Université de Bordeaux — **N1MA9W05 – Algo. de la crypto. à clé publique**
Mathématiques — 2014–2015

Examen, 19 décembre 2014 (08:30 – 11:30)
Durée 3 heures. Notes de cours et programmes GP autorisés.

La clarté des programmes et la pertinence des commentaires est un élément important d'appréciation.

- Créer un fichier par exercice, intitulés `login1.gp`, `login2.gp`, etc.
- Pour rendre votre copie, taper `~kbelabas/copie` dans un terminal, depuis le répertoire où se trouvent vos fichiers. (Vous pouvez rendre plusieurs fois votre copie : seule la dernière fait foi, les précédentes sont détruites.)

On rappelle la *borne de Hasse* : pour toute courbe elliptique $E/\mathbb{F}_q$, on a

$$|\#E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Exercice 1 – Prouver que l'entier $9 \cdot 2^{500} + 19$ est composé.

Exercice 2 – Donner une preuve de primalité (par exemple $p-1$ ou méthode des courbes elliptiques) des entiers N suivants :

$$10^{50} + 151, \quad 10^{101} + 3, \quad 10^{199} + 153.$$

Exercice 3 – Soit $m > 0$ un entier. On cherche une puissance q d'un premier p et une courbe elliptique E définie sur $\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = m$.

1) Dans quel intervalle faut-il chercher q ?

2) Trouver un premier p et une courbe elliptique $E/\mathbb{F}_p$ telle que $\#E(\mathbb{F}_p) = 2014$.

3) Trouver q non premier et $E/\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = 2014$.

Exercice 4 – Construire explicitement une implantation minimale du protocole ElGamal (chiffrement et déchiffrement) basée sur une courbe elliptique « sure » de cardinal $\approx 2^{200}$. On ne se préoccupera pas d'assurer l'intégrite ou l'authenticité du message (via fonctions de hachage, etc.). Indiquer explicitement les attaques contre lesquelles vous vous prémunissez, et pour quelle raison.

Exercice 5 – Soit p un nombre premier impair et $a \in \mathbb{F}_p$ un carré. On désire calculer une racine carrée de a dans $\mathbb{F}_p$.

1) a) Si $p \equiv 3 \pmod 4$, montrer que $a^{(p+1)/4}$ est une racine carrée de a.
b) Implanter l'algorithme correspondant. Quelle est sa complexité binaire ?

2) Soit $u \in \mathbb{F}_p$ tel que $D := u^2 - a$ ne soit pas un carré modulo p.

a) Dans $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[t]/(t^2 - D)$, montrer que $t^p = -t$, puis que

$$(u + t)^{p+1} = u^2 - t^2 = a.$$

b) En déduire une formule simple donnant une racine carrée de a.

c) Implanter l'algorithme correspondant, en testant $u = 0, 1, 2, \ldots$ On pourra poser `t = ffgen(t^2 - Mod(D,p))`.

d) Quelle est sa complexité binaire ?

Exercice 6 – Soit $p = 10^{20} + 39$.

1) Calculer l'ordre de 3 dans $\mathbb{F}_p^*$ sans utiliser `znorder`.

2) Calculer x dans $\mathbb{Z}/(p-1)\mathbb{Z}$ tel que $3^x = 5$ dans $\mathbb{F}_p$ sans utiliser `znlog`.

3) Existe t'il y tel que $5^y = 3$ dans $\mathbb{F}_p$?