TD9 – Chiffrement asymétrique

Exercice 1. *Attaque sur RSA simple*

On a vu une attaque sur RSA simple dans laquelle l'attaquant demande la signature de deux messages m_1 et m_2, puis calcule un couple valide (m, σ) où $m \notin \{m_1, m_2\}$.

1. Rappeler et détailler cette attaque.
2. Effectuer une variante de cette attaque où l'attaquant n'a besoin de demander la signature que d'un message m' avant de calculer un couple valide (m, σ).

Exercice 2. *Signature RSA rembourrée*

On considère une version *rembourrée* de la signature RSA simple. La génération de clef est identique, et on suppose que (N, e) est la clef publique et (N, d) la clef privée, avec N de $2n$ bits.
Pour signer un message $m \in \{0,1\}^\ell$, on tire uniformément $r \in \{0,1\}^{2n-\ell}$ tel que $r\|m \in (\mathbb{Z}/N\mathbb{Z})^\times$. La signature de m est $\sigma = (r\|m)^d \bmod N$.

1. Proposer une solution si $r\|m \notin (\mathbb{Z}/N\mathbb{Z})^*$. Estimer le temps de calcul en plus que nécessite cette solution.
2. Décrire l'algorithme de vérification de ce protocole.
3. Montrer qu'une des deux attaques décrites contre la signature RSA simple s'applique toujours ici.

Exercice 3. *Attaques sur RSA-FDH*

La preuve de sécurité de RSA-FDH suppose que la fonction de hachage est aléatoire. Dans cet exercice, on montre que si la fonction de hachage utilisée est au contraire *faible*, on peut attaquer le protocole.
Rappel. Dans RSA-FDH, la signature de $m \in \{0,1\}^*$ avec la clef privée (N, d) est $H(m)^d \bmod N$. La vérification avec la clef publique (N, e), se fait en vérifiant si $H(m) = \sigma^e \bmod N$. On dit que le couple (m, σ) est *valide* si l'égalité est vérifiée.

1. On suppose que H n'est pas résistante à la pré-image : étant donné h, on peut calculer x tel que $H(x) = h$.Montrer qu'un attaquant peut produire un couple (m, σ) valide. *Indication. Utiliser presque la même attaque que pour RSA simple.*
2. On suppose que H n'est pas résistante à la seconde pré-image : étant donné x, on peut calculer $y \neq x$ tel que $H(x) = H(y)$. Montrer qu'un attaquant ayant accès à un oracle de signature peut calculer la signature σ pour un message m *de son choix. Remarque. L'attaquant peut demander la signature des messages* m' *de son choix, sauf celle de* m.
3. On suppose que H n'est pas résistante aux collisions : il est possible de trouver $x \neq y$ tels que $H(x) = H(y)$. Montrer qu'un attaquant ayant accès à un oracle de signature peut produire un couple (m, σ) valide.