**École normale supérieure** **2018-2019**
**Département d'informatique**

**Introduction à la cryptologie**
**TD n° 9 : Chaîne de blocs [1], suite et fin.**

**Exercice 1** (Ring signature)**.** Dans une signature de cercle, le signataire peut choisir un ensemble quelconque de clefs publiques incluant sa propre clef publique, et signer son message sans révéler quelle clef publique parmi cet ensemble a été utilisée. Essayons de construire une signature de ce type.
On part d'un schéma de signature à clef publique, mettons RSA. Notons sa fonction de chiffrement $E_{pk}(m)$ pour la clef publique $pk$, et sa fonction de déchiffrement $D_{sk}(c)$. Dans le schéma de signature de cercle que nous construisons, une signature pour un « cercle » de clefs publiques $(pk_1, \ldots, pk_n)$ est une solution d'une certaine équation qui dépend du haché du message $H(m)$ et des clefs publiques :

$$\mathsf{Eq}(H(m), E_{pk_1}(x_1), \ldots, E_{pk_n}(x_n)).$$

La signature de $m$ est $(pk_1, \ldots, pk_n, x_1, \ldots, x_n)$. Vérifier une signature, c'est vérifier $\mathsf{Eq}$.

1. Essayons :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : y_1 \oplus \cdots \oplus y_n = h.$$
   (a) Comment le signataire peut-il calculer une signature ?
   (b) Décrire une attaque contre ce schéma, qui permet à un adversaire de calculer efficacement la signature d'un message quelconque pour un ensemble quelconque (suffisamment grand) de clefs publiques, en résolvant un système linéaire. Le schéma de signature est-il résistant aux forges existentielles avec messages choisis ?
2. On suppose qu'on utilise RSA avec un exposant public $e = 3$, c'est-à-dire que la fonction de chiffrement est $m \mapsto m^3 \bmod N$ (attention, ceci n'est pas un vrai chiffrement à clef publique, mais ce n'est pas grave pour notre utilisation). On suppose que tous les modules RSA ont le même nombre de bits $b$. Deuxième tentative :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : y_1 + \cdots + y_n = h \quad \text{dans } \mathbb{Z}_{2^b}.$$
   Décrire une attaque contre ce schéma, du même type que dans la question précédente.
   **Indication non-triviale :** tout nombre entier $x \in \mathbb{N}$ peut se décomposer efficacement en une somme $\sum x_i^3$ de 9 cubes avec $x_i \in \mathbb{N}$.
3. Soit $S_k$ la fonction de chiffrement d'un chiffrement symmétrique pour la clef $k$. On suppose que tous les $y_i$ vivent dans le même espace, qui est aussi l'entrée/sortie de $S$. Dernière tentative :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : S_h(y_1 \oplus S_h(y_2 \oplus \ldots S_h(y_n))) = 0.$$
   (a) Expliquer comment un signataire légitime (donc connaissant la clef privée d'un des $pk_i$ du cercle) peut signer un message.
   (b) Montrer que pour $s \leq n$ et $h, y_1, \ldots, y_{s-1}, y_{s+1}, \ldots, y_n$ fixés quelconques, la solution $y_s$ à l'équation $\mathsf{Eq}(h, y_1, \ldots, y_n)$ est unique.
   (c) Montrer que la distribution de probabilité générée en tirant $y_1, \ldots, y_{s-1}, y_{s+1}, \ldots, y_n$ de manière indépendante et uniforme, et en calculant le $y_s$ approprié, ne dépend pas de $s$.
   (d) En déduire une manière de signer qui garantit que la signature ne révèle *rien* sur quel membre du cercle a signé.
   (e) Comment la taille d'une signature croît-elle avec le nombre $n$ de personnes dans le cercle ?

1. Traduction officielle par la Commission d'enrichissement de la langue française, parue au Journal officiel en 2017.

**Exercice 2** (Commitment)**.** Un *commitment* (mise en gage) est une famille de fonctions (paramétrée par la taille des entrées) $C : \mathcal{X} \times \mathcal{A} \to \mathcal{S}$ avec les propriétés suivantes :

a) Il est difficile de trouver $x \neq x'$ et $a$, $a'$ tels que $C(x, a) = C(x', a')$.
b) Si $A$ est la distribution uniforme sur $\mathcal{A}$, alors pour tout $x \neq x'$, les distributions $C(x, A)$ et $C(x', A)$ sont (calculatoirement) indistinguables.

Alice et Bob veulent tirer à pile ou face pour savoir qui va décider du nom de la prochaine cryptomonnaie qu'ils inventent. Mais ils sont à distance. Ils veulent utiliser un protocole avec les propriétés suivantes :

— Si les deux participants sont honnêtes, le résultat du protocole est un tirage pile/face uniformément aléatoire.
— Si seulement un des deux participants suit honnêtement le protocole, le résultat est soit un abort $\perp$, soit un tirage pile/face uniformément aléatoire.

1. On suppose qu'on a un schéma de commitment sur $\mathcal{X} = \{0, 1\}$. Inventer un protocole de tirage à pile ou face cryptographique, comme le veulent Alice et Bob.
2. Montrer (informellement) que si l'une des deux propriétés du schéma de commitment n'est pas réalisée, le schéma n'est pas sûr.
   *Remarque.* Il y a beaucoup de réponses possibles à la première question. Si vous en trouvez une pour laquelle la seconde question est fausse ou n'a pas de sens, vous avez probablement fait exprès !
3. Donner une construction, heuristique ou non, de schéma de mise en gage.

**Exercice 3** (Wifi Protected Setup, ou comment ne pas utiliser des commitments, exercice de détente)**.** En 2006, la Wifi Alliance, qui gouverne les normes Wifi, a créé le Wifi Protected Setup (WPS), qui permet entre autres à un ordinateur de s'authentifier auprès d'une box wifi à l'aide d'un code PIN de 8 chiffres. Les 8 chiffres $c_1, \ldots, c_8$ vérifient $c_1 + 3c_2 + c_3 + 3c_4 + c_5 + 3c_6 + c_7 + 3c_8 = 0 \bmod 10$. Le code est à vie pour l'appareil et ne peut pas être changé.
Le protocole utilisé est le suivant. Soit $A$ l'ordinateur d'Alice et $B$ la box internet en wifi. On utilise un schéma de commitment $C$ comme décrit dans l'exercice précédent. S'*engager* sur une valeur $m \in \mathcal{X}$ signifie tirer $a \in \mathcal{A}$ uniformément, et publier $e = C(m, a)$. *Dévoiler* l'engagment signifie publier $a$. *Vérifier* l'engagement est simplement vérifier $e = C(m, a)$ une fois $a$ dévoilé. Le code PIN est composé de deux moitiés de 4 chiffres $m_1 \parallel m_2$ (où $\parallel$ dénote la concaténation). $A$ et $B$ commencent par faire un échange de clef Diffie-Hellman pour chiffrer les communications avec un secret commun, puis continuent comme suit.

a) La box s'engage sur $m_1$ et sur $m_2$.
b) Alice publie $m_1$ et s'engage sur $m_2$.
c) La box vérifie l'engagement d'Alice sur $m_1$, et dévoile son engagement sur $m_1$.
d) Alice vérifie l'engagement de la box sur $m_1$, et dévoile le sien sur $m_2$.
e) La box vérifie l'engagement d'Alice sur $m_2$, et dévoile le sien sur $m_2$.
f) Alice vérifie l'engagement de la box sur $m_2$.

Si une étape de vérification échoue, le protocole est arrêté.

1. Si un adversaire se fait passer pour la box auprès d'Alice, combien d'essais sont nécessaires pour apprendre le code PIN ?
2. Même question si l'adversaire se fait passer pour Alice auprès de la box.