

---

## Fiche TD N° 3

### Signature numérique & Certification

---

#### Questions de cours

- 1) Citer trois services de sécurité assurés par la signature numérique.
- 2) A quoi sert un certificat à clé publique ?
- 3) Comment vérifier un certificat à clé publique ?
- 4) Quelle est l'utilité d'usage d'une fonction de hachage dans la signature numérique ?
- 5) Comment peut-on évaluer l'efficacité d'une fonction de hachage. ?
- 6) Citer quelques exemples d'algorithmes de hachage.

#### Exercice 2 :

Soit  $(p, q, e) = (17, 31, 7)$  des paramètres RSA,

$H$  étant une fonction de hachage :  $H(x) = x^{150} \bmod 155$ .

Calculer la signature numérique du message  $M = 25$  puis vérifier sa validité.

#### Exercice 3 :

Soit un système hiérarchique de gestion de clés publiques qui possède les caractéristiques suivantes :

- Les clés utilisées sont à base de RSA.
- Tous les utilisateurs du système font confiance à une autorité de certification mère qui porte l'identité 1 et qui possède la clé publique (851, 1643).
- Les certificats sont formatés comme suit :  $[ID_{\text{Autorité}}, ID_{\text{Porteur}}, e_{\text{Porteur}}, n_{\text{Porteur}}, \text{Signature}]$ .
- La fonction de hachage utilisée est définie comme suit :

$$H(ID_{\text{Autorité}}, ID_{\text{Porteur}}, e_{\text{Porteur}}, n_{\text{Porteur}}) = ID_{\text{Autorité}} + ID_{\text{Porteur}} + e_{\text{Porteur}} + n_{\text{Porteur}}$$

- Les certificats de délégation sont définis avec  $e_{\text{Porteur}} = 0, n_{\text{Porteur}} = 0$ .
- L'annuaire du système de certification contient les certificats suivants :

$C_1 = [1, 2, 0, 0, 1346]$  ;  $C_2 = [1, 2, 147, 253, 1333]$  ;  $C_3 = [1, 3, 41, 167, 1060]$  ;  $C_4 = [1, 4, 7, 187, 1150]$  ;  $C_5 = [2, 5, 3, 97, 17]$  ;  $C_6 = [2, 6, 13, 103, 16]$  ;  $C_7 = [2, 7, 11, 143, 146]$  .

- 1) Schématiser l'hierarchie du système en indiquant les autorités de certification.
- 2) Déterminer et vérifier la validité de l'ensemble de certificats nécessaires pour que l'utilisateur 3 puisse vérifier la validité de la clé publique de l'utilisateur 4.
- 3) Même question pour l'utilisateur 3 et l'utilisateur 6.

#### Exercice 4 :

Soit un système complètement distribué de gestion de clés publiques qui possède les caractéristiques suivantes :

- Les clés utilisées sont à base de RSA.
- Les certificats sont formatés comme suit :  
[ ID<sub>Signataire</sub> , ID<sub>Porteur</sub>, e<sub>Porteur</sub>, n<sub>Porteur</sub>, Signature].
- La fonction de hachage utilisée est définie comme suit :

$$H(\text{ID}_{\text{Signataire}}, \text{ID}_{\text{Porteur}}, e_{\text{Porteur}}, n_{\text{Porteur}}) = (\text{ID}_{\text{Signataire}} + \text{ID}_{\text{Porteur}} + e_{\text{Porteur}} + n_{\text{Porteur}}) \bmod 100.$$

- L'annuaire du système de certification contient les certificats suivants :

$$C_1 = [3, 7, 17, 2159, 158] ; C_2 = [2, 6, 31, 1207, 735] ; C_3 = [1, 5, 15, 1411, 487] ;$$

$$C_4 = [1, 6, 31, 1207, 461] ; C_5 = [5, 4, 9, 1819, 1179] ; C_6 = [7, 4, 9, 1819, 600] ; C_7 = [2, 1, 181, 611, 121] ;$$

$$C_8 = [4, 1, 181, 611, 22] ; C_9 = [4, 3, 239, 161, 265] ; C_{10} = [1, 7, 17, 2159, 383] ; C_{11} = [2, 7, 17, 2159, 7] ;$$

$$C_{12} = [6, 5, 15, 1411, 1026].$$

- 1) Schématiser le graphe de confiance ce système.
- 2) Déterminer et vérifier la validité des différentes chaînes de certificats qui permettent à l'utilisateur 6 d'authentifier la clé publique de l'utilisateur 7.