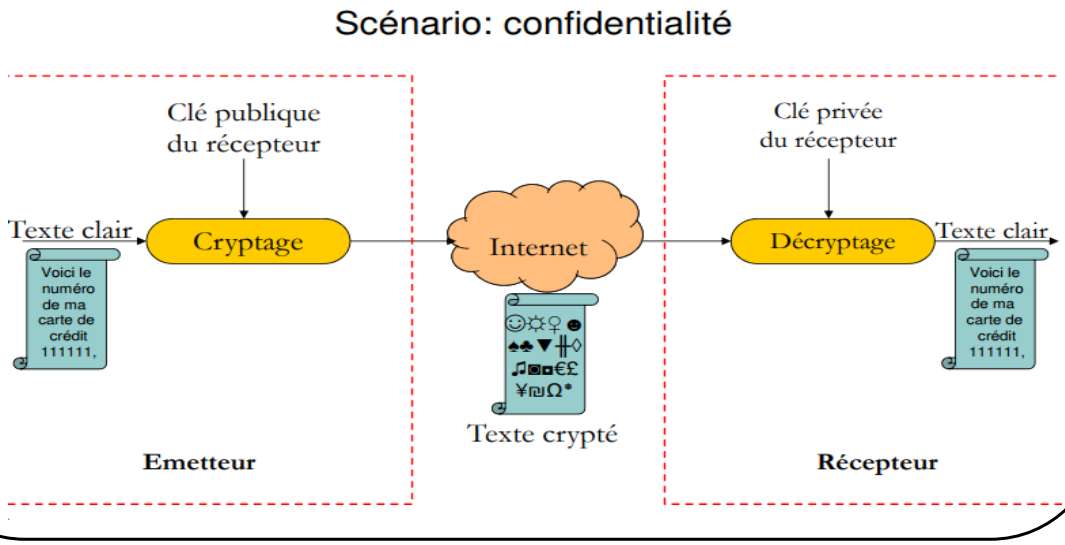
12

Le cryptage asymétrique

- Utilisation d'une paire de clés:
  - Publique: Connue par tout le monde, utilisée généralement pour **crypter** ou **vérifier** la signature des messages.
  - Privée: Connue uniquement par le détenteur, utilisée pour **décrypter** et **signer** des messages.
- Impossible de trouver la clé privée à partir de la clé publique.
- Exemples: RSA, Diffie-Hellman
- Généralement dix fois plus lent que le cryptage symétrique.
- Utilisé généralement pour
  - Cryptage / décryptage: assurer la confidentialité.
  - Signature numérique: assurer l'authentification et la non répudiation.
  - Distribution de clés: se mettre d'accord sur une clé de session.
- Clés à grande taille (ex: RSA: 1024-2048-…)

13

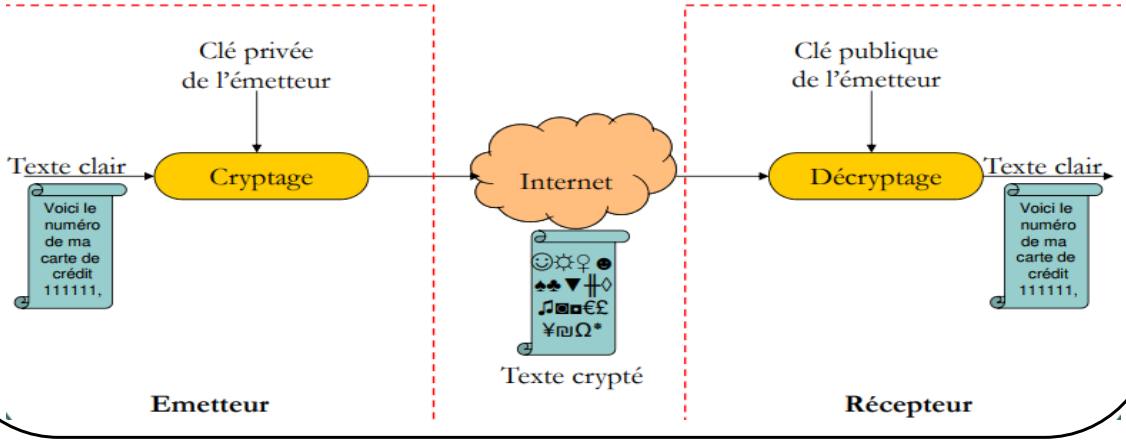
Cryptage asymétrique



14

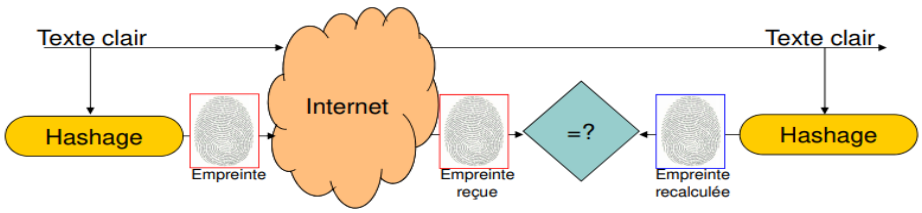
Cryptage asymétrique

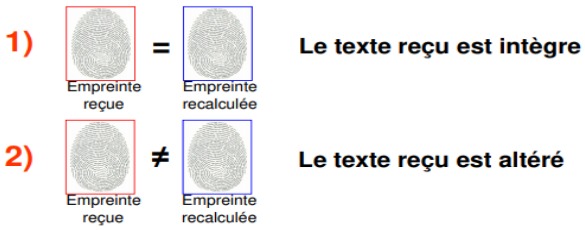
Scénario: authenticité de l'émetteur et non répudiation d'envoi



15

Fonction de hachage : principes





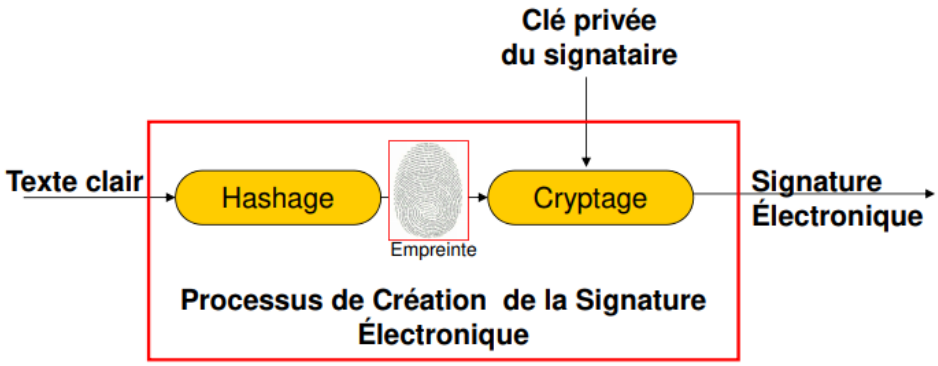
16

Signature numérique

- Idée clé:
  - Le *Hash* (résultat de la fonction de hachage) d'un message est crypté avec la clé privée de l'émetteur.
  - La clé publique est utilisée pour la vérification de la signature
- Soit:
  - M: message à signer, H: fonction de hachage
  - Kpr, Kpu: paire de clés privée / publique de l'émetteur.
  - E / D: fonction de cryptage / Décryptage en utilisant Kpu / Kpr.
- En recevant $(M, E_{Kpr}(H(M)))$, le récepteur vérifie si: $H(M)=D_{Kpu}(E_{Kpr}(H(M)))$

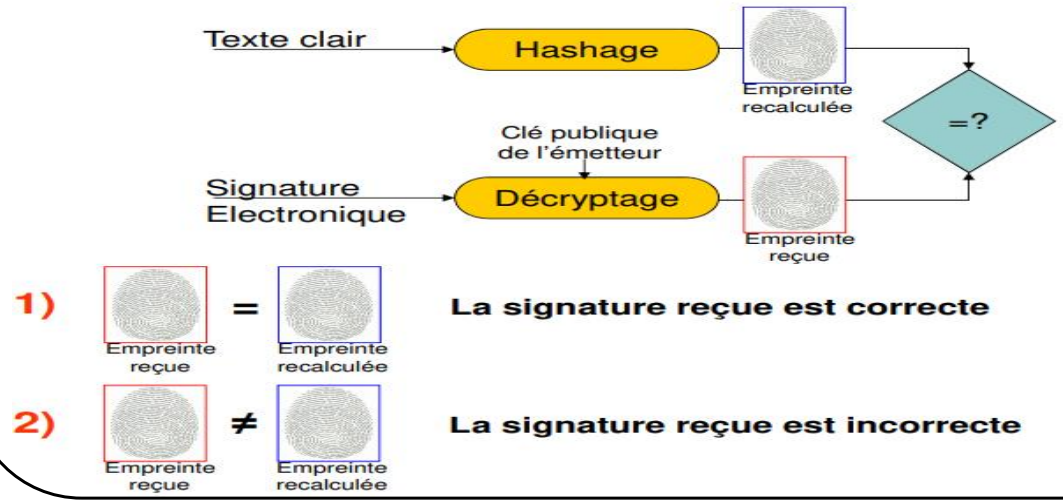
17

Signature numérique : création



18

Signature numérique : vérification



19

Signature numérique

- La signature permet de mettre en œuvre les services:
  - Intégrité du message
  - Authentification
  - Non-répudiation
  - Génération d'une clé de chiffrement symétrique pour le service de Confidentialité

20