Une Attaque : n’importe quelle action qui compromet la sécurité des informations.

Mécanismes de Sécurité : un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.

Service de Sécurité : un service qui augmente la sécurité des traitements et des échanges de données d’un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

Définitions des Services de Sécurité

Voici quelques définitions informelles à retenir concernant les services de sécurité les plus importants

Authentification Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée.

Confidentialité

Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables

Contrôle d'intégrité

Permet de vérifier qu’une donnée n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)

Contrôle d'accès

Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée

Non répudiation

Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication

Introduction à la cryptographie

Cette partie du cours introduira les mécanismes de base de la cryptographie moderne qui permettent de réaliser quatre services de sécurité fondamentaux :

1. La confidentialité
2. L'intégrité des données
3. L'authentification de l'origine de données
4. La non-répudiation de l'origine

Pour chacun de ces services nous rappellerons la définition puis nous introduirons le mécanisme cryptographique permettant de le réaliser.

La cryptographie

Le mot « Cryptographie » est composé des mots grecques :

- CRYPTO = caché
- GRAPHY = écrire

C'est donc l'art de l'écriture secrète.

C'est une science permettant de préserver la confidentialité des échanges.

Cryptanalyse

La cryptanalyse est l'art de décrypter des messages chiffrés.

Objectifs

Parmi les objectifs de la cryptographie :

- Garantir la confidentialité
- Vérifier l'intégrité des données
- Gérer l'authentification

1.Confidentialité et chiffrement

Confidentialité La confidentialité est la propriété qui assure que l'information est rendu inintelligible aux individus, entités, et processus non autorisés.

Définition : Chiffrement / déchiffrement

Le chiffrement est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire. Le déchiffrement est l'opération qui permet de restaurer le message original à partir du message chiffré.

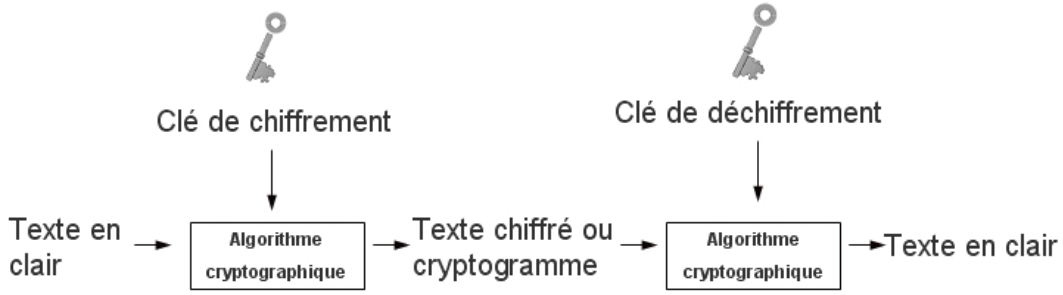
Clé de chiffrement

Dans la cryptographie moderne, l'habilité de maintenir un message chiffré secret, repose non pas sur l'algorithme de chiffrement (qui est largement connu), mais sur une information secrète dite CLE qui doit être utilisée avec l'algorithme pour produire le message chiffré.

Selon que la clé utilisée pour le chiffrement et le déchiffrement est la même ou pas, on parle de système cryptographique symétrique ou asymétrique.

Chiffrement symétrique

Dans le chiffrement symétrique, une même clé est partagée entre l'émetteur et récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour chiffrer message te par le récepteur pour le déchiffrer en utilisant un algorithme chiffrement symétrique.



Algorithmes de chiffrement symétriques

Il existe deux types d'algorithmes de chiffrement symétrique :

1. Chiffrement par bloc : division du texte clair en blocs fixe, puis chiffrement bloc par bloc

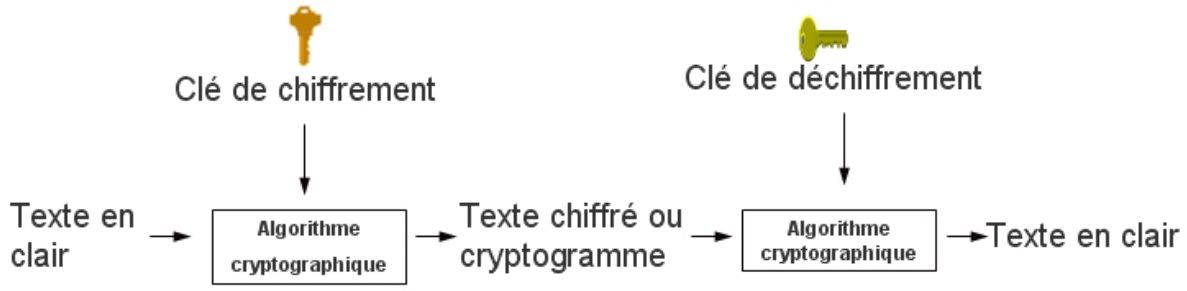
   - DES: Data Encryption Standard IBM, Standard NIST 1976
   - 3DES: W. Diffie, M. Hellman, W. Tuchmann 1978.
   - IDEA International Data Encryption Algorithm: Xuejia Lai et James Massey en 1992
   - Blowfish: Bruce Schneier en 1993
   - AES Advanced **Encryption** Standard (Rijndael): Joan Daemen et Vincent Rijmen 2000

2. Chiffrement par flux : le bloc a une dimension unitaire (1 bit, 1 octet, ...), ou une taille relativement petite

   - RC4 Rivest Cipher 4: Ron Rivest 1987
   - SEAL Software-optimized Encryption Algorithm: Don Coppersmith et Phillip Rogaway pour IBM 1993.

Chiffrement asymétrique

Dans un système asymétrique, le récepteur génère une paire de clés asymétrique : une clé publique qui est diffusée à tout le monde et une clé privée maintenue secrète chez le récepteur. La particularité de cette paire de clé est que tout message chiffrée avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante. D'où la confidentialité des messages chiffré avec la clé publique d'un récepteur. Bien évidemment la clé privée correspondante ne peut être calculée à partir de la clé publique correspondante.



Algorithmes de chiffrement asymétrique

- RSA: Rivest, Shamir et Adleman 1978
- Diffie et Hellman 1976

Intégrité de données :

C'est la propriété qui permet de vérifier qu'une donnée n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement).

Une fonction de hachage est typiquement utilisée pour vérifier l'intégrité de données.

Fonction de hashage cryptographique

Une fonction de hashage associe à une chaîne binaire (de longueur variable) une chaîne de longueur fixe

Une fonction de hashage cryptographique a les propriétés suivantes :

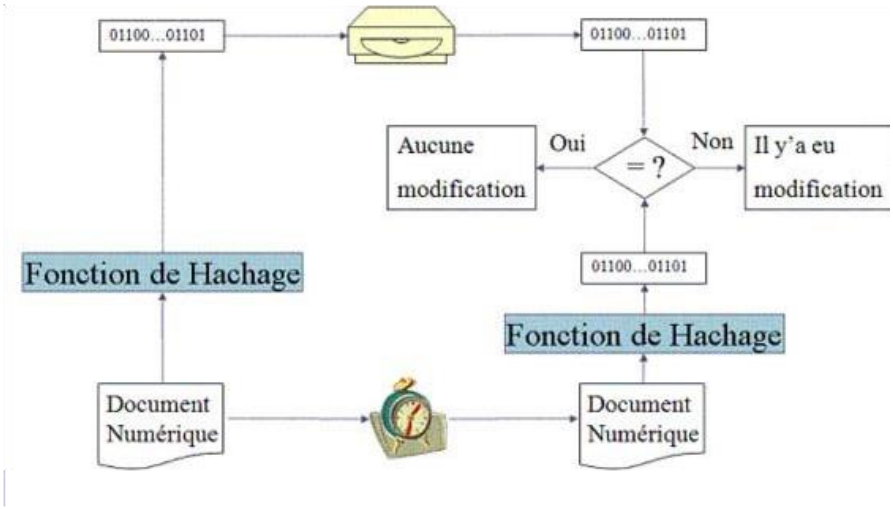
- Étant donné m, il est facile de calculer h(m)
- Étant donné h, il est difficile de calculer m tel que h(m)=h
- Étant donné m, il est difficile de trouver un autre message, m', tel que h(m)=h(m').

Comment utiliser une fonction de hashage pour contrôler l'intégrité de données.

La figure ci-contre illustre comment utiliser une fonction de hashage pour vérifier l'intégrité d'un document numérique.

Initialement le code de hashage du document numérique est calculé et stocké dans un endroit sûre. Ultérieurement ce code est recalculé et comparé à celui qui a été stocké.

Si les deux valeurs sont égales alors le document n'a pas été modifié. Sinon, le document a subit une modification.



Il existe plusieurs fonctions de hashages ; En voici quelques unes :

•MD2 (Message Digest 2) : Opère sur des bloques de 16 octets, manipule des mots de 8 bits Output 128 bits.

•MD4 (Message Digest 4) : Manipule des mots de 32 bits, plus performant sur des processeurs 32 bits.

•MD5 (Message Digest 5) : Une passe de plus / MD4, plus sûre

•SHA-1 (Secure Hash Algorithm) : Proposé par le NIST Input message 2^{64} octets (au max), output 160 bits.

Authentification de l'origine de données

C'est la propriété qui permet de vérifier que la source de données est bien l'identité prétendue.

Définition : Message Authentication Code (MAC)

C'est est un mécanisme cryptographique qui permet de vérifier l'authenticité de l'origine des données et leur intégrité en même temps.

Un MAC est une famille de fonctions hk paramétrée par une clé secrète k avec les propriétés suivantes :

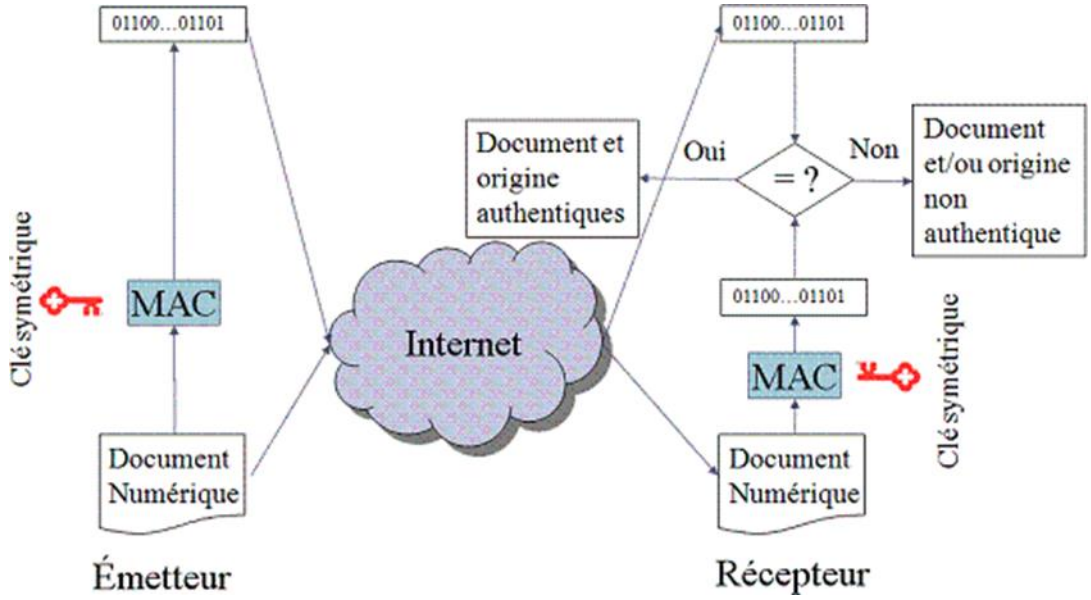
- Étant donné une clé k et un message m, hk(m) est facile à calculer,
- Étant donné zéro ou plusieurs paires (mj,hk(mj)), il est très difficile de calculer n'importe quelle paire (m,hk(m)) pour n'importe quel message m.

Méthode : Comment utiliser un MAC pour garantir l'authentification d l'origine

Pour garantir d'authenticité de l'origine, l'émetteur et le récepteur doivent partager une clé symétrique.

Cette clé sera utilisée par l'émetteur pour calculer un MAC sur le message à envoyer. Ce MAC (code de hashage) est la preuve d'authenticité qui accompagnera le message.

Le récepteur utilisera la même clé secrète pour calculer le MAC de nouveau sur le message reçus. Le MAC nouvellement calculé sera comparé au MAC accompagnant le message. Si les deux valeurs sont égales alors le message et l'origine sont authentiques. Sinon, soit le message ou l'origine n'est pas authentique.



Non-répudiation de l'origine

La non répudiation de l'origine assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur.

La signature digitale

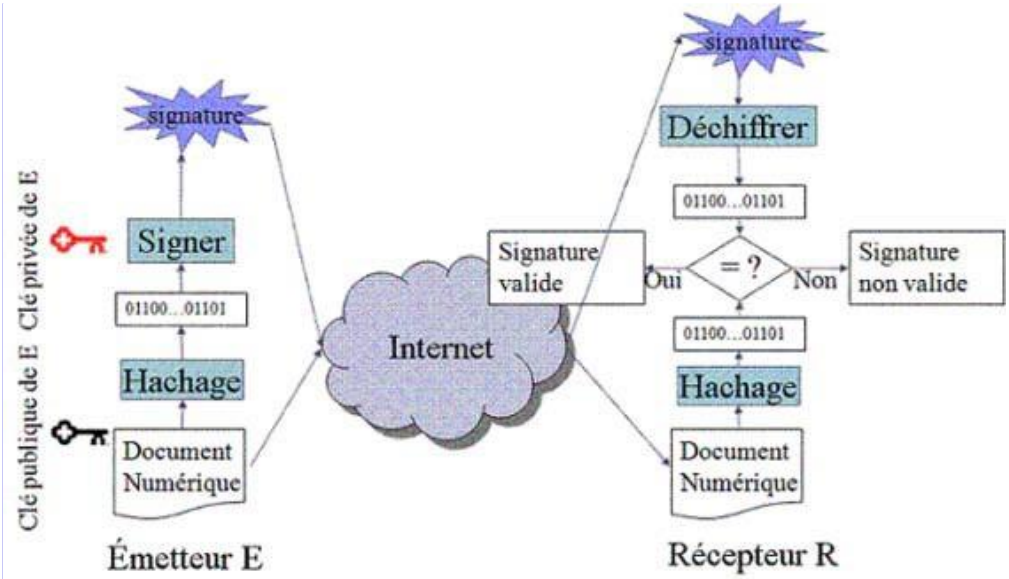
La signature digitale est un mécanisme cryptographique qui permet d'assurer la non répudiation de l'origine.

Ce mécanisme repose sur un système cryptographique asymétrique La signature est calculée en utilisant la clé privée de l'émetteur La signature est vérifiée en utilisant la clé publique de l'émetteur

Comment utiliser la signature digitale pour assurer la non- répudiation de l'origine ?

L'émetteur du message génère sa paire de clés (publique, privée). Il diffuse sa clé publique te maintient sa clé privée secrète. Pour signer un document l'émetteur commence par calculer le code hashage du document puis signe ce code de hashage avec sa clé privée. Le résultat de cette dernière opération (chiffrement avec clé privée dans le cas de RSA) est la signature digitale qui accompagnera le document. Quand le récepteur reçoit le message et la signature digitale, il recalcule le code de hashage, déchiffre la signature avec la clé publique de l'émetteur et compare les deux codes de hshages. Si les deux codes sont similaires alors la signature est valide.

L'émetteur ne pourra pas nier dans le futur avoir émis le message puisque y a que lui qui peut générer la signature digitale avec sa clé privée secrète.



Signature digitale et non-répudiation