Année universitaire 2013-2014
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 4

Exercice 1

Notons C l'ensemble des entiers de la forme $p^r m$ avec p premier, $r \geq 1$ et $m \in \{1; 2\}$. Soit n un entier ≥ 2 tel que $n \notin C$.

a. Montrer qu'il existe $b \geq 3$, $c \geq 3$ et $a \in \{1; \cdots; n-1\}$ vérifiant : $n = bc$, b et c sont premiers entre eux, b divise $a+1$ et c divise $a-1$.

b. Démontrer que $2 \leq a \leq n-2$ et que $a^2 \equiv 1 \bmod n$.

c. Soit α un entier vérifiant : $2 \leq \alpha \leq n-2$ et $\alpha^2 \equiv 1 \bmod n$. Comment trouver un facteur non trivial de n à l'aide de α ?

Exercice 2

Soient m et n deux entiers ≥ 1. Prouver que m et n sont premiers entre eux si et seulement si $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$.

Exercice 3

On considère k personnes $B_1, \cdots, B_k$ ayant pour clefs RSA publiques respectives $(n_1; e), \cdots, (n_k; e)$, avec le même exposant public e. Désignons par P le ppcm de $n_1, \cdots, n_k$.

Alice envoie les chiffrés d'un même message m à tous les B_i. Montrer qu'un attaquant peut déterminer m si $m^e < P$ (*indication :* considérer m^e modulo P).

Exercice 4

Bob a choisi la clef RSA publique $(n; e_B)$ et Catherine la clef $(n; e_C)$, avec le même module n.

a. On suppose e_B et e_C premiers entre eux. Alice envoie les chiffrés d'un même message m à Bob et à Catherine. Comment l'attaquant Oscar peut-il obtenir m ?

b. Supposons $n = 221$, $e_B = 11$ et $e_C = 7$. Oscar intercepte les chiffrés 210 et 58 à destinations respectives de Bob et de Catherine. Retrouver le message m.

Exercice 5 : chiffrement de Paillier

Partie 1. Soit n un entier ≥ 1.

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 $r \in (\mathbb{Z}/n^2\mathbb{Z})^*$.

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 ≥ 1 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 $r = 8$.

Exercice 6 : critère de Korselt

Soient m et n deux entiers ≥ 2. Montrer que les propriétés suivantes sont équivalentes :
(α) Pour tout entier a, n divise $a^m - a$;
(β) Pour tout premier p divisant n, p^2 ne divise pas n et $p-1$ divise $m-1$.

Prouver que 561 divise $a^{561} - a$ pour tout $a \in \mathbb{Z}$.