Licence 3 – MHT633 Université Bordeaux 1
2010/2011

Feuille 7 : Fonctions de hachage et signatures

Exercice 1. Propriétés des fonctions de hachage

Soit g une fonction de hachage résistante aux collisions fortes, et à valeurs dans $\{0,1\}^n$. On considère la fonction de hachage suivante h, à valeurs dans $\{0,1\}^{n+1}$:

$$h(x) = \begin{cases} 1\|x & \text{si } x \text{ possède } n \text{ bits} \\ 0\|g(x) & \text{sinon} \end{cases}$$

où $\|$ désigne la concaténation des chaînes binaires.

1. Montrer que h est résistante aux collisions fortes.
2. Montrer que h n'est pas à sens-unique.

Exercice 2. Signature RSA

1. Rappeler le fonctionnement de la signature RSA.
2. Alice a pour clef publique $(n, e) = (143, 7)$ et clef privée $d = 103$. Vérifier que ce choix convient.
3. Calculer la signature d'Alice pour le message $m = 5$.
4. Alice a signé le message $m = 79$ par la signature $\sigma = 118$. Vérifier que cette signature est correcte.

Exercice 3. Attaques sur la signature RSA

Supposons que n soit un entier produit de deux nombres premiers distincts p et q. On note e, premier avec $\varphi(n)$. Alice utilise la signature RSA avec (n, e) pour clef publique. On note d sa clef privée.

1. Oscar récupère les signatures valides σ_1 et σ_2 de deux messages $m_1, m_2 \in \mathbb{Z}/n\mathbb{Z}$, signés par Alice. Montrer comment Oscar peut construire la signature valide d'un autre message.
2. Oscar souhaite obtenir la signature valide d'Alice d'un message $m \in \mathbb{Z}/n\mathbb{Z}$, signifiant « Alice doit 1000 € à Oscar ». Montrer, en utilisant la question précédente, comment Oscar peut arriver à ses fins en demandant à Alice de signer deux messages apparemment anodins.

3. Montrer comment Oscar peut construire un message (possiblement sans sens) et sa signature valide, sans interaction avec Alice.
4. On utilise maintenant une fonction de hachage h à valeurs dans $\mathbb{Z}/n\mathbb{Z}$. Alice signe un message m en calculant $\sigma = h(m)^d$ dans $\mathbb{Z}/n\mathbb{Z}$. On dit qu'une signature σ' d'un message m' est valide si et seulement si $\sigma'^e = h(m')$ dans $\mathbb{Z}/n\mathbb{Z}$. À quelle condition l'attaque de la première question ne fonctionne plus ?
5. Si h est à sens unique, l'attaque de la question 3. est elle possible ?
6. On suppose que h n'est pas résistante à la 2^{de} pré-image. Oscar récupère la signature valide σ d'un message m. Montrer comment Oscar peut construire une signature valide pour un message différent de m.

Exercice 4. Signature d'ElGamal

Soit p un nombre premier, α un générateur du groupe $\left((\mathbb{Z}/p\mathbb{Z})^\times, \times\right)$. Soit

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}$$

Pour $K \in \mathcal{K}$, on choisit un nombre aléatoire (secret) : $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$. On signe alors le message $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ à l'aide de la fonction :

$$sig(x, k) = \left(\alpha^k \mod p, (x - a\gamma)k^{-1} \mod p - 1\right)$$

où $\gamma = \alpha^k \mod p$

1. Montrer que $(sig(x,k) = (\gamma, \delta)) \iff \left(\beta^\gamma \gamma^\delta \equiv \alpha^x \mod p\right)$
2. En déduire que $ver\,(x, (\gamma, \delta)) = vrai \iff \left(\beta^\gamma \gamma^\delta \equiv \alpha^x \mod p\right)$. De quoi a-t-on besoin pour effectuer la vérification ?
3. Dans cette question on prends $p = 47$, $\alpha = 11$ et $a = 8$.
   (a) Vérifier que α est un générateur de $(\mathbb{Z}/47\mathbb{Z})^\times$ et calculer β.
   (b) Signer le message $x = 12$ (en utilisant k=5).
   (c) Vous recevez le message $x = 2$ avec la signature $(11, 6)$. La signature est elle valide ?

Exercice 5. Attaque de signature d'ElGamal Dans cette exercice on cherche à falsifier une signature.

1. Montrer que si k est dévoilé on peut casser le système de signature.
2. Dans cette question on construit un triplet $(x, (\gamma, \delta))$ valide.
   (a) En utilisant l'équation que doit vérifier le triplet et en écrivant $\gamma = \alpha^i \beta^j$ où $0 \leq i, j \leq p-2$, montrer que :

$$\beta^{\gamma + \delta j} \equiv \alpha^{x - i\delta} \pmod{p}$$

(b) En déduire une condition suffisante sur $\gamma + \delta j$ et $x - i\delta$ sous forme de système.

(c) Expliquer comment choisir i et j pour avoir un triplet valide.

Exercice 6.

Dans un protocole d'identification, un vérificateur V veut vérifier l'identité d'un prouveur P. Pour cela, P doit convaincre V qu'il est en possession d'un certain secret s. Les deux objectifs essentiels d'un tel protocole sont d'une part qu'un usurpateur U ne connaissant pas s ne puisse pas convaincre V, et d'autre part que P puisse convaincre V qu'il possède s sans lui révéler la valeur de s (sinon V pourrait devenir à son tour un usurpateur de l'identité de P).

Nous décrivons maintenant le protocole d'identification de Schnorr :
p et q sont des nombres premiers tels que q divise $p-1$ et α est un élément d'ordre q du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Un nombre $s \mod q$ est le secret de P, tandis que les valeurs de p, q, α, et $v := \alpha^{-s} \mod p$ sont publiques. Le protocole d'identification se déroule en quatre étapes :

(1. Engagement :) P choisit aléatoirement un entier $r \mod q$ et transmet $x = \alpha^r \mod p$ à V.

(2. Challenge :) V envoie un challenge $e \in [0, q-1[$ à P.

(3. Réponse :) P envoie $y = r + es \mod q$ à V.

(4. Vérification :) V vérifie que $x = \alpha^y v^e \mod p$.

P a réussit son identification auprès de V si la vérification est positive.

1. Montrer que P réussit toujours son identification auprès de V.
2. Comment doit-on choisir les nombres premiers p et q pour que personne d'autre que P ne puisse calculer s en un temps raisonnable ?
3. U tente de s'identifier auprès de V. Pour cela il répond un y aléatoire à l'étape 3. Quelles sont ses chances de succès ?
4. Supposons que le protocole précédent soit mal exécuté, et que l'ordre des étapes 1 et 2 soit inversé. Montrez que U peut alors réussir son identification auprès de V.
5. Montrez que, si pour un même engagement r, U est capable de répondre correctement à deux questions e et e' distinctes posées par V, alors il connait s.