UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2001–2002

DESS CCSI

TP de méthodes mathématiques en cryptographie

Durée 2 heures

On demande de rédiger tous les programmes en GP.

Soit p un nombre premier plus grand ou égal à 5. On rappelle que sous GP les éléments de $\mathbb{F}_p$, qu'on identifiera aux éléments de $\mathbb{Z}/p\mathbb{Z}$, s'écrivent sous la forme `Mod(a,p)` (avec un M majuscule). On pourra supposer si on le désire que p est une variable globale, sinon il faut le passer en paramètre partout.

1) On veut travailler dans le corps $\mathbb{F}_{p^2}$ à p^2 éléments. Pour cela, on va représenter $\mathbb{F}_{p^2}$ comme $\mathbb{F}_p[X]/((X^2 - d)\mathbb{F}_p[X])$, où $X^2 - d$ est un polynôme irréductible dans $\mathbb{F}_p[X]$. Il faut et il suffit pour cela que d soit un non résidu quadratique modulo p.

a) Ecrire une petite fonction qui, étant donné un nombre premier p, retourne un non résidu quadratique d modulo p (on rappelle que le nom sous GP du symbole de Legendre généralisé est `kronecker`). Désormais, le corps $\mathbb{F}_{p^2}$ sera représenté comme $\mathbb{F}_p[X]/((X^2 - d)\mathbb{F}_p[X])$, et donc un élément de ce corps pourra s'écrire dans GP sous la forme `Mod(a*x+b,x`^{2}`-d)`, où `a` et `b` sont dans $\mathbb{Z}/p\mathbb{Z}$.

b) Ecrire une fonction simple qui, étant donnée un élément non nul $u \in \mathbb{F}_{p^2}$ écrit sous la forme `Mod(a*x+b,x`^{2}`-d)`, calcule *l'ordre* de u, c'est à dire le plus petit exposant $n > 0$ tel que $u^n = 1$ dans $\mathbb{F}_{p^2}$.

c) Application numérique : pour $p = 71$, calculer une valeur convenable pour d, puis calculer l'ordre de `Mod(a*x+b,x`^{2}`-d)` en prenant pour a votre mois de naissance, et pour b votre jour de naissance (que bien sûr vous indiquerez dans le programme). Faire bien attention d'exprimer a, b et d comme des `Mod(n,p)`, sinon GP ne peut pas savoir que ce sont des éléments de $\mathbb{F}_p$.

2) Quand p est grand (disons $p > 10^5$), la fonction simple ci-dessus est beaucoup trop lente. Le but de cette question est d'écrire une fonction beaucoup plus rapide. On supposera quand même que la factorisation de $p - 1$ et de $p + 1$ n'est pas trop longue, ce qui est le cas si $p < 10^{50}$, par exemple.

a) En factorisant $p - 1$ et $p + 1$ séparément, écrire une fonction qui calcule (comme vecteur de GP) la liste des diviseurs premiers de $p^2 - 1$.

Fonctions GP à utiliser : la fonction `factor(n)` rend une matrice `M` à k lignes et 2 colonnes, la première colonne (à laquelle on accède par `M[,1]`) représentant les k facteurs premiers, la deuxième (`M[,2]`) les exposants.

Pour faire la réunion (*pas* la concaténation) de deux vecteurs `v1` et `v2`, utiliser la commande `eval(Set(concat(v1,v2)))`. La longueur (d'un vecteur ou autre) est obtenue par la fonction `length`.

b) L'ordre de u comme ci-dessus peut se calculer intelligemment grâce à l'algorithme suivant (qu'on ne demande pas de justifier, bien que ce soit facile) :

1. [Initialisations] Poser $n \leftarrow p^2 - 1$, et grâce à la question a), calculer les diviseurs premiers de $p^2 - 1$, notés $p_1, p_2, \ldots, p_k$.

2. [Boucle en p_j] Pour j allant de 1 à k, effectuer l'étape **3**, puis retourner n et terminer l'algorithme.

3. [Boucle centrale] Poser $r \leftarrow 1$, puis tant que p_j divise n et $r = 1$, poser $m \leftarrow n/p_j$, calculer $r \leftarrow u^m$, et si $r = 1$ poser $n \leftarrow m$.

Ecrire une fonction GP implantant cet algorithme. La commande GP principale à utiliser est `while` (syntaxe `while(condition, suite de commandes séparées par des ``;'' puis ``)'')`.

c) Application numérique : prendre pour p le plus petit nombre premier plus grand que 10^{40} (fonction `nextprime`), pour a et b les mêmes valeurs que dans l'application numérique ci-dessus, et calculer l'ordre du u correspondant. Attention à bien modifier `a` et `b` dans le programme, puisque auparavant c'étaient des quantités modulo p avec $p = 71$, et que maintenant p a changé.

3) Un théorème important affirme que le groupe multiplicatif d'un corps fini est *cyclique*. En particulier, cela implique que pour tout p, dans le corps $\mathbb{F}_{p^2}$ il existe un générateur, c'est-à-dire un élément u d'ordre égal à $p^2 - 1$. Nous écrirons comme d'habitude u sous la forme `Mod(a*x+b,x^2-d)`.

Il est facile de voir (petit théorème de Fermat dans $\mathbb{F}_p$) que si $a = 0$ l'ordre de u divise $p - 1$, et si $b = 0$ il divise $2(p - 1)$. Il en résulte que l'on doit avoir a et b différents de 0 dans $\mathbb{F}_p$.

a) Ecrire une fonction de p qui calcule un générateur u de $\mathbb{F}_{p^2}$. On pourra utiliser la fonction `random()` qui pour génère un nombre pseudo-aléatoire compris entre 0 et $2^{31} - 1$ inclus. Attention, il y a un piège ici : comme la variable p a été utilisé comme variable globale dans les autres programmes (à moins que vous ayez fait autrement), il faut la mettre à sa valeur. Il faut donc écrire une fonction d'une autre variable, q par exemple, et commencer le programme en posant $p = q$, affectation d'une variable locale dans une variable globale.

Calculer un tel u explicitement pour $p = 10^{40}$. On fera la commande `setand(1)` (qui réinitialise le générateur de nombres pseudo-aléatoire) juste avant d'exécuter le programme.

b) Il résulte de la cyclicité de $\mathbb{F}_{p^2}^*$ qu'un élément α est un carré dans $\mathbb{F}_{p^2}^*$ si et seulement si $\alpha^{(p^2-1)/2} = 1$. Ecrire une fonction `krop2(v)` analogue au symbole de Legendre, qui pour $v \in \mathbb{F}_{p^2}$ rend 0 si $v = 0$, 1 si v est un carré dans $\mathbb{F}_{p^2}^*$, et -1 sinon.

4) On considère l'équation $y^2 = x^3 + ax + b$, où à nouveau a est votre mois de naissance et b votre jour de naissance. Pour tout nombre premier p ne divisant pas $-16(4a^3 + 27b^2)$, ceci définit une courbe elliptique E à coefficients dans $\mathbb{F}_p$.

a) En utilisant la formule

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{0 \le m \le p-1} \left(\frac{m^3 + am + b}{p}\right) ,$$

écrire un programme GP qui calcule $|E(\mathbb{F}_p)|$. Calculer ce cardinal pour $p = 137$ (E sera toujours une courbe elliptique dans ce cas).

b) En utilisant la formule analogue

$$|E(\mathbb{F}_{p^2})| = p^2 + 1 + \sum_{m \in \mathbb{F}_{p^2}} \texttt{krop2}(m^3 + am + b) ,$$

où `krop2` est la fonction introduite en 3b), écrire un programme pour calculer $|E(\mathbb{F}_{p^2})|$ (attention à la boucle sur m : $\mathbb{F}_{p^2}$ n'est bien sûr *pas* égal à $\mathbb{Z}/p^2\mathbb{Z}$). Calculer ce cardinal pour $p = 137$. Attention : ici les coefficients des éléments de $\mathbb{F}_{p^2}$ *doivent* être modulo p, donc il faut commencer par les forcer à être modulo p.

Vérification : on doit trouver

$$|E(\mathbb{F}_{p^2})| = |E(\mathbb{F}_p)|(2p + 2 - |E(\mathbb{F}_p)|) .$$