CHAPITRE 5

SIGNATURE NUMÉRIQUE

5.1 Définition

La norme [ISO 7498-2] définit la signature numérique comme des "données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données. Une signature numérique fournit donc les services d'authentification de l'origine des données, d'intégrité des données et de non répudiation.

5.2 Fonctionnement

Supposons qu'Alice souhaite envoyer à Bob un message dont il puisse vérifier l'authenticité. Le message que souhaite envoyer Alice est un fichier binaire **M** de nature quelconque (texte, image, exécutable. . .) qui peut être assimilé à un fichier texte. La description d'une méthode classique de signature par chiffrement asymétrique se résume comme suit :

5.2.1 Mise en place d'une architecture de signature

Alice procède comme suit :

- Choisit un chiffrement asymétrique constitué d'une fonction de chiffrement **C** et d'une fonction de déchiffrement **D** ;
- Choisit une fonction de hachage que nous noterons **H** ;
- Pour le chiffrement choisi, Alice a généré une clé privée K_{pr} et une clé publique K_{pb} ;
- Elle transmet la clé publique K_{pb} et la fonction de hachage **H** à Bob par un canal non sécurisé ;
- Elle garde la clé privée K_{pr} secrète.

5.2.2 Préparation du message signé

Alice prépare le message signé, pour cela :

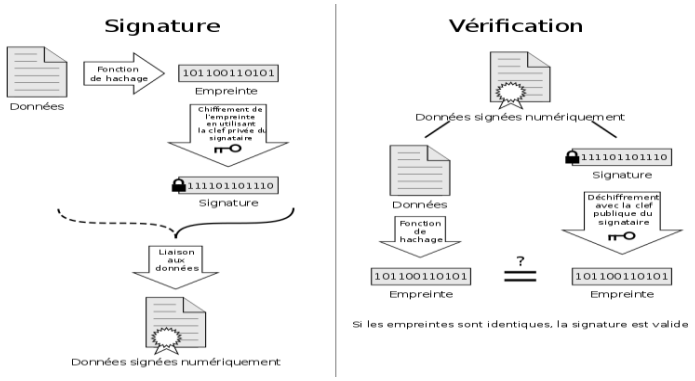
- Elle produit un haché (condensat) du message par la fonction de hachage choisie H(M) ;
- Elle chiffre ce condensat grâce à la fonction de chiffrement **C** en utilisant sa clé privée K_{pr}. Le résultat obtenu est la signature du message : $S(M) = C(K_{pr}, H(M))$;
- Elle prépare le message signé en plaçant le message en clair **M** et la signature **S(M)** dans un conteneur quelconque : M_{signe} =(S(M), M).
- Alice transmet M_{signe},le message signé, à Bob par un canal non sécurisé.

5.2.3 Réception du message signé

Bob réceptionne le message signé. Pour vérifier l'authenticité du message :

- Il produit un haché du texte clair en utilisant la fonction de hachage d'Alice : H(M) ;
- Il déchiffre la signature en utilisant la fonction de déchiffrement **D** avec la clé publique K_{pb} soit : $D_{S(M)} = D(K_{pb}, SM)$;
- Il compare $D_{S(M)}$ avec H(M).
- Dans le cas où la signature est authentique, $D_{S(M)}$ et H(M) sont égaux car, par les propriétés du chiffrement asymétrique : $D_{S(M)} = D(K_{pb}, SM) = D(K_{pb}, C(K_{pr}, H(M))) = H(M)$. Le message est alors authentifié.

Le principe d'un schéma de signature numérique est illustré à la Figure.



5.3 Propriétés des signatures numériques

Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature (propriété d'identification).
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte (propriété d'intégrité).

Pour cela, les conditions suivantes doivent être réunies :

- Authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine ;
- Infalsifiable : la signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre ;
- Non réutilisable : la signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document ;
- Inaltérable : un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier ;
- Irrévocable : la personne qui a signé ne peut le nier.

5.4 Les principaux algorithmes de signature

5.4.1 Signature RSA

- **Génération des paramètres :** Le procédé de génération des paramètres est identique à celui utilisé pour l'algorithme de cryptage RSA, l'expéditeur **A** doit disposer d'une clé publique **(e,n)** et d'une clé privée **(d,n)**.
- **Création de la signature :** Les étapes de la création de la signature numérique du message **M** avec RSA sont :
  - **Etape 1** : calculer le haché de **M** tel que : **h= H(M)** ;
  - **Etape 2** : calculer $S = h^d mod n$;
  - **Etape 3** : envoyer la signature numérique **(M, S)**;
- **Vérification de la signature** : Les étapes de vérification de l'entité **B** de la signature numérique transmise par **A** Sont :
  - **Etape 1** : Calculer du hache h_1, tel que h_1 = H(M) ;
  - **Etape2** : Calculer de $h_2 = S^e mod n$;
  - **Etape3** : Comparer les deux signatures h_1 et h_2, si les deux signatures sont égales, alors le message M est authentique, sinon le message M est altéré.

5.4.2 Signature El-Gamal

- **Génération des paramètres :** Le procédé de génération des paramètres est identique à celui utilisé pour l'algorithme de cryptage El gamal, l'expéditeur A doit disposer d'une clé publique **(A,g, p)**, et d'une clé privée **a**.
- **Création de la signature :** Les étapes de la création de la signature numérique du message **M** avec ElGamal sont :
  - **Etape 1** : calculer **h = H(M)** ;
  - **Etape 2** : Choisir un nombre aléatoire b(b<p et pgcd(b; p-1) = 1) ;
  - **Etape 3** : Calculer les $B = g^b mod p$;
  - **Etape 4** : Calculer **C** tel que $h = (a * B + b * C) mod (p - 1)$;
  - **Etape 5** : envoyer la signature numérique (M;S) tel que S = (B;C).

- **Vérification de la signature :** Les étapes de vérification de l'entité B de la signature numérique transmise par A Sont :
  - Etape 1 : Calculer h1 = H(M) ;
  - Etape 2 : Si $(A^B * B^C)$ mod p = g^h mod p alors la signature est valide.