

Exercice 1 - Généralités

1. Décrire une manière simple de construire un schéma de signature à partir d'un cryptosystème à clé publique quelconque.
2. Que signifie pour un schéma de signature d'être résistant à la falsification sélective ?
3. On considère un schéma de signature (sig_K, ver_K) utilisant une fonction de hachage H :

$$ver_K(m, \sigma) = \text{Vrai} \iff \sigma = sig_K(H(m))$$

On suppose que le schéma sans la fonction de hachage est sujet à la falsification existentielle selon une attaque sans message connu. A quelle condition sur H le schéma complet devient-il résistant à ce type d'attaques ?

Exercice 2 - Signature RSA

Soit (n, p, q, e, d) des paramètres RSA, (n, e) étant la donnée publique d'Alice.

1. Rappeler le fonctionnement du schéma de signature RSA.
2. Montrer qu'il est facile de générer des signatures valides (sans contrôle sur le message signé).
3. Soient (m_1, σ_1) et (m_2, σ_2) deux documents signés par Alice. Montrer qu'il est facile de fabriquer une signature valide pour le message $m_1 m_2$.
4. Montrer qu'une attaque à clair choisi permet de signer n'importe quel message.

Exercice 3 - Vérification simultanée de signatures RSA

Soit (n, p, q, e, d) des paramètres RSA, d étant l'exposant privé.

1. Soient $\sigma_1, \dots, \sigma_l$ l signatures RSA signées avec la même clé. Quel est le coût de la vérification individuelle de chacune des signatures ?
2. En utilisant la multiplicativité de la fonction RSA, proposer une méthode pour vérifier simultanément si l'ensemble des l signatures est valide en $2(l - 1)$ multiplications et une seule exponentiation.

3. Soient $(m_1, \sigma_1), \dots, (m_l, \sigma_l)$ l couples message/signature valides. Soient $\alpha_1, \dots, \alpha_l \in \mathbb{Z}/n\mathbb{Z}$ tels que $\sum \alpha_i = 1$. Montrer que la méthode précédente validera l'ensemble $(m_1, \alpha_1 \sigma_1), \dots, (m_l, \alpha_l \sigma_l)$.

Exercice 4 - Signature El Gamal

Soit (p, α, β, a) des paramètres ElGamal, a étant la clé privée d'Alice.

1. Rappeler le schéma de signature ElGamal.
2. Montrer que la connaissance de l'entier aléatoire r permet de calculer la clé privée d'Alice.
3. Montrer que la connaissance de deux signatures de deux messages différents utilisant le même entier aléatoire r permet de calculer la clé privée d'Alice.
4. On suppose qu'Alice utilise le générateur aléatoire suivant :

$$k_0 = r \text{ et } k_{i+1} = k_i + 2 \pmod{p-1} \text{ pour tout } i \geq 1.$$

Montrer que la connaissance de 2 messages signés consécutifs permet de retrouver la clé privée d'Alice.

Exercice 5 - ElGamal modifié

On modifie légèrement le schéma de signature Elgamal. Une signature d'un message m est toujours définie par $sig(m) = (\gamma, \delta)$ où maintenant $\delta = (m - k\gamma)a^{-1} \pmod{p-1}$.

1. Décrire la fonction de vérification.
2. Quel est l'avantage de cette fonction de signature (en coût de calcul) ?
3. Étudier brièvement la sécurité du schéma.