Année universitaire 2013-2014
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 6

Exercice 1

Soit $a \in (\mathbb{Z}/47\mathbb{Z})^*$ tel que $a \notin \{-1; 1\}$. Montrer que a ou $-a$ engendre $(\mathbb{Z}/47\mathbb{Z})^*$.

Exercice 2

Bob a choisi la clef RSA publique $(n; 3)$. Alice envoie à Bob le chiffré c du message m et le chiffré c' du message $m + r$.

a. Exprimer $c' - c + 2r^3$ et $c' + 2c - r^3$ en fonction de m et r.

b. Oscar intercepte c et c'. On suppose qu'il connait r et que $c' - c + 2r^3 \not\equiv 0 \bmod n$. Comment peut-il obtenir m en temps polynomial ?

c. Supposons $n = 2173$, $r = 1$, $c = 793$ et $c' = 2083$. Retrouver le message m.

Exercice 3

Soit p un nombre premier impair ; posons $G = (\mathbb{Z}/p\mathbb{Z})^*$. Soit $g \in G$.

a. Comment tester si g engendre le groupe G en effectuant au plus $\dfrac{p-3}{2}$ multiplications dans G ?

b. Supposons maintenant que la factorisation de $p - 1$ est connue. Comment tester si g engendre G en n'effectuant que $O(\ln^2 p)$ multiplications dans G ?

Exercice 4 : chiffrement d'Elgamal

Soit n un entier ≥ 1. Soit $g \in (\mathbb{Z}/n\mathbb{Z})^*$ un élément d'ordre d. Soit x un entier ; posons $h = g^x$. Pour chiffrer un message $m \in (\mathbb{Z}/n\mathbb{Z})^*$, on choisit un entier r et on calcule $(c_1; c_2) = (g^r; h^r m)$.

a. Quelle est la clef publique de ce cryptosystème ? Combien un message clair a-t-il de chiffrés possibles ?

b. Calculer c_1^x. En déduire la clef privée et la fonction de déchiffrement D.

c. Vérifier que D est un morphisme de groupes.

Exercice 5 : théorème de Pocklington

Soient n et d deux entiers ≥ 2. On suppose que pour tout facteur premier p de d, il existe un entier a_p vérifiant : n divise $a_p^d - 1$ et $n \wedge (a_p^{d/p} - 1) = 1$.
Soit q un facteur premier de n.

a. Soit p un facteur premier de d. Montrer que $p^{v_p(d)}$ divise l'ordre de $\bar{a_p}$ dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$.

b. En déduire que d divise $q - 1$.

c. Prouver que si $d + 1 > \sqrt{n}$, alors n est premier.

Exercice 6 : algorithme $p - 1$ de Pollard

Soit b un entier ≥ 2. On dit qu'un entier $m \geq 1$ a la propriété F_b lorsque pour tout facteur premier q de m, on a $q^{v_q(m)} \leq b$.
Soient n et a deux entiers ≥ 2 premiers entre eux. Supposons qu'il existe un facteur premier p de n tel que $p - 1$ ait la propriété F_b. Notons M le ppcm de $1, 2, \cdots, b$. On calcule a^M modulo n, puis $d = n \wedge (a^M - 1)$.

a. Montrer que d est un diviseur > 1 de n. Cet algorithme trouve donc un facteur non trivial de n si $a^M \not\equiv 1 \bmod n$.

b. Tester l'algorithme avec $n = 221$ et $a = 2$ (en faisant varier b).

Exercice 7

Soient $n \geq 2$ et a deux entiers premiers entre eux.

a. Supposons n premier. Montrer la congruence $(X + a)^n \equiv X^n + a \bmod n$.

b. Soit p un facteur premier de n. Prouver que $p^{v_p(n)}$ ne divise pas C_n^p.

c. Supposons que $(X + a)^n \equiv X^n + a \bmod n$. Démontrer que n est premier.