Année universitaire 2014-2015
Licence 3 de mathématiques
Cryptographie et arithmétique - Devoir à la maison

Problème : chiffrement de Paillier

Partie 1. Soit n un entier ≥ 2.

a. Montrer que $1+n$ est d'ordre n dans le groupe $(\mathbb{Z}/n^2\mathbb{Z})^*$.

b. Notons G le sous-groupe de $(\mathbb{Z}/n^2\mathbb{Z})^*$ engendré par $1+n$. Comment calculer en temps polynomial le logarithme discret d'un élément de G en base $1+n$?

c. Exprimer $\varphi(n^2)$ en fonction de n et $\varphi(n)$.

d. Construire un morphisme de groupes $s : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n^2\mathbb{Z})^*$ tel que $s(r \bmod n) = r^n$ pour tout $r \in (\mathbb{Z}/n^2\mathbb{Z})^*$; *indication :* observer que $r^n = 1$ si $r \equiv 1 \bmod n$.

e. Supposons n et $\varphi(n)$ premiers entre eux. Soit $r \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $r^n = 1$. Prouver que $r = 1$.

Partie 2. Soit n un entier ≥ 2 tel que n et $\varphi(n)$ soient premiers entre eux. On désigne par $E : \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n^2\mathbb{Z})^*$ le morphisme vérifiant : $E(m \bmod n; r \bmod n) = (1+n)^m r^n$ pour tout $(m; r) \in \mathbb{Z} \times (\mathbb{Z}/n^2\mathbb{Z})^*$.

a. Montrer que E est un isomorphisme de groupes.

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

b. Calculer $c^{\varphi(n)}$. En déduire l'algorithme de déchiffrement et la clef privée de ce cryptosystème. Sur quoi repose sa sécurité ?

c. Chiffrer le message $m = 3$ avec $n = 35$ et $r = 8$.