Master 1 M7 Cryptographie

Examen de janvier 2008

Exercice. 1

Pour factoriser l'entier $n = 24961$ en utilisant la méthode du crible quadratique, on considère la base de factorisation $B = \{-1,2,3,5,13,23\}$.

1) Expliquer pourquoi on a exclu les nombres $\{7,11,17,19\}$ de la base B.

2) On rappelle que $157 < \sqrt{24961} < 158$. Utiliser le tableau suivant pour la factorisation de n, en se servant de l'indication qui suit:

On cherche une relation de dépendance linéaire entre les vecteurs v_i. Les relations $v_2 + v_4 + v_5 = 0$ et $v_5 + v_6 + v_7 = 0$ n'aboutiront pas à une solution.

a_i	a_i^2(mod n)	b_i	$v_i \in (\mathbb{F}_2)^6$
151	-2160	$-2^4.3^3.5$	$v_1 = (1,0,1,1,0,0)$
155	-936	$-2^3.3^2.13$	$v_2 = (1,1,0,0,1,0)$
156	-625	-5^4	$v_3 = (1,0,0,0,0,0)$
157	-312	$-2^3.3.13$	$v_4 = (1,1,1,0,1,0)$
158	3	3	$v_5 = (0,0,1,0,0,0)$
159	320	$2^6.5$	$v_6 = (0,0,0,1,0,0)$
161	960	$2^6.3.5$	$v_7 = (0,0,1,1,0,0)$

Exercice. 2

Soit le nombre premier $p = 751$.

1. (a) Calculer l'inverse 4^{-1} de 4 dans $\mathbb{F}_p$.
   (b) Sachant que α est un carré de $\mathbb{F}_p$, expliquer pourquoi les racines carrées de α sont $\pm\alpha^{\frac{p+1}{4}}$.
2. Soit Γ la courbe d'équation $y^2 + y = x^3 - x$, définie sur le corps $\mathbb{F}_p$.
   (a) Ecrire le polynôme P, homogène de degré 3, associé à Γ dans le plan projectif $\mathbb{P}^2(\mathbb{F}_p)$.
   (b) Montrer que la courbe projective définie par $P(X,Y,Z) = 0$ possède sur la droite de l'infini $Z = 0$ un unique point Ω, dont on donnera les coordonnées homogènes.
   (c) Vérifier que cette courbe n'admet pas de point singulier.

   On note E la courbe elliptique sur $\mathbb{F}_p$ définie par $E = \Gamma \cup \{\Omega\}$, munie de la structure de groupe additif usuelle où Ω est l'élément neutre.
3. (a) Par le changement de variables $t = y + 376$, trouver a et b dans $\mathbb{F}_p$ tels que l'équation de Γ devienne $t^2 = x^3 + ax + b$.
   (b) Montrer que E possède au plus 1503 points.
   (c) En fait E possède $N = 727$ points. En déduire que $B = (0,0)$ est un générateur du groupe E.

4. Par le procédé cryptographique d'El Gamal elliptique, nous voulons envoyer le message-point $P_m = (x_m,y_m) = (562,576)$ de la courbe à un correspondant qui a fait savoir que sa clef publique est le point $C = (201,380)$.

   Nous connaissons aussi le point de base $B = (0,0)$ choisi sur sur la courbe. Et nous utilisons $k = 386$ pour chiffrer notre message.

   (a) Donner, en fonction de B, C, k, P_m l'expression du message chiffré que nous envoyons.

   (b) Expliquer comment notre correspondant peut déchiffrer.

   (c) Si nous voulons envoyer un nouveau message-point P_m, de valeur différente, pourquoi devons-nous choisir une nouvelle valeur de k?

   (d) Donner une méthode de calcul rapide du point $386(0,0)$.

   (e) Faire le calcul du message chiffré obtenu avec les valeurs données.

   Nous voulons maintenant envoyer le message en clair $STOP007$ que nous devons d'abord transformer en 7 messages-points de la courbe.

5. Pour cela, on fait correspondre les chiffres 0, ... ,9 du message aux entiers $0, \ldots, 9$ et les lettres du message $A, \ldots, Z$, aux entiers $10, \ldots, 35$. Chaque lettre ou chiffre du message est donc devenu un entier m avec $0 \leq m < M = 36$.
   Pour faire correspondre à m un point P_m de la courbe, on utilise l'algorithme probabiliste suivant:

   (i) choisir $d = 20$ tel que $M \times d = 720 < p = 751$

   (ii) faire correspondre à m l'élément $\widetilde{x}$ défini par $\widetilde{x} = md + j$, pour $1 \leq j \leq d$ représentant d'un $x \in \mathbb{F}_p$

   (iii) essayer les valeurs successives $j = 1, \ldots, d$, pour obtenir que $f(x) = x^3 + ax + b$ soit un carré de $\mathbb{F}_p$.

   (iv) En cas de succès en (iii), calculer y tel que $P_m = (x,y) \in E$.

   Questions:

   (a) Quelle méthode peut-on employer pour le test de (iii)?

   (b) Comment calculer y dans (iv)?

   (c) Quelle est la probabilité de ne trouver aucun point P_m correspondant à x, quand on fait varier j de 1 à d?

   (d) Pour un point $P_m = (x,y)$ obtenu ainsi, retrouver la valeur de m, en fonction de $\widetilde{x}$ et d.

   (e) Utiliser cet algorithme pour calculer P_m dans le cas du chiffre 0 (zéro), puis dans le cas de la lettre S.

   (f) Retrouver m, puis la lettre correspondante, pour le point de la courbe $P_m = (\,581, 395\,)$.

6. En prenant successivement les 7 valeurs $k = 386, 209, 118, 589, 312, 483, 335$, calculer le message chiffré par le procédé décrit en 4), qui correspond à $STOP007$.