IUT ANNECY
UNIVERSITÉ SAVOIE MONT BLANC

Cryptographie et sécurité

Cours 3: Hachage

Mickaël Bettinelli
(mickael.bettinelli@univ-smb.fr)

Prérequis et objectifs

Compétences maîtrisées à la fin du cours:

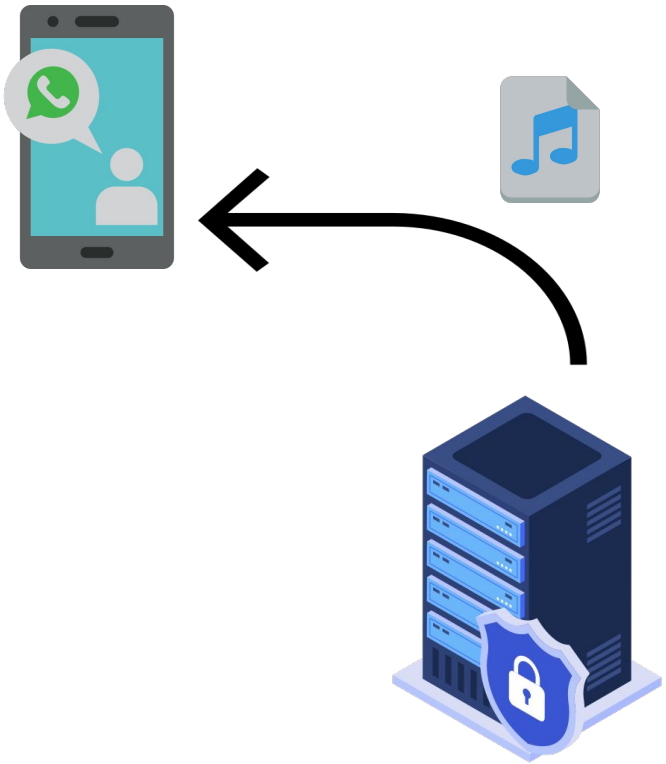
- Connaître le concept de fonction de hachage (rappel)
- Savoir comment utiliser les fonctions de hachage pour vérifier l’intégrité d’un fichier
- Implémenter des fonctions de hachage pour sécuriser ses applications

Sommaire

1. Les fonctions de hachage en théorie
2. Vérifier l’intégrité d’un fichier

Problématique

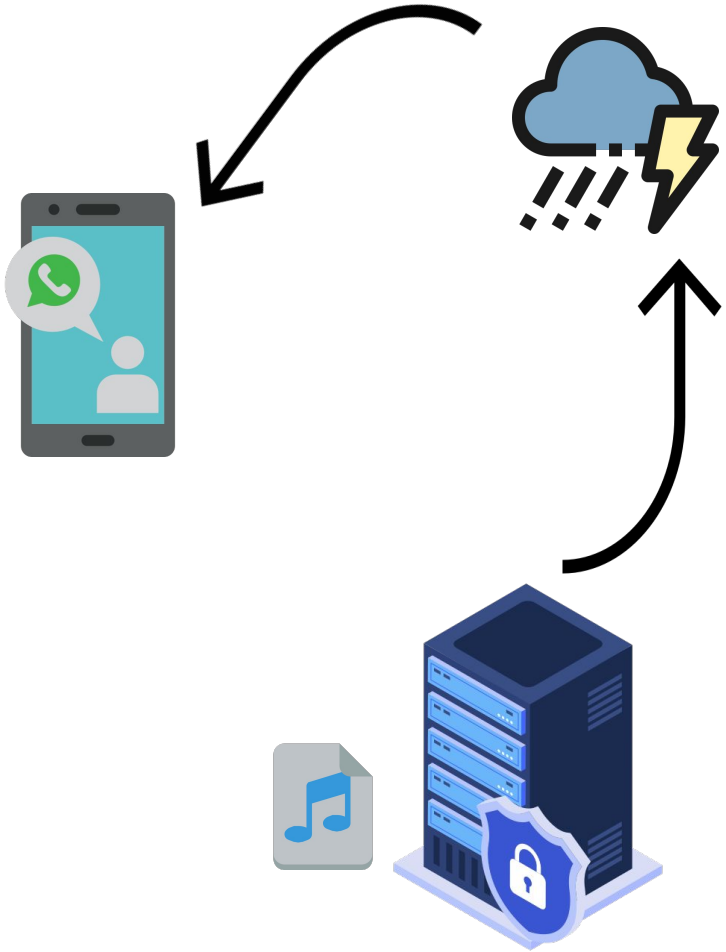
Cas d’étude:
Envoie d’un fichier d’un serveur à un client.



Problématique

Problème: *corruption de fichiers (erreur de transmission, erreur logicielle, etc.)*

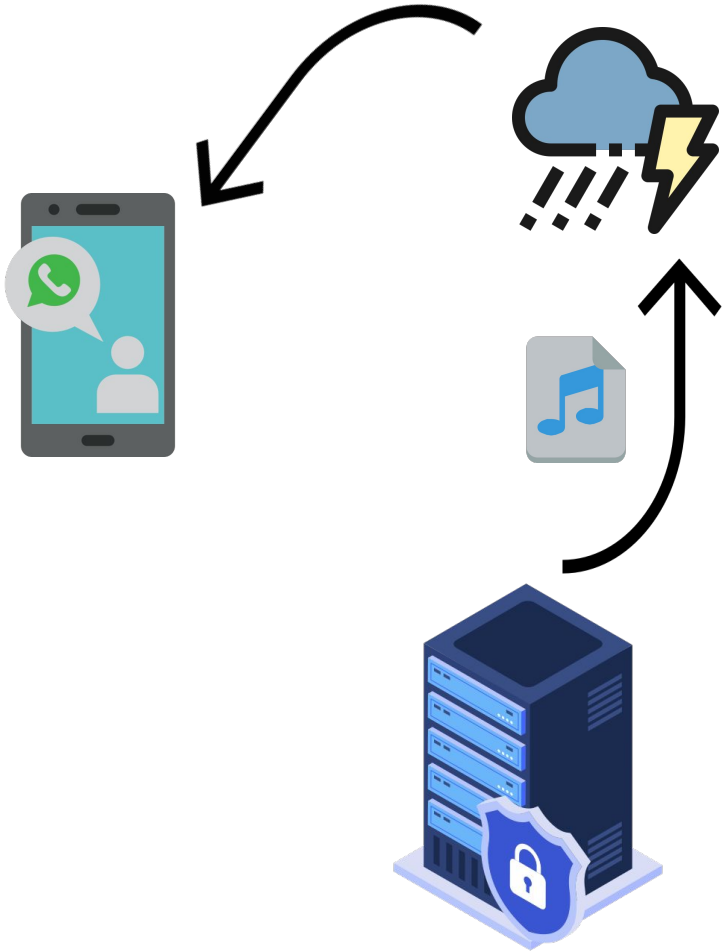
Les communications sont constamment soumises à du bruit pouvant altérer les messages.



Problématique

Problème: *corruption de fichiers (erreur de transmission, erreur logicielle, etc.)*

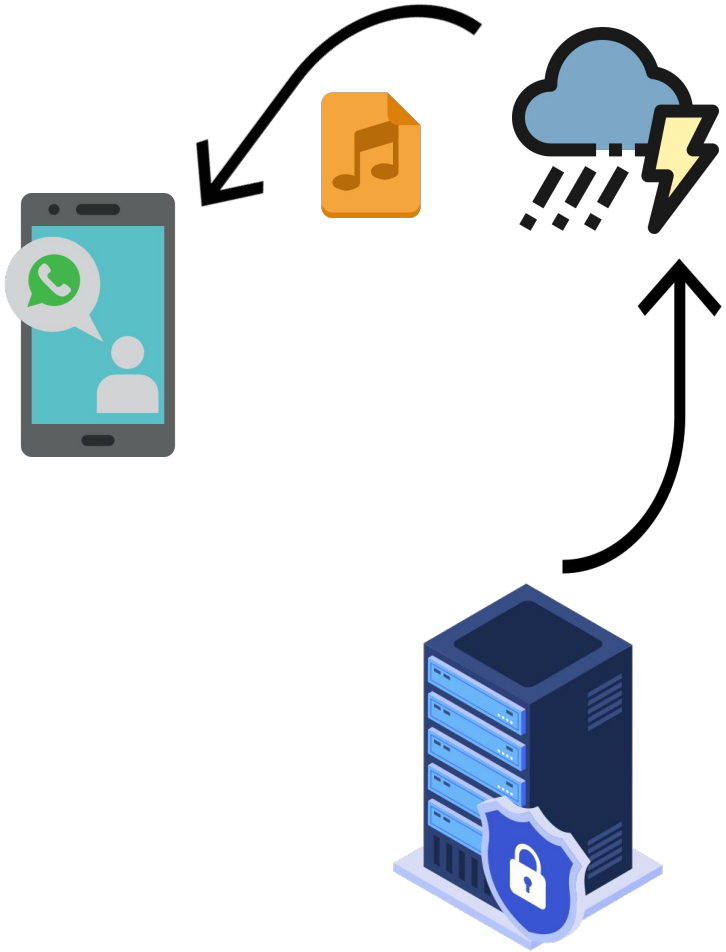
Le fichier peut être victime du bruit ou d’une erreur logicielle au moment de l’envoie.



Problématique

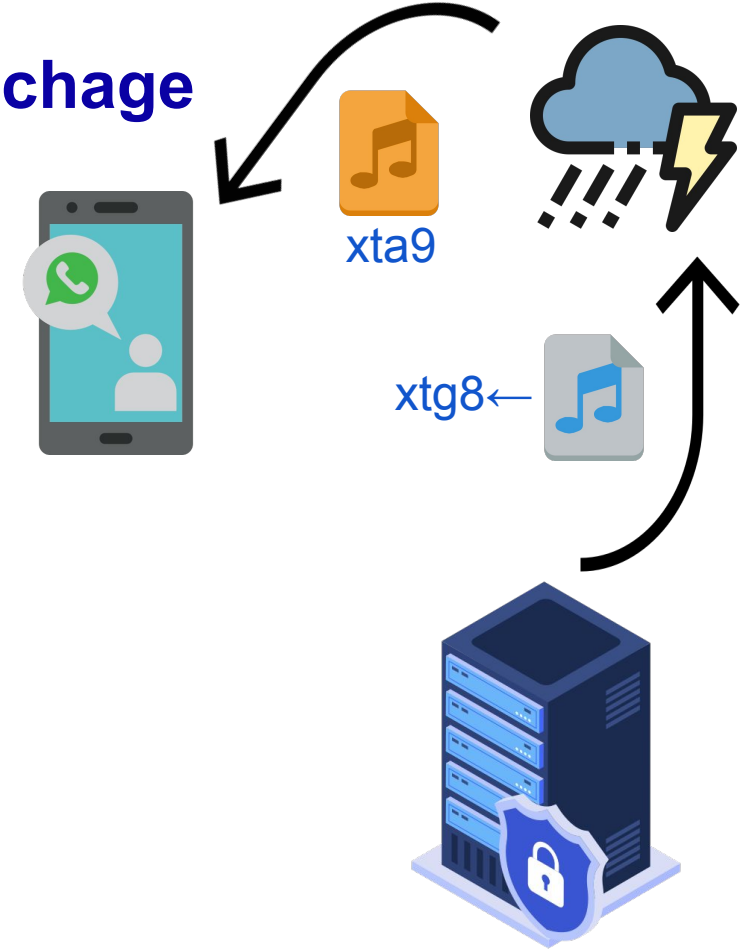
Problème: *corruption de fichiers (erreur de transmission, erreur logicielle, etc.)*

Et peut être différent au moment de sa réception par le client.



Solution : les fonctions de hachage

Elles permettent de **calculer l'empreinte d'un fichier.**
Chaque fichier a une **empreinte unique**.



Solution : les fonctions de hachage

Elles permettent de **calculer l'empreinte d'un fichier.**
Chaque fichier a une **empreinte unique**.

Les caractéristiques des fonctions de hachage.

1. Fonction à sens unique: impossible de déchiffrer une empreinte
2. **Déterminisme**: hacher deux fois le même message conduit au même résultat
3. **Unicité de la signature**: un même message va correspondre une signature unique

Solution : les fonctions de hachage

Comment vérifier qu'un fichier n'a pas été modifié par un tiers ?

1. Le créateur du fichier calcule son empreinte et l'envoie au destinataire
2. Le destinataire télécharge le fichier
3. Le destinataire re-calcule l'empreinte du fichier et la compare à l'empreinte calculée par le créateur

Quelques exemples de fonctions: MD5, SHA1, SHA3

MD5 (Message Digest) - dépréciée

- Inventé par Ronald Rivest en 1991
- Empreintes de 128 bits, avec une forte probabilité que deux haches soient différents
- En 1996, une faille permet de créer des collisions à la demande

Fonctionnement général.

1. Découpe du message en blocs de 512 bits
2. Effectue 64 séries d'opérations AND, XOR, OR, ROT, ADD sur chaque blocs
3. Produit une empreinte condensée de 128 bits

SHA-1 (Secure Hash Algorithm) - dépréciée

Caractéristiques:

- Inventé par la NSA (National Security Agency) en 1995
- Empreintes de 160 bits

Fonctionnement général.

1. Découpe du message en blocs de 512 bits
2. Effectue 80 séries d'opérations AND, XOR, OR, ROT, ADD sur chaque blocs
3. Produit une empreinte condensée de 160 bits

SHA-3

Caractéristiques:

- Inventé en 2015
- Empreintes de 224 à 512 bits selon la version de SHA-3
- SHA-3 se distingue des versions précédentes par une nouvelle méthode de hache

Fonctionnement général.

1. Découpe du message en blocs de 512 bits
2. Effectue 24 séries d'opérations AND, XOR, ROT sur chaque blocs
3. Produit une empreinte condensée de 1600 bits

En résumé

2 familles de fonctions de hachage:

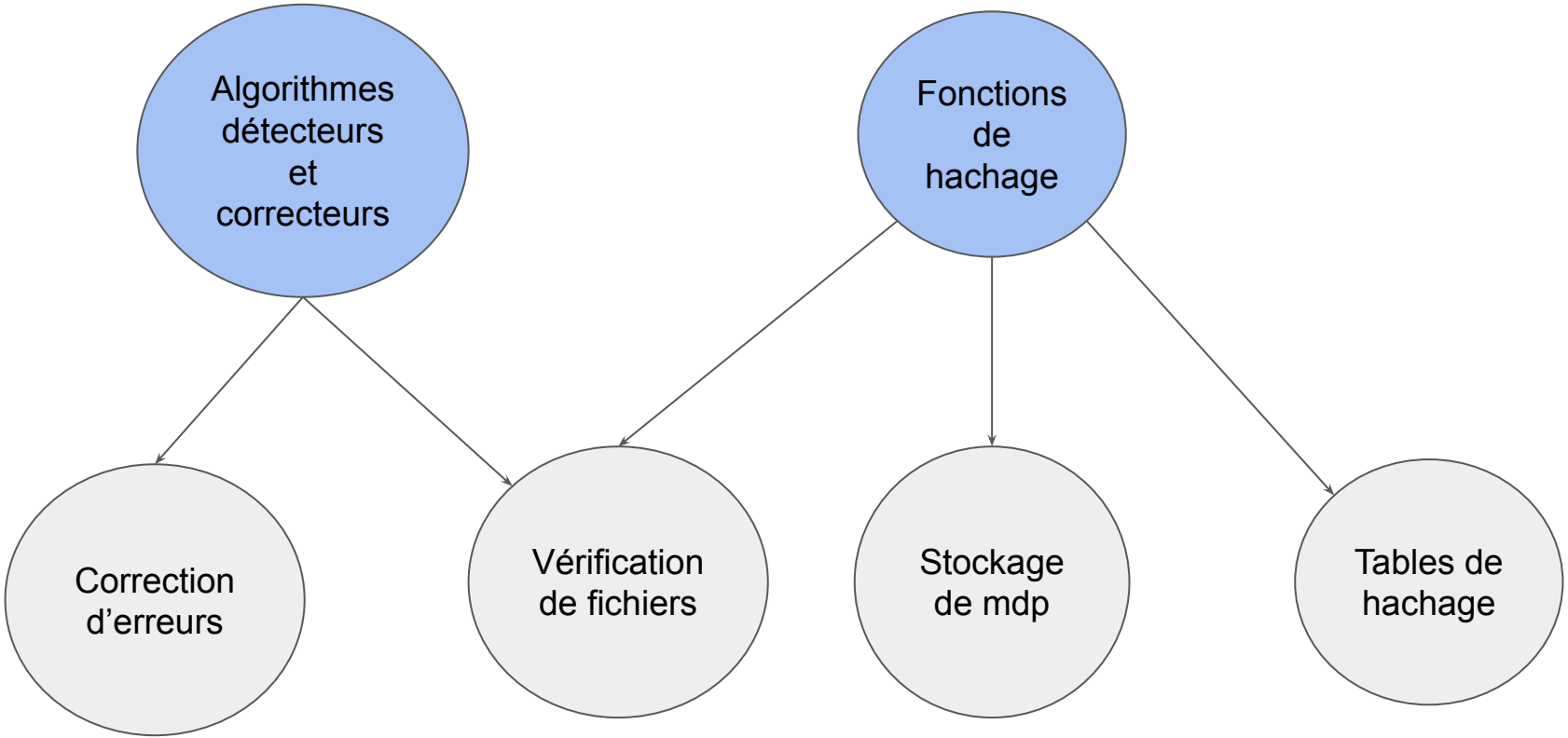
- MD (Message Digest):
  - Plus rapide que les algorithmes SHA
  - Peu sécurisé
- SHA (Secure Hash Algorithm):
  - Fonctionnement plus complexe et plus lent
  - Plus sécurisé que MD5

Méthodes alternatives

Les méthodes de détection et de correction d’erreur:

Le CRC et le code de Hamming permettent également de générer une empreinte !

Identification des concepts



Quelle méthode utiliser dans votre application ?

Les méthodes MD* et SHA* sont plus sécurisées contre des attaques humaines.

Les méthodes CRC* sont plus efficaces pour repérer des erreurs de bruit / logicielles.

A vous de choisir :-)

Sondage

On fait quoi durant la séance du 3 avril ?

1. Une introduction à la blockchain (+ petit projet)
2. Une séance de plus pour terminer l’app, rédiger le rapport et ajouter des features

Ressources complémentaires

- https://en.wikipedia.org/wiki/Hash_function
- https://www.youtube.com/watch?v=KyUTuwz_b7Q&ab_channel=ComputerScience
- Distributed Systems, Marteen Van Steen, 2023 (chapitre 9: cybersécurité)