Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Devoir Maison 1

Exercice 1. Le système de Goldwaser-Micali

1. **Les carrés de $\mathbb{Z}/p\mathbb{Z}$**
   Soit p un nombre premier impair et

$$\begin{array}{rcl}\phi : (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^2\end{array}$$

   (a) Montrez que $\ker\phi = \{\pm 1\}$.
   (b) En déduire que $\operatorname{Im}\phi$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $(p-1)/2$, et que, si $y \in \operatorname{Im}\phi$ alors l'équation $x^2 = y$ a exactement deux solutions, c'est à dire que y a exactement deux racines carrées.
   (c) En déduire que si y est un carré de $(\mathbb{Z}/p\mathbb{Z})^\times$ alors $y^{\frac{p-1}{2}} = 1$.
   (d) On veut établir la réciproque de la question précédente. Soit $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Que vaut $g^{\frac{p-1}{2}}$? Exprimer y en fonction de g. En déduire que si $y^{\frac{p-1}{2}} = 1$ alors y est un carré de $(\mathbb{Z}/p\mathbb{Z})^\times$.
   (e) On suppose que $p \equiv 3 \pmod 4$. Soit y un carré de $(\mathbb{Z}/p\mathbb{Z})^\times$, monter que les racines carrés de y sont $y^{\frac{p+1}{4}}$ et $-y^{\frac{p+1}{4}}$.

2. **Les carrés de $\mathbb{Z}/n\mathbb{Z}$**
   Soit $n = pq$ où p et q sont des nombres premiers impairs distincts congrus à 3 modulo 4.

   (a) Caractériser les carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$.
   (b) Ecrire un algorithme qui prend pour entrées n, p, q et $y \in \{0, 1, \dots, n-1\}$ tel que $n = pq$ et qui détermine si $y \in \{0, 1, \dots, n-1\}$ représente un carré modulo n.
   (c) Si $y \in (\mathbb{Z}/n\mathbb{Z})^\times$, montrer que l'équation $x^2 = y$ admet soit quatre solutions soit aucune.
   (d) Ecrire un algorithme qui prend pour entrées n, p, q et $y \in \{0, 1, \dots, n-1\}$ tel que $n = pq$ et y est un carré modulo n et qui renvoie ces 4 racines carrés.

3. **Le chiffrement de Goldwasser-Micali**
   Soit $n = pq$ où p et q sont des nombres premiers impairs distincts congrus à 3 modulo 4. On fixe $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui n'est pas un carré modulo n, ni modulo p, ni modulo q. Le système de Goldwasser-Micali chiffre un élément $m \in \{0, 1\}$ avec la clé publique (n, α) par $\alpha^m x^2$ où x est un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ choisit au hasard.

(a) Quelle est la clé privée ?

(b) Montrer que le chiffré de m est un carré modulo p si et seulement si $m = 0$.

(c) En déduire la fonction de déchiffrement.

(d) Si on veut envoyer un message de l bits, quelle est la taille du message chiffré.

(e) Expliquer comment construire un élément α convenable à partir d'un élément α_p de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui n'est pas un carré, et d'un élément α_q de $(\mathbb{Z}/q\mathbb{Z})^\times$ qui n'est pas un carré.

(f) Ecrire un algorithme aléatoire qui renvoie un α convenable. Quelle est sa probabilité de réussite ?

Exercice 2. Chiffrement de Paillier (1999)

1. **Préliminaires**

(a) Soit $n \in \mathbb{N}^*$. Montrer que $(1 + n)$ est inversible modulo n^2.

(b) Calculer $(1 + n)^m \pmod{n^2}$ pour tout $0 \leq m \leq n^2 - 1$.

(c) Quel est l'ordre de $(1 + n)$ dans $(\mathbb{Z}/n^2\mathbb{Z})^\times$?

(d) Soit G le sous groupe de $(\mathbb{Z}/n^2\mathbb{Z})^\times$ engendré par $(1 + n)$. Expliquez comment calculer en temps polynomial le logarithme discret d'un élément de G en base $(1 + n)$.

(e) Dans la suite, on suppose que $n = p \times q$ avec p et q deux nombres premiers distincts. Exprimez le cardinal de $(\mathbb{Z}/n^2\mathbb{Z})^\times$ en fonction de n et $\varphi(n)$.

(f) On suppose de plus dans la suite que n est premier avec $\varphi(n)$, quelles conditions cela impose t'il sur les nombres premiers p et q ?

(g) Montrer que la fonction

$$\begin{array}{rccl} s: & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \left(\mathbb{Z}/n^2\mathbb{Z}\right)^\times \\ & r \mod n & \longrightarrow & r^n \mod n^2 \end{array}$$

est bien définie, c'est à dire que si $a \equiv b \pmod{n}$ alors, $s(a) \equiv s(b) \pmod{n^2}$.

(h) Montrer que s est un morphisme de groupe.

(i) Montrer que s est injective, c'est à dire que $\ker s = \{1\}$ (indication : si $s(x) \equiv 1 \pmod{n^2}$, considérer $s(x) \pmod{n}$ et se servir du fait que n est premier avec $\varphi(n)$ et raisonner comme pour RSA).

2. **Description du système de chiffrement**

   On suppose toujours que $n = pq$ est le produit de deux grands nombres premiers distincts et que n est premier avec $\varphi(n)$.
   On munit l'ensemble $\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times$ de la loi de groupe $(a, b) \diamond (a', b') = (a + a' \mod n, bb' \mod n))$.
   On considère l'application suivante :

$$\begin{array}{rccl} \mathcal{E} : & \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \left(\mathbb{Z}/n^2\mathbb{Z}\right)^\times \\ & (m, r) & \longrightarrow & (1+n)^m r^n \end{array}$$

   (a) Montrer que $\mathcal{E}$ est bien définie et que $\mathcal{E}$ est un morphisme de groupe (utiliser le morphisme s).

   (b) Montrer que $\mathcal{E}$ est injectif (utiliser encore les résultats sur s). En déduire que $\mathcal{E}$ un isomorphisme de groupe.

   Le cryptosystème de Paillier utilise n comme clef publique. Pour chiffrer un message $m \in \mathbb{Z}/n\mathbb{Z}$ avec cette clef publique, on choisit $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ au hasard et on calcule $c = \mathcal{E}(m, r)$.

   (c) Est ce que $n = 35$ est un bon choix de clef publique (hormis le fait qu'il est facile de retrouver p et q) ? Chiffrer le message $m = 3$ avec $n = 35$ et $r = 8$.

   On cherche maintenant à établir l'algorithme de déchiffrement.

   (d) Soit c un message chiffré de m avec l'aléa r. Calculer $c^{\varphi(n)} \pmod{n^2}$. En déduire l'algorithme de déchiffrement et la clef privée du cryptosystème de Paillier.

   (e) Calculer la clef privée pour $n = 35$ et déchiffrer le message chiffré précédemment.

   (f) Expliquez sur quoi repose la sécurité de ce système de chiffrement.

3. **Une application du système de Paillier : le vote électronique**

   Alice, Bob et Charlie veulent utiliser le système de Paillier pour voter à un référendum. Une autorité $\mathcal{A}$ est chargée d'organiser le vote et de calculer le résultat. L'autorité génère un couple clef publique, clef secrète pour le système de Paillier. Si Alice veut voter « oui » au référendum, elle envoie le message 1 à $\mathcal{A}$, chiffré avec la clef publique de $\mathcal{A}$, si elle veut voter « non », elle envoie un chiffré du message 0. De même pour Bob et Charlie. On note v_A, v_B et v_c les votes chiffrés envoyés à $\mathcal{A}$ respectivement par Alice, Bob et Charlie.

   (a) Montrer comment $\mathcal{A}$ peut, en déchiffrant le produit $v_A v_B v_C$, retrouver le résultat du référendum.

   (b) Charlie souhaite que le « oui » l'emporte au référendum. Comment pourrait il faire pour falsifier le vote en ce sens ?

(c) On suppose que Alice, Bob et Charlie ne « trichent » pas. Proposer une manière de modifier ce protocole de vote pour qu'ils votent pour élire un candidat parmi ℓ, avec $\ell > 2$.