D31: Protocoles cryptographiques
TD 4: Signatures Numériques

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 séléctive?
3. On considère un shcéma de signature (sig_K, ver_K) utilisant une fonction de hachage H:

$$ver_K(x, y) = \text{Vrai} \iff y = sig_K(H(x)).$$

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

Exercice 2. Signature RSA

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

1. Rappeler le fonctionement du schéma de signature RSA.
2. Montrer qu'il est facile de générer des signatures valides (sans controle sur le message signé).
3. Soient (x_1, s_1) et (x_2, s_2) deux documents signés par Alice. Monter qu'il est facile de fabriquer une signature valide pour le message x_1x_2.
4. Montrer qu'un attaque à clair choisi permet de signer n'importe quel message.

Exercice 3. Vérification simultanée de signatures RSA

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

1. Décrire le schéma de signature RSA.
2. Soient $s_1, \ldots, s_l$ l signatures RSA signées avec la même clé. Quel est le coût de la vérification individuelle de chacune des signatures?
3. En utilisant de 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.
4. Soient $(m_1, s_1), \ldots (m_l, s_l)$ l couples message/signature valides. Soient $\alpha_1, \ldots, \alpha_l \in \mathbb{Z}_n$ tels que $\prod_{i=1}^{l} \alpha_i = 1$. Montrer que la méthode précédente validera l'ensemble $\{(m_1, \alpha_1 s_1), \ldots, (m_l, \alpha_l s_l)\}$.

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. Monter 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: $k_0 = r$ et $k_{i+1} = k_i + 2 \mod (p-1)$ 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 x est toujours définie par $\texttt{sig}(x) = (\gamma, \delta)$ où maintenant $\delta = (x - k\gamma)a^{-1} \mod p - 1$.

1. Décrire la fonction de vérification `ver`.
2. Quel est l'avantage de cette fonction de signature (en cout de calcul).
3. Étudier briévement la sécurité du schéma.