Université Bordeaux 1 — **M1 CSI, Cryptologie**
Mathématiques, Informatique — Année 2019–2020

FEUILLE D'EXERCICES n° 9

Hachage, signature

Exercice 1 – Soient un entier $n > 0$ et $h : \{0,1\}^{2n} \to \{0,1\}^n$ définie par $h(x_1 \| x_2) = x_1 \oplus x_2$ pour $x_1, x_2 \in \{0,1\}^n$. Que penser de cette fonction de compression ?

Exercice 2 – Soient un entier $n > 0$ et $h : \{0,1\}^* \to \{0,1\}^n$ une fonction de hachage résistante à la préimage et aux collisions. On définit $H : \{0,1\}^* \to \{0,1\}^{n+1}$ par :

$$H(x) = \begin{cases} 0 \| x & \text{si } x \in \{0,1\}^n \\ 1 \| h(x) & \text{sinon.} \end{cases}$$

Montrer que H est encore résistante aux collisions mais n'est pas résistante à la préimage.

Exercice 3 – Soient p, q deux grands premiers distincts (tenus secrets) et $n = pq$. On note K_n l'ensemble des carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$. Que penser de la fonction de compression $h : (\mathbb{Z}/n\mathbb{Z})^\times \to K_n$ définie par $h(x) = x^2$?

Exercice 4 – Soient un entier $n > 0$ et $h : \{0,1\}^{2n} \to \{0,1\}^n$ une fonction de compression. On considère $H : \{0,1\}^{4n} \to \{0,1\}^n$ définie par

$$H(x_1 \| x_2) = h(h(x_1) \| h(x_2)), \quad \text{où } x_1, x_2 \in \{0,1\}^{2n}.$$

1) Montrer que si h est résistante à la préimage, H l'est aussi.

2) Supposons que h soit résistante aux collisions. H l'est-elle aussi ?

3) Même question avec la résistance à la seconde préimage.

Exercice 5 – Alice utilise un système ElGamal. Elle a choisi le premier $p = 83$. Comme dans l'exercice 5 de la feuille 8, elle prend $g = 2$ qui est une racine primitive modulo p et son exposant secret est $s = 32$. Sa clé publique est donc $(p, g, g^s \bmod p) = (83, 2, 77)$. Elle décide d'envoyer deux messages $M_1 = 41$ et $M_2 = 25$ à Bob. Elle les signe $(u_1, v_1) = (56, 67)$ et $(u_2, v_2) = (56, 63)$ respectivement.

1) Que fait Bob pour vérifier ces deux signatures ? Donner le détail de ses calculs.

2) Bob remarque que $u_1 = u_2$. Montrer comment il peut retrouver la clé secrète d'Alice.

Exercice 6 – Considérons la variante suivante de la signature ElGamal. Alice choisit un grand premier p et α une racine primitive modulo p. Elle choisit aussi une fonction $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}$. Son secret est un entier s. Elle calcule $\beta = \alpha^s \bmod p$. Les entiers p, α, β et la fonction f sont publics. Pour signer un message $M \in \{1, 2, \dots, p-1\}$ elle choisit un entier k premier avec $p - 1$, calcule

$$u = \alpha^k \bmod p \text{ et } v = k^{-1}(M - f(u)s) \bmod (p-1).$$

Le message signé est (M, u, v).

1) Comment Bob vérifie-t-il la signature ?

2) Montrer que si Alice choisit $f = 0$, Ève peut construire une signature valide pour n'importe quel message.

Exercice 7 –

1) Décrire une falsification existentielle sur la signature ElGamal.

2) Comment se prémunir contre une telle attaque ?

Exercice 8 – Décrivons le schéma de signature DSA (Digital Signature Algorithm). Alice choisit un premier q et un premier p tel que $q \mid p-1$. Soient g une racine primitive modulo p et $\alpha = g^{(p-1)/q} \bmod p$. Le secret d'Alice est un entier $1 \leqslant s \leqslant q-1$. Elle calcule $\beta = \alpha^s \bmod p$. Les entiers p, q, α, β sont publics. Le message $0 \leqslant M \leqslant q-1$ est signé de la façon suivante : Alice choisit en secret un entier k vérifiant $0 < k < q-1$ et tel que, si $u = (\alpha^k \bmod p) \bmod q$, alors u et $M + su$ sont non nuls modulo q. Soit $v = k^{-1}(M + su) \bmod q$. Le message signé est (M, u, v).

1) Comment Bob vérifie-t-il la signature ?

2) Analyser la différence avec la signature ElGamal.