Université Bordeaux 1 — **MHT633 – Arithmétique et Cryptologie**
Mathématiques — Année 2008–2009

FEUILLE D'EXERCICES n° 5
Cryptographie asymétrique

Exercice 1 – Nous décrivons un chiffrement à clé publique par les données suivantes :

- $(G, \times)$ est un groupe abélien, H et K sont des sous-groupes de G tels que $H \cap K = \{1\}$ et $G = HK$. Tout élément $g \in G$ s'écrit alors $g = hk$ de façon unique, avec $h \in H$, $k \in K$. On note $\pi : G \to H$ l'homomorphisme surjectif défini par $\pi(g) = h$ si $g = hk$.
- L'espace des messages est un groupe H_0 isomorphe à H. On fixe un isomorphisme $f : H \to H_0$ et on suppose connue une application injective $i : H_0 \to G$ telle que $f \circ \pi \circ i(x) = x$ pour tout $x \in H_0$.
- La clé publique est (G, k) où $k \in K$ est un élément générateur de K (ou au moins d'un « gros » sous-groupe de K).
- La clé privée est la surjection $\pi : G \to H$.
- Le chiffrement est $e(x) = i(x)k^r$ où r est un entier choisi aléatoirement.
- Le déchiffrement est $d(y) = f \circ \pi(y)$.

1) Vérifiez que ces données définissent bien un système de chiffrement à clé publique. Quel est l'avantage de l'utilisation du nombre aléatoire r ?

2) On considère l'instanciation suivante : $n = pq$ est un produit de deux nombres premiers distincts et $G = (\mathbb{Z}/n\mathbb{Z})^*$. Rappelez pourquoi $G \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

3) On note H et K les sous-groupes de G canoniquement isomorphes à respectivement $(\mathbb{Z}/p\mathbb{Z})^*$ et $(\mathbb{Z}/q\mathbb{Z})^*$. Précisez les données du système dans ce cas.

4) Montrez que, pour que le système soit sûr n doit être suffisamment grand pour qu'il soit calculatoirement impossible de le factoriser.

5) Montrez que $k \equiv 1 \pmod{p}$ et en déduire que $p = \mathrm{pgcd}(k-1, n)$.

6) Expliquez pourquoi ce système n'est pas sûr !

Exercice 2 – [L'ALGORITHME ρ DE POLLARD POUR LE LOG DISCRET]

Soit G un groupe multiplicatif et $\alpha \in G$ un élément fixé d'ordre n. Soit $\beta \in \langle\alpha\rangle$ un élément dont on veut calculer le log discret de base α. L'idée de l'algorithme est de calculer une suite $x_1, x_2, \ldots, x_i, \ldots$ d'éléments de G, de sorte qu'une collision $x_i = x_j$ pour $i < j$ permette de calculer $c = \log_\alpha(\beta)$. La suite des x_i est calculée en itérant une certaine fonction f. Plus précisément chaque élément x de la suite fait partie d'un triplet (x, a, b) vérifiant $x = \alpha^a\beta^b$. Les triplets (x_i, a_i, b_i) définissent une « marche aléatoire » dans un certain ensemble fini.

Description de l'algorithme: On partitionne G en trois ensembles (disjoints) de même taille $G = S_1 \cup S_2 \cup S_3$ et on définit l'application $f : \langle\alpha\rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \langle\alpha\rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ par :

$$f(x,a,b) = \begin{cases} (\beta x, a, b+1) & \text{si } x \in S_1, \\ (x^2, 2a, 2b) & \text{si } x \in S_2, \\ (\alpha x, a+1, b) & \text{si } x \in S_3. \end{cases}$$

On définit par récurrence la suite $U_i = (x_i, a_i, b_i)$, en posant

$$U_0 = (1,0,0), \quad U_i = f(U_{i-1}),\ i \geqslant 1.$$

Pour chaque i, on calcule $U_{2i} = f(f(U_{2i-2}))$ et $U_i = f(U_{i-1})$, et la condition $x_{2i} = x_i$ est testée ; si elle est vraie et si $(b_{2i} - b_i, n) = 1$, alors $c = \log_\alpha(\beta)$ est calculé par la formule : $c = (a_i - a_{2i})(b_{2i} - b_i)^{-1} \mod n$. Remarquer qu'il n'est pas nécessaire de conserver en mémoire tous les U_i, il suffit d'un couple (U_i, U_{2i}) pour déterminer le couple suivant !

1) Montrez que, si (x, a, b) vérifie $x = \alpha^a\beta^b$, alors les triplets $(\beta x, a, b+1)$, $(x^2, 2a, 2b)$ et $(\alpha x, a+1, b)$ vérifient la même relation. En déduire que $x_i = \alpha^{a_i}\beta^{b_i}$, pour tout $i \geqslant 0$.

2) On suppose qu'une collision $x_j = x_i$ se produit pour $i < j$.

a) Montrez que si $(b_j - b_i, n) = 1$, alors $c = (a_i - a_j)(b_j - b_i)^{-1} \mod n$.

b) Montrez qu'il existe s tel que $x_s = x_{2s}$ avec $s < j$.

3) Soit $G = (\mathbb{Z}/p\mathbb{Z})^*$ avec p un nombre premier. On propose de prendre pour S_1, S_2, S_3, les trois classes de congruence modulo 3. Expliquez pourquoi on ne doit pas avoir $1 \in S_2$.

4) On prend $p = 47$ et $\alpha = 2$. Montrez que α est d'ordre 23. On cherche le log de 37 en base α. Expliquez pourquoi le choix

$$\begin{aligned} S_1 &= \{0 \leqslant x \leqslant p-1 \colon x = 1 \mod 3\}, \\ S_2 &= \{0 \leqslant x \leqslant p-1 \colon x = 0 \mod 3\}, \\ S_3 &= \{0 \leqslant x \leqslant p-1 \colon x = 2 \mod 3\} \end{aligned}$$

n'est pas satisfaisant en essayant de faire marcher l'algorithme. Faites-le ensuite fonctionner pour

$$\begin{aligned} S_1 &= \{0 \leqslant x \leqslant p-1 \colon x = 2 \mod 3\}, \\ S_2 &= \{0 \leqslant x \leqslant p-1 \colon x = 0 \mod 3\}, \\ S_3 &= \{0 \leqslant x \leqslant p-1 \colon x = 1 \mod 3\}. \end{aligned}$$

Exercice 3 – [Algorithme du calcul d'indice pour le log discret]

Soit $p = 227$. L'élément $\alpha = 2$ est primitif dans $(\mathbb{Z}/p\mathbb{Z})^*$. La notation log désigne le log discret de base α dans $(\mathbb{Z}/p\mathbb{Z})^*$.

1) Calculez α^{32}, α^{40}, α^{59} et α^{156} modulo p et factorisez-les sur la base de facteurs $\{2, 3, 5, 7, 11\}$.

2) En déduire le calcul de $\log 3$, $\log 5$, $\log 7$, $\log 11$.

3) On veut calculer $\log 173$. Multipliez 173 par le nombre « aléatoire » $2^{177} \mod p$. Factorisez le résultat sur la base de facteurs puis calculez $\log 173$ en utilisant les questions précédentes.