Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

Examen du 16 juin 2022

Durée 2h

Les documents du cours et des travaux dirigés, ainsi que les calculatrices portables, sont autorisés. Les ordinateurs portables sont interdits. Toutes les réponses doivent être soigneusement justifiées.

Les quatre exercices sont indépendants.

Exercice 1

Posons $N = 481$.

1) Factoriser l'entier N avec la méthode rho de Pollard, en utilisant le couple (f, x_0) où $f = X^2 + 1 \in \mathbb{Z}[X]$ et $x_0 = 3$.
2) Résoudre l'équation $x^2 = 1$ dans l'anneau $\mathbb{Z}/N\mathbb{Z}$.

Exercice 2

Dans l'anneau $\mathbb{F}_2[X]$, posons $f = X^3 + X + 1$. Considérons l'anneau quotient

$$K = \mathbb{F}_2[X]/(f).$$

1) Montrer que K est un corps. Quel est son cardinal ?

   Soit α la classe de X modulo l'idéal (f).

2) Justifier pourquoi α est un générateur de K^*.
3) Une personne Alice souhaite permettre à quiconque de lui envoyer des messages confidentiels sous forme d'éléments de K en utilisant l'algorithme de El Gamal. Pour cela, elle publie le triplet $(K, \alpha, \alpha^2 + 1)$.

   3.1) Quelle est la clé secrète d'Alice ?

   3.2) Bob envoie à Alice le couple (α^2, α). Quel est le message décrypté ?

Exercice 3

Soient p un nombre premier congru à 1 modulo 4 et E une courbe elliptique supersingulière définie sur $\mathbb{F}_p$.

1) Quel est l'ordre du groupe $E(\mathbb{F}_p)$ des points de E rationnels que $\mathbb{F}_p$?
2) En utilisant le théorème 4.5 du cours, montrer que $E(\mathbb{F}_p)$ est un groupe cyclique.

Exercice 4

Soit E la courbe projective plane sur $\mathbb{F}_7$ d'équation

$$y^2z = x^3 + 2xz^2 + 3z^3.$$

1) Décrire le groupe $E(\mathbb{F}_7)$ des points de E rationnels sur $\mathbb{F}_7$. En déduire que $E(\mathbb{F}_7)$ est cyclique d'ordre 6.
2) Quel est le point d'ordre 2 de $E(\mathbb{F}_7)$?

Posons désormais

$$P = (3, 1) \in E(\mathbb{F}_7).$$

3) Montrer que P est d'ordre 3.
4) En déduire quels sont les générateurs du groupe $E(\mathbb{F}_7)$.

Notons $\mathbb{F}_{7^n}$ le corps de cardinal 7^n dans une clôture algébrique de $\mathbb{F}_7$.

5) Quel est le polynôme caractéristique du Frobenius de E ?
6) Calculer l'ordre de $E(\mathbb{F}_{49})$.
7) Quel est le corps des points de 2-torsion de E ?
8) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{49})$.
9) Notons ϕ_7 l'endomorphisme de Frobenius de E. Soient R un point de E et $n \geq 1$ un entier. Montrer que R appartient à $E(\mathbb{F}_{7^n})$ si et seulement si $\phi_7^n(R) = R$.

Soit $E[3]$ le groupe des points de 3-torsion de E.

10) Soit Q un point de $E[3]$ tel que (P, Q) soit une base de $E[3]$ sur $\mathbb{Z}/3\mathbb{Z}$. Soit M la matrice de ϕ_7, restreint à $E[3]$, dans la base (P, Q). En utilisant un théorème du cours que l'on précisera, montrer qu'il existe a non nul dans $\mathbb{Z}/3\mathbb{Z}$ tel que l'on ait

$$M = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

11) Que vaut M^3 ?
12) En déduire quel est le corps des points de 3-torsion de E.
13) Calculer l'ordre de $E(\mathbb{F}_{7^3})$.
14) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{7^3})$.
