UE MA9W05

Algorithmique de la cryptographie à clés publiques

Master mentions *Mathématiques* et *Informatique*

Enseignant responsable : Jean-Marc Couveignes.

Examen du 16/12/2011, de 8h30 à 11h30 (trois heures)

⋆ ⋆ ⋆

Documents et calculette autorisés.

⋆ ⋆ ⋆

Ce sujet comporte deux pages.

Exercice 1 : Résoudre l'équation $x^3 = 5 \bmod 13$.

Résoudre l'équation $x^3 = 6 \bmod 13$.

Résoudre l'équation $x^3 = 2 \bmod 11$.

Exercice 2 :

Soit p un nombre premier congru à 2 modulo 3. Soit $a \in \mathbb{Z}/p\mathbb{Z}$. On considère l'équation

$$x^3 = a,$$

pour x dans $\mathbb{Z}/p\mathbb{Z}$. Combien cette équation a-t-elle de solutions ?

Que se passe-t-il si p est congru à 1 modulo 3 ?

Donnez un algorithme efficace pour calculer les solutions de l'équation $x^3 = a$ dans $\mathbb{Z}/p\mathbb{Z}$. Quelle est la complexité de cet algorithme (le nombre d'opérations élémentaires) en fonction de p ?

Exercice 3 : Donnez une description (en pseudo code) de l'algorithme d'Euclide étendu.

On considère les deux polynômes $a(x) = x^2 - x + 1$ et $b(x) = x^3 - x - 1$ dans $\mathbb{F}_3[x]$.

En utilisant l'algorithme d'Euclide étendu, calculer le pgcd $c(x)$ de $a(x)$ et $b(x)$ ainsi que deux polynômes $u(x)$ et $v(x)$ dans $\mathbb{F}_3[x]$ tels que $u(x)a(x) + v(x)b(x) = c(x)$.

Exercice 4 :

Montrez que le polynôme $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ est irréductible.

On note $\mathbf{K}$ le quotient $\mathbb{F}_2[x]/f(x)$. Montrez que $\mathbf{K}$ est un corps.

On note $\mathbf{K}^*$ le groupe des éléments non-nuls de $\mathbf{K}$. On note $g = x \bmod f(x)$ la classe de x modulo $x^4 + x + 1$.

Montrez que g est un générateur de $\mathbf{K}^*$.

Écrire la table des exponentielles et des logarithmes discrets en base g.

Exercice 5 : Décrivez un protocole cryptographique reposant sur la difficulté de calculer un logarithme discret.

Illustrer ce protocole à l'aide d'un exemple simple (par exemple en utilisant les résultats de l'exercice précédent).

Exercice 6 :

On dispose d'un générateur aléatoire qui retourne un nombre entier entre 0 et 255 avec distribution uniforme. On veut utiliser efficacement ce générateur pour tirer un nombre entier au hasard entre 1 et 6 avec distribution uniforme. Comment faire ?

On veut utiliser efficacement ce même générateur pour tirer un nombre entier au hasard entre 1 et 100000 avec distribution uniforme. Comment faire ?

Exercice 7 : Soit $\mathbf{K} = \mathbb{Z}/5\mathbb{Z}$ le corps à 5 éléments. Soit E la courbe elliptique sur $\mathbf{K}$ d'équation affine $y^2 = x^3 + x + 1$.

Écrivez les bornes de Hasse. Dans quel intervalle se trouve le cardinal de $E(\mathbf{K})$?

Montrez que les points $P = (0,1)$ et $Q = (4,2)$ appartiennent à $E(\mathbf{K})$.

Calculer $P + Q$ en détaillant toutes les étapes (en particulier le calcul de l'équation de la droite sécante).

Calculer $2P$ en détaillant toutes les étapes (en particulier le calcul de l'équation de la droite tangente).

Montrez que $E(\mathbf{K})$ est d'ordre 9 et que P est un générateur de ce groupe.

Exercice 8 : On veut factoriser le nombre $N = 7571$ en utilisant le crible quadratique.

1 . On observe que $\sqrt{N} \simeq 87.011493$. Écrivez une congruence modulo N du type

$$(a+m)^2 \equiv a^2 + u_1 a + u_0 \bmod N$$

dépendant d'un paramètre entier a. Ici m, u_0, u_1 sont des constantes entières bien choisies.

2 . Cherchez des valeurs de a comprises entre -6 et 6 qui permettent d'obtenir une congruence entre un carré et un nombre 11-friable modulo N. Vous expliquerez comment utiliser un crible, c'est-à-dire un tableau contenant toutes les valeurs de a. Vous illustrerez en détail l'utilisation de ce crible.

3 . Écrivez proprement toutes les congruences intéressantes obtenues. Portez les signes et les valuations dans une matrice M à coefficients entiers.

4 . Calculez le noyau de la réduction modulo 2 de la matrice M. Donnez la dimension de ce noyau, ainsi qu'une base.

5 . Pour chaque élément de cette base écrivez une congruence entre deux carrés modulo N. En déduire une factorisation (éventuellement triviale) de N.

Exercice 9 : On cherche un nombre premier p de 2000 bits tel que $p - 1$ soit divisible par un nombre premier q aussi grand que possible.

Donnez un méthode efficace pour trouver un tel nombre premier ? Quelle est la complexité de cette méthode ?

Quel est l'intérêt cryptographique d'un tel nombre premier ?
