UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2004–2005

**Master CCSI 2**

Méthodes mathématiques de la cryptologie

Examen de janvier 2005

Durée 2 heures. Documents manuscrits autorisés

## Exercice I

Soient $a$ et $n$ deux entiers positifs. On pose $N = a^n - 1$.

1) Montrer que $a$ est premier avec $N$ et calculer l'ordre de $a$ modulo $N$, c'est à dire le plus petit entier strictement positif $k$ tel que $a^k \equiv 1 \pmod{N}$.

2) Déduire du théorème d'Euler–Fermat que pour tout $a$ et $n$ on a $n \mid \phi(a^n - 1)$, où $\phi$ est la fonction d'Euler.

## Exercice II

Soit $p$ un nombre premier **différent de** 2. On rappelle que l'on peut définir le corps $\mathbb{F}_{p^2}$ comme $\mathbb{F}_p[X]/(X^2 - d)\mathbb{F}_p[X]$ (c'est-à-dire l'ensemble des $u + v\alpha$, où $u$ et $v$ sont dans $\mathbb{F}_p$ et $\alpha^2 = d$), où $d$ est un élément de $\mathbb{F}_p$ **fixé** tel que $\left(\frac{d}{p}\right) = -1$.

1) En distinguant 3 cas, donner très soigneusement la solution générale dans $\mathbb{F}_{p^2}$ de l'équation du deuxième degré $ax^2 + bx + c = 0$, où $a$, $b$ et $c$ sont dans $\mathbb{F}_p$ (**pas** dans $\mathbb{F}_{p^2}$) avec $a \neq 0$. Les solutions données devront toutes être exprimées sous la forme $u + v\alpha$ avec $u$ et $v$ dans $\mathbb{F}_p$ comme ci-dessus.

2) Application numérique : on choisit $p = 47$.

a) Montrer que $d = -1$ convient pour définir $\mathbb{F}_{47^2}$. On choisit donc $d = -1$, et on note $i$ une racine de $i^2 = -1$ dans $\mathbb{F}_{47^2}$.

b) Calculer les solutions dans $\mathbb{F}_{47^2}$ de l'équation $x^2 + x + 1 = 0$, qui doivent toutes s'exprimer sous la forme $u + iv$ avec $u$ et $v$ dans $\mathbb{F}_{47} = \mathbb{Z}/47\mathbb{Z}$, **sans dénominateurs ni racines carrées**.

## Exercice III

1) a) Montrer que le polynôme $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ (attention : il ne suffit pas de montrer qu'il n'a pas de racines dans $\mathbb{F}_2$).

On peut donc définir

$$\mathbb{F}_{16} = \mathbb{F}_{2^4} = \mathbb{F}_2[\alpha] = \{u_3\alpha^3 + u_2\alpha^2 + u_1\alpha + u_0\} ,$$

où $u_i \in \mathbb{F}_2$ (donc égal à la classe de 0 ou 1 modulo 2), et $\alpha$ vérifie $\alpha^4 + \alpha + 1 = 0$, en d'autres termes $\alpha^4 = \alpha + 1$.

b) Il est clair que $\alpha^3 \neq 1$. Calculer $\alpha^5$, et en déduire que $\alpha^5 \neq 1$ également. En déduire que $\alpha$ est d'ordre 15 dans $\mathbb{F}_{16}^*$, donc que c'est un générateur du groupe cyclique $\mathbb{F}_{16}^*$.

2) On va faire un tableau analogue à celui fait en devoir, mais cette fois-ci pour $\mathbb{F}_{16}$, et plus intelligemment. Le tableau ayant 15 lignes plus les en-têtes, il est préférable de le rédiger sur une nouvelle page. On fera comme suit:

- Dans la première colonne on mettra les entiers de 0 à 14, avec comme en-tête $n = \log(z)$.
- Dans la deuxième colonne on mettra les $\alpha^n$ correspondants comme polynômes de degré au plus 3 en $\alpha$, avec comme en-tête $z = \alpha^n$. Cette colonne sera calculée ligne par ligne en utilisant simplement $x + x = 0$ pour tout $x$, ainsi que la relation $\alpha^4 = \alpha + 1$. Les 15 éléments de cette colonne sont donc les 15 éléments $z$ de $\mathbb{F}_{16}^*$, l'indice $n$ correspondant étant le logarithme discret de $z$ à base $\alpha$. On vérifiera qu'on a bien $\alpha^{15} = 1$.
- Dans les colonnes suivantes, en utilisant le log discret modulo 15, il est alors immédiat de faire les calculs suivants : $z^2$ (log discret double modulo 15), $1/z$ (opposé du log discret modulo 15, donc $15 - \log(z)$ pour $z \neq 1$), puis par addition ordinaire modulo 2, les valeurs de $z^2 + z$ et de $z + 1/z$. Vous devez donc avoir 6 colonnes : $n = \log(z)$, $z = \alpha^n$, $z^2$, $1/z$, $z^2 + z$ et $z + 1/z$.

3) On considère la courbe elliptique $E$ sur $\mathbb{F}_2$ vue en devoir d'équation

$$y^2 + xy = x^3 + x .$$

On a calculé que son discriminant est égal à $-63$, ce qui est non nul dans $\mathbb{F}_2$, donc il est inutile de redémontrer que c'est une courbe elliptique. On rappelle qu'une équation $y^2 + by + c = 0$ possède une solution dans $\mathbb{F}_{16}$ si $b = 0$, et sinon possède 2 ou 0 solutions selon que $c/b^2$ est de la forme $z^2 + z$ ou non.

En remarquant que $(x^3 + x)/x^2 = x + 1/x$ et en utilisant le tableau fait ci-dessus qui donne à la fois les $x + 1/x$ et les $z^2 + z$, compter le nombre de points de $E$ dans $\mathbb{F}_{16}$. Ne pas oublier le point à l'infini, mais également le point éventuel avec $x = 0$.

4) (Facultatif.) Même question pour la courbe elliptique $y^2 + xy = x^3 + \alpha x$ (il faut ici faire la colonne des $z + \alpha/z$).