Généralités sur la cryptographie

Introduction

Dans ce chapitre nous commençons par les concepts de base de la cryptographie, ensuite nous allons parler des systèmes de cryptographie moderne à savoir la cryptographie à clé secrète et la cryptographie à clés publiques.
Enfin nous clôturons ce chapitre par les fonctions de hachages et signature numérique.

2.1 Notion de cryptographie

L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : «cryptos », qui signifie caché et « logos » qui signifie mot. La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisé depuis des milliers d'années pour assurer les communications militaires et diplomatiques. par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes [18, 19].
Dans le domaine de l'un de cryptologie peut voir deux visions : la cryptographie et la cryptanalyse.
Le cryptographe cherche des méthodes pour assurer la sûreté et la sécurité des conversations alors que le Crypto analyse tente de défaire le travail ancien en brisant ses systèmes. La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle et la cryptanalyse, à l'inverse est l'étude des procédés cryptographiques, qui dépendent d'un paramètre appelé clé.

La principale mission de la cryptographie est de garantir la sécurité des communications c'est-à-dire de permettre à des entités qui ne se font pas confiance en général de communiquer en toute sécurité en présence de potentiels adversaires (susceptibles entre autres d'accéder à des secrets en violant la confidentialité, d'intercepter et de modifier les informations échangées ou d'usurper des identités lors d'une communication) [1].
Sous l'angle des cryptosystèmes, la cryptographie est composés des systèmes à clés secrète et des systèmes à clés publique.
En cryptographie à clés secrète, une même clés est utilisée pour chiffrer et pour déchiffrer ; en cas de deux clés, on s'assure que chacune d'elles, est facile à calculer à partir

de l'autre (on parle aussi de cryptographie symétrique).
En cryptographie à clés publique, on utilise deux clés dont l'une soit k' est difficile à déduire de l'autre soit k (on parle aussi de cryptographie non symétrique).
La clé k est appelée clé publique et est utilisée pour le chiffrement ou la vérification de signature selon le système ; la clé k' est appelée clé privée et est utilisée pour le déchiffrement ou la signature selon le système .

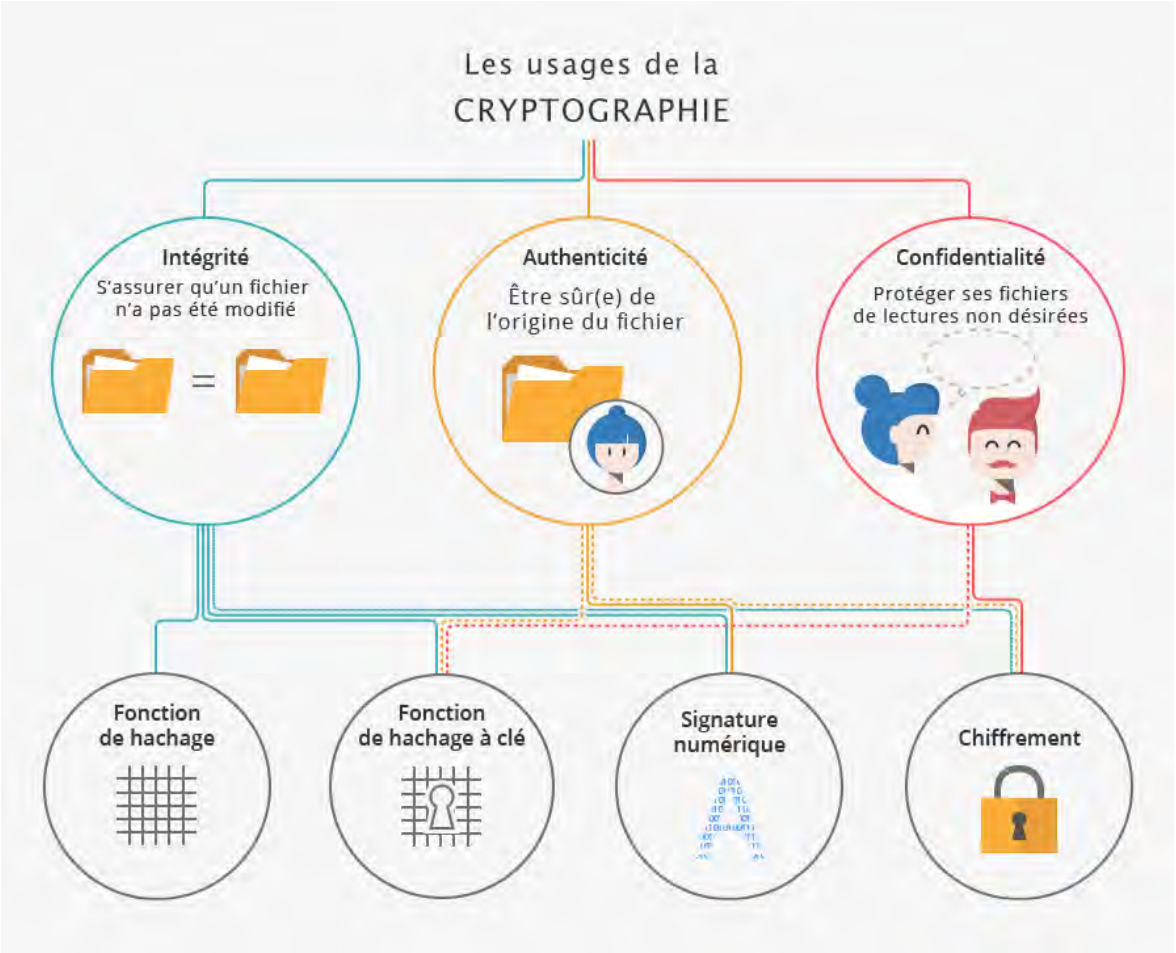

Figure 2.1 – Les usages de la cryptographie (source voir [29])

2.1.1 Repères historiques

- **Age artisanal : (→ 1900)** [9]
  César : chaque lettre est remplacée par celle située trois positions plus loin dans l'alphabet
  Systèmes de substitutions et de permutations basiques
- **Age technique : (1900 → 1970)**
  Substitutions et permutations utilisant des machines mécaniques ou électro-mécaniques : Hagelin, Enigma (2ème guerre mondiale)

- **Age paradoxal (depuis 30 ans)**
  Nouveaux mécanismes répondant à des questions a priori hors d'atteinte Comment assurer un service de confidentialité sans avoir établi une convention secrète commune sur un canal qui peut être écouté par un attaquant ?
  Comment assurer un service d'authenticité basé sur la possession d'un secret sans révéler la moindre information sur le secret ?

2.1.2 Terminologie de la cryptographie

La cryptographie utilise des concepts issus de nombreux domaines (Informatique, Mathématiques, Electronique). Toutefois,les techniques évoluent et trouvent aujourd'hui régulièrement racine dans d'autres branches (Biologie, Physique, etc.)

- **Cryptologie :** C'est une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.
- **Cryptographie :** C'est l'étude des méthodes permettant d'envoyer des données de manière confidentielle sur un support donné.
- **Chiffrement :** Il consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible pour une personne autre que celui qui a créé le message et celui qui en est le destinataire.
- **Texte chiffré :** Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **Texte en clair :** c'est le message à protéger.
- **Déchiffrement :** C'est l'opération permettant de retrouver le texte clair à partir du texte chiffré.
- **Clef :** Il s'agit du paramètre impliqué permettant des opérations de chiffrement ou de déchiffrement.
  Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.
- **Cryptanalyse :** Elle est opposée à la cryptographie et a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Cryptosystème :** Il est défini comme l'ensemble des clefs possibles (espace de clefs), des textes clairs et des textes chiffrés possibles associés à un algorithme donné.

- **Décryptage :** Le déchiffrement désigne l'action permettant de retrouver le texte clair sans connaître la clef de déchiffrement On emploie parfois les termes "cryptage" et "crypter" pour qualifier l'action de chiffrer un message.

- **Cryptographe :** est une personne qui conçoit des cryptosystèmes

- **Cryptanaliste :** est une personne qui tente de casser les cryptosystèmes.

2.1.3 Les services de sécurité de la cryptographie

- **L'authentification** : Garantir l'identité d'une entité (identification) ou l'origine d'une communication ou d'un fichier (authentification de données) **Mécanismes cryptographiques : signature, MAC** [9]

- **La non-répudiation (signature)** : le signataire ne peut pas renier sa signature

- **La confidentialité** : Garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers (GSM,Internet)
Mécanismes cryptographiques : Chiffrement

- **L'intégrité** : Garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié **Mécanismes cryptographiques : signature, MAC**

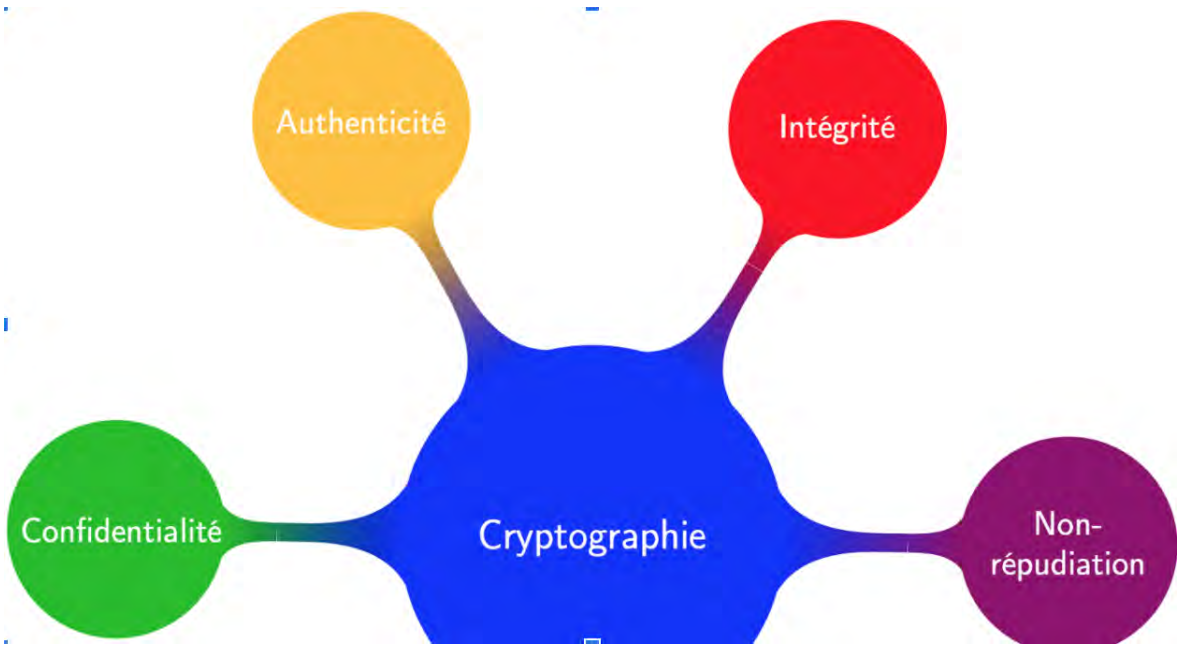

Figure 2.2 – Les services de sécurité de la cryptographie (source voir [17])

2.1.4 Modélisation des systèmes de chiffrement

Un système cryptographique est un ensemble d'algorithmes cryptographiques, de textes clairs, de textes chiffrés et de clés de chiffrement et de déchiffrement. Formellement, un système cryptographique est un tuple $<P, C, K, E, D>$, où :

— P : est un ensemble de textes clairs ;
— C : est un ensemble de textes chiffrés ;
— K : est un ensemble de clés d'encryption/décryption ;
— $\varepsilon = \{E_k : k \in K\}$: est un ensemble de fonctions d'encryption $E_k : P \longrightarrow C$;
— $D = \{D_k : k \in K\}$: est un ensemble de fonctions de décryption $D_k : C \longrightarrow P$.

tel que pour tout $k \in K$, il existe $k' \in K$ tel que $D'_k(E_k(p)) = p$ pour tout $p \in P$.

2.2 Cryptographie à clé secrète (ou symétrique)

Les clés de chiffrement (K_E) et de déchiffrement (K_D) sont identiques : $K_E = K_D = K$, cette clé est le plus souvent appelée « secrète ».
Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clef.
La confidentialité des messages dépend de la confidentialité de cette clé et de la robustesse de l'algorithme utilisé.
Les algorithmes les plus répandus sont le **DES, AES, 3DES**, ...

Avantages

- L'avantage principal de ce mode de chiffrement est sa rapidité ;
- Possibilité de chiffrer des messages de grands tailles ;

Inconvénients

- Le principal désavantage réside dans la distribution des clefs : pour une meilleure sécurité, on préfèrera l'échange manuel ;
- Malheureusement, pour plusieurs communicants,le nombre de clés peut devenir conséquent. En effet, pour un système à N utilisateurs, il y aura $N(N-1)/2$ paires de clefs ;
- Un seul service est garanti (Confidentialité)
- Problème d'authentification, de non-répudiation et d'intégrité

Schéma du système symétriqu

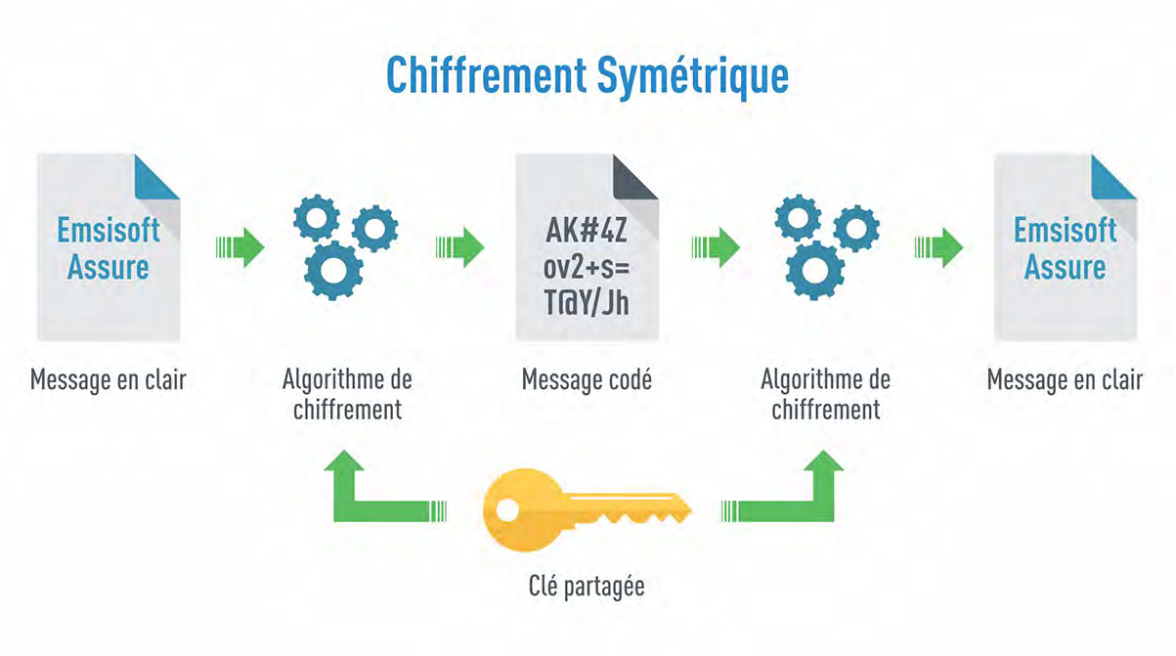

Figure 2.3 – Schéma du système symétrique (source voir [3])

2.3 Cryptographie à clés publiques (ou asymétrique)

La cryptographie à clé publique, ou cryptographie asymétrique, est une méthode de chiffrement qui utilise deux clés qui se ressemblent mathématiquement mais qui ne sont pas identiques :
une clé publique K_pub et une clé privée K_priv.
A l'inverse des algorithmes de cryptographie symétrique qui dépendent d'une seule clé pour le chiffrement et le déchiffrage, les clés de la cryptographie asymétrique ont chacune une fonction bien spécifique :

- la clé publique K_pub sert à chiffrer ou ou vérifier une signature ;
- la clé privée K_priv sert à déchiffrer ou signer ;
- Il est impossible de deviner la clé privée K_priv à partir de la clé publique K_pub.

Schéma du système asymétrique

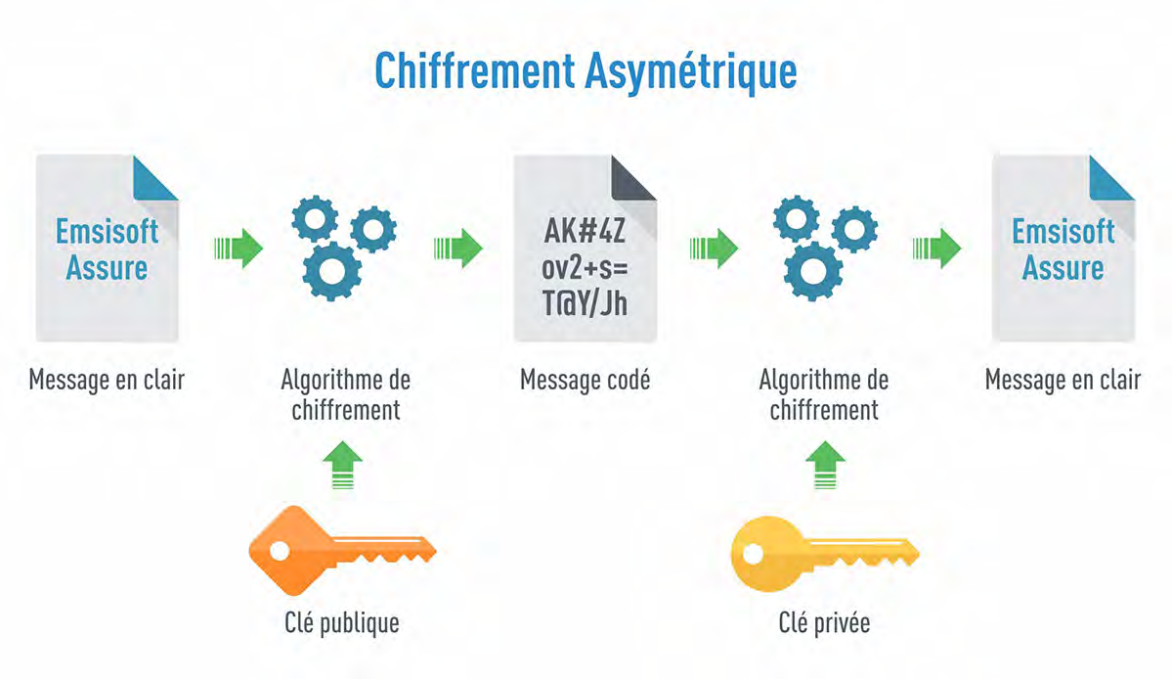

Figure 2.4 – Schéma du système symétrique [3]

L'algorithme de cryptographie asymétrique le plus connu est le RSA, ElGamal, ... La sécurité de tels systèmes repose sur des problèmes calculatoires :

- RSA : factorisation de grands entiers.
- ElGamal : logarithme discret.
- Merkle-Hellman : problème du sac à dos (knapsacks)

2.4 Fonction de hachage et signature

2.4.1 Fonction à sens unique

Définition 2.4.1. *Une fonction $f : X \longrightarrow Y$ est dite à sens unique s'il est "facile" de calculer $f(x)$ pour tout $x \in X$, mais pour tous les éléments $y \in Im(f)$ il est "calculatoirernent presqu'impossible" de trouver un $x \in X$ tel que $f(x) = y$ [12].*

2.4.2 Fonction à sens unique avec trappe

Définition 2.4.2. *Une fonction $f : X \longrightarrow Y$ est dite à trappe si f est une fonction à sens unique telle que : pour tout $y \in Im(f)$ il est possible de trouver $x \in X$ tel que $f(x) = y$ sachant une information additionnelle [12].*

2.4.3 Fonction de hachage [13]

Une fonction de hachage est une fonction publique $h : \{0,1\}^* \longrightarrow \{0,1\}^n$ telle que :

- h transforme un message (binaire) de longueur quelconque en un message de longueur fixe appelé hache ou empreinte,
  (Fonction de Compression) ;
- pour tout $x, h(x)$ est facile à calculer ;
  (Facilement calculable)

h est fonction de hachage en cryptographie en plus elle vérifie les propriétés suivantes :

1. Pour tout y, il est impossible de trouver x tel que $h(x) = y$, **(Fonction à sens unique sans trappe)** ;
2. Pour presque tout x, il est difficile de trouver x' tel que $h(x) = h(x')$, **(Résistante aux collusions)** ;
3. Il est impossible de trouver x, y tels que $h(y) = h(x)$ **(Fortement résistante aux collusions)**.

Fonctions de hachage : Intégrité

Si M est un message alors pour garantir l'intégrité de M, on envoie ou stocke le couple $(M, h(M))$ où $h(M)$ est l'empreinte de M via une fonction de hachage h.
Le message est considéré intègre s'il est bien accompagné par son empreinte qu'on ne peut falsifier.

Fonctions de hachage : Usage

1. assurer l'intégrité ;
2. construire des générateurs aléatoires cryptographiquement sûrs ;
3. pour la modélisation théorique des fonctions à sens unique tel que le modèle de l'oracle aléatoire.

Fonctions de hachage : Algorithmes

Les fonctions de hachages comptent deux familles

— celles utilisant des clés : **MAC (Message Authencation Code)**

— celles n'utilisant pas de clés : **MD (Message Digest)**

Les algorithmes de hachages les plus répandus sont : **SHA1, SHA2, SHA3** [**?**]

2.4.4 Signature numérique : Définition et Propriétés

Définition 2.4.3. *Une signature (digitale-manuelle ou numérique-cryptographique) est un procédé, qui, appliqué à un message, garantit la non répudiation par le signataire et donc réalise les deux objectifs suivants :*

1. *identification unique du signataire,*
2. *et preuve d'accord sur le contenu du document.*

Une signature numérique est un mécanisme de cryptographie utilisé pour vérifier l'authenticité et l'intégrité de données numériques.
Elle doit posséder les propriétés suivantes :

1. unique : dépendre du message signé (employer une information unique propre à l'expéditeur pour empêcher la contrefaçon et le démenti).
2. impossible à usurper : c'est à dire être mathématiquement infaisable à forger (par construction de nouveaux messages pour une signature numérique existante, ou par construction d'une signature numérique frauduleuse pour un message donné).
3. impossible à répudier par son auteur.
4. facile à vérifier (reconnaitre) par un tiers.
5. être relativement facile à générer (produire) et à stocker.

2.4.5 Schéma d'une signature numérique

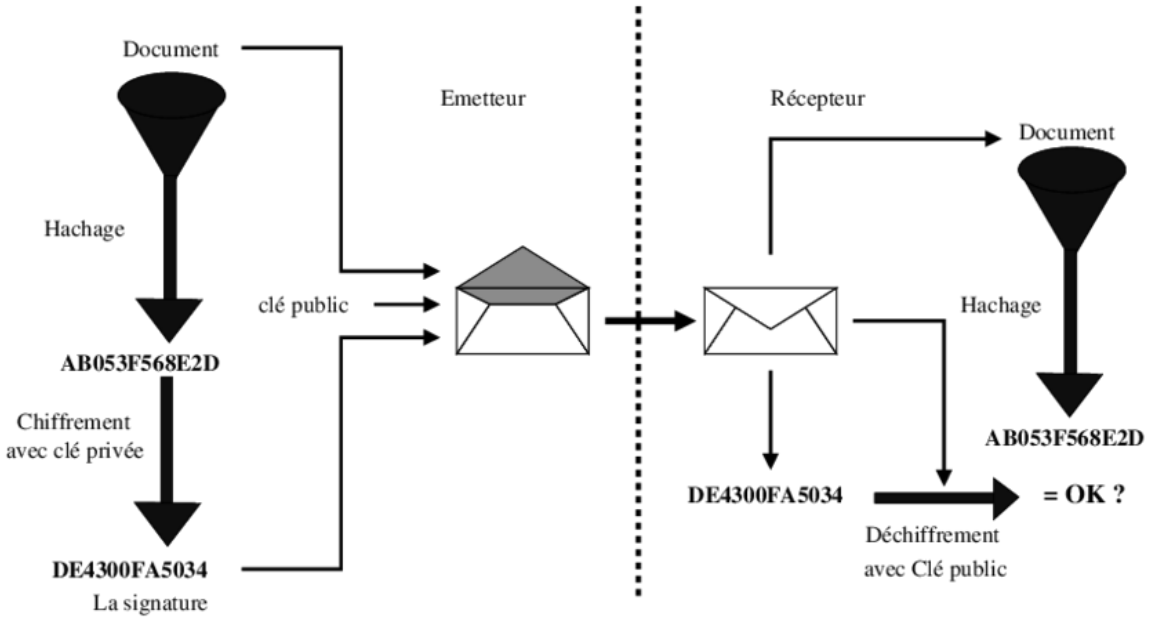

Figure 2.5 – Signature numérique : Schéma

2.4.6 Modélisation d'une signature numérique [13]

Définition 2.4.4. *Un système de signature est composé d'un 6-tuplet* $(P, H, S, S_{k'}, V_k, K)$ *où :*

1. P *est un ensemble appelé espace des textes clairs ;*
2. S *est un ensemble appelé espace des signatures ;*
3. $h : P \longrightarrow H$ *une fonction de hachage ;*
4. K *l'ensemble des paramétres utilisés est l'espace des clés ;*
5. $S_{k'} : H \longrightarrow S$ *est une fonction injective dite fonction de signature (non nécessairement bijective) qui dépend d'un paramètre* k' *appelé clé privée ;*
6. $V_k : P \times S \longrightarrow \{vrai, faux\}$ *est la fonction de vérification de signature binaire telle que* $V_k(m, s) = vrai$ *si et seulement si* $S_{k'}(h(m)) = s$ *(dépendant de la clé publique* k*)*

Pour assurer cette demande, trois méthodes sont possibles :

— chiffrer le message

— utiliser une fonction de hachage

— utiliser un code d'authentification de message (MAC - Message authentication code)