Année universitaire 2014-2015
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 6

Exercice 1

Soient p et q deux nombres premiers distincts. Posons $\Phi = X^{q-1} + \cdots + X + 1$. On suppose que Φ a une racine a dans $\mathbb{Z}/p\mathbb{Z}$.

a. Déterminer l'ordre de a dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

b. En déduire que q divise $p - 1$.

Exercice 2

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

Exercice 3

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 4 : algorithme de Dixon

On pose ici $n = 2041$.

a. Calculer $x^2 \bmod n$ pour $46 \leq x \leq 51$.

b. Factoriser n avec l'algorithme de Dixon et la base de facteurs $\{2; 3; 5; 7\}$.

Exercice 5

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

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

b. On suppose 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 ? (*indication :* considérer $g^{(p-1)/q}$ pour tout facteur premier q de $p-1$)

Exercice 6 : algorithme baby-step giant-step

Soient G un groupe cyclique d'ordre n et g un générateur de G. On pose ici $b = \lceil \sqrt{n} \rceil$.

a. Soit h un élément de G. Montrer qu'il existe $(q; r) \in \{0; \cdots; b-1\}^2$ vérifiant $g^{bq}h = g^r$.

b. En déduire un algorithme donnant le logarithme discret d'un élément de G en base g en n'effectuant que m multiplications dans G, avec $m < 2\sqrt{n}$.

c. Supposons $G = (\mathbb{Z}/31\mathbb{Z})^*$. Calculer le logarithme discret de 15 en base 3.

Exercice 7

Soient q un entier impair ≥ 3 et r un entier naturel.

a. Soit m un entier ≥ 1. Prouver (par récurrence sur r) la congruence

$$(1+q)^{q^r m} \equiv 1 + q^{r+1}m \mod q^{r+2} .$$

b. En déduire que le noyau du morphisme canonique $(\mathbb{Z}/q^{r+2}\mathbb{Z})^* \to (\mathbb{Z}/q\mathbb{Z})^*$ est un groupe cyclique d'ordre q^{r+1}.

c. Montrer que si q est premier, alors le groupe $(\mathbb{Z}/q^{r+2}\mathbb{Z})^*$ est cyclique.