Faculté des Sciences et Techniques de Limoges 2016–2017
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Contrôle du 13 décembre 2016 (durée 1h30)

Seuls documents autorisés : Notes personnelles manuscrites.

Les exercices sont indépendants.

A. Racines cubiques et factorisation

1. – Soit p un nombre premier congru à 1 modulo 3, et soit x un cube modulo p (i.e. il existe y tel que $y^3 \equiv x$ modulo p. Combien de racines cubiques a x modulo p ?

2. – Même question modulo q nombre premier congru à 2 modulo 3.

Pour le reste de l'exercice, on pose $N = pq$ avec p, q premiers distincts, différents de 2 et 3. Dans un premier temps on suppose p et q congrus à 1 modulo 3.

3. – On suppose que x est un cube modulo N et que $\text{pgcd}(x, N) = 1$. Combien x a-t-il de racines cubiques modulo N ?

4. – On suppose que x est un cube modulo N et que $\text{pgcd}(x, N) = 1$. Montrer que la donnée de deux racines cubiques y et z de x modulo N peut dans certains cas permettre de factoriser de N. Avec quelle probabilité obtient-on une factorisation non triviale de N lorsque y et z sont des racines cubiques prises au hasard ?

5. – Montrer que la donnée d'un oracle calculant des racines cubiques modulo N permet de factoriser N en temps probabiliste polynomial.

6. – Que se passe-t-il si $p \equiv q \equiv 2$ modulo 3 ?

7. – Que se passe-t-il si $p \equiv 1$ et $q \equiv 2$ modulo 3 ?

B. Algorithme d'Adleman

L'algorithme d'Adleman permet de calculer des logarithmes discrets dans un corps fini premier. On souhaite ici calculer des logarithmes discrets sur un corps fini non premier.

8. – Déterminer l'ensemble $\mathcal{B}$ des polynômes unitaires irréductibles sur $\mathbb{F}_3$ de degré inférieur ou égal à 2.

9. – Montrer que le corps $\mathbb{F}_{243}$ est de la forme $\mathbb{F}_3[\alpha]$, où α vérifie la relation $\alpha^5 = \alpha + 2$.

10. – On donne l'expression de certaines puissances de α en polynômes u_i de degré $\leqslant 6$ en α :

$$\begin{cases} \alpha^{79} = u_1(\alpha) = \alpha^3 + 2\alpha^2 + 2\alpha + 1 \\ \alpha^{98} = u_2(\alpha) = 2\alpha^4 + \alpha^3 + 2\alpha^2 + 1 \\ \alpha^{103} = u_3(\alpha) = 2\alpha^4 + \alpha^3 + \alpha^2 \\ \alpha^{111} = u_4(\alpha) = 2\alpha^4 + \alpha^2 + 2\alpha + 1 \\ \alpha^{120} = u_5(\alpha) = \alpha^4 + 2 \end{cases}$$

Factoriser les polynômes $u_i(X)$ en produits d'éléments de $\mathcal{B}$.

11. – En déduire des relations faisant intervenir les logarithmes des éléments de $\mathcal{B}$ en base α.

12. – Calculer les logarithmes des éléments de $\mathcal{B}$ en base α.

13. – En déduire le logarithme de $\alpha^2 + 2$ en base α.