Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 4 : Logarithme discret

Exercice 1. Cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p-1$. Montrer qu'il existe $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $y^{(p-1)/q} \neq 1$. En déduire qu'il existe un élément x d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Soit q^α la plus grande puissance de q qui divise $p-1$. Montrer qu'il existe un élement y de $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que $y^{(p-1)/(q^\alpha)} \neq 1$.
3. Soit $x_y = y^{(p-1)/q^\alpha}$. Montrer que l'ordre de x_y est q^k avec $0 \leq k \leq \alpha$.
4. Supposons que $k \leq \alpha - 1$ pour tout x_y. Montrer que tout élément du groupe y vérifie $y^{(p-1)/q^{\alpha-k}} = 1$. En déduire l'existence d'un élément x d'ordre q^α.
5. Dans $(\mathbb{Z}/p\mathbb{Z})^\times$, si x est un élément d'ordre a et y d'ordre b avec a et b premiers entre eux, quel est l'ordre de xy ? Conclure.

Exercice 2. Le logarithme discret

Soit G un groupe cyclique d'ordre n dont la loi est notée multiplicativement et α un générateur de G.

1. Monter que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que l'application exponentielle de base α est une bijection de $\{0, 1, \ldots, n-1\}$ sur G. Le logarithme est son application réciproque.
3. Soit $G = (\mathbb{Z}/11\mathbb{Z})^\times$. Vérifier que 2 est un générateur de G. Calculer le logarithme en base 2 de 3.

Exercice 3. Calculs d'indices

Soit $p = 227$. $\alpha = 2$ est un élément primitif dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Calculer α^{32} modulo p. De même, on obtient $\alpha^{40} = 110, \alpha^{59} = 60$ et $\alpha^{156} = 28$ modulo p.
2. Factoriser ces puissances sur la base $\{2, 3, 5, 7, 11\}$. En déduire les valeurs de $\log_2(3), \log_2(5), \log_2(7)$ et $\log_2(11)$.
3. On veut calculer $\log_2(173)$. On choisit une puissance de 2 au hasard, disons 2^{177}. Le calcul donne $2^{177} = 123 \pmod p$. En factorisant 173.2^{177} modulo p sur notre base, trouver la valeur de $\log_2(173)$.

Exercice 4. Chiffrement d'Elgamal

Soit p un nombre premier et g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit x un entier tel que $1 \leq x \leq p-1$ et $y = g^x \pmod p$. Pour chiffrer $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ avec le chiffrement d'Elgamal, on choisit $r \in \mathbb{Z}/(p-1)\mathbb{Z}$. La fonction de chiffrement est alors :

$$e(m, r) = (g^r \pmod p,\ my^r \pmod p)$$

et la fonction de déchiffrement est :

$$d(c_1, c_2) = c_2(c_1^x)^{-1} \pmod p.$$

1. Précisez les données $(\mathcal{P}, \mathcal{C}, \mathcal{E}, \mathcal{D})$. Quelle est la clé publique ? La clé privée ?
2. Montrer que si $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ alors $d \circ e(m) = m$.
3. On considère dans cette question la clé publique p_k suivante : $(p, g, y) = (31, 3, 15)$.
   (a) Peut on prendre une telle clé ?
   (b) Chiffrer le message $m = 5$ à l'aide de cette clé (on prendra $r = 8$).
   (c) Le message chiffré $(6, 14)$ a été obtenu à l'aide de la clé p_k. Trouver la clef secrète correspondante et déchiffrer.

Exercice 5. Signature d'Elgamal

Soit p un nombre premier, g un générateur du groupe $\left((\mathbb{Z}/p\mathbb{Z})^\times, \times\right)$. Soit x un entier tel que $1 \leq x \leq p-1$ et $y = g^x \pmod p$

On choisit un nombre aléatoire (secret) : $r \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$. On signe alors le message $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ à l'aide de la fonction :

$$sig(m, r) = \left(g^r \mod p, (m - xw)r^{-1} \mod p - 1\right)$$

avec $w = g^r \mod p$.

1. Montrer que $(sig(m, r) = (w, s)) \iff (y^w w^s \equiv g^m \mod p)$
2. En déduire que $ver\,(x, (w, s)) = vrai \iff (y^w w^s \equiv g^m \mod p)$. De quoi a-t-on besoin pour effectuer la vérification ?
3. Dans cette question on prends $p = 47$, $g = 11$ et $x = 8$.
   (a) Vérifiez que g est un générateur de $(\mathbb{Z}/47\mathbb{Z})^\times$ et calculer y.
   (b) Signez le message $m = 12$ (en utilisant $r = 5$).
   (c) Vous recevez le message $m = 2$ avec la signature $(11, 6)$. La signature est elle valide ?

Exercice 6. Attaque de signature d'Elgamal

Dans cette exercice on cherche à falsifier une signature.

1. Montrer que si r est dévoilé on peut casser le système de signature.
2. Dans cette question on construit un triplet $(m, (w, s))$ valide.
   (a) En utilisant l'équation que doit vérifier le triplet et en écrivant $w = g^i y^j$ où $1 \leq i, j \leq p-2$, montrer que :
   $$y^{w+sj} \equiv g^{m-is} \pmod{p}$$
   (b) En déduire une condition suffisante sur $w + sj$ et $m - is$.
   (c) Expliquez comment choisir i et j pour avoir un triplet valide.

Exercice 7. Factorisation avec un logarithme

Soit p et q des nombres premiers impairs distincts et $n = pq$.

1. Soit α un inversible de $\mathbb{Z}/n\mathbb{Z}$. On note (α_p, α_q) son image dans $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. Montrer que :
   $$o(\alpha) = \text{ppcm}(o(\alpha_p), o(\alpha_q))$$
   où $o(x)$ est l'ordre de x.
2. Soit $d = \text{pgcd}(p-1, q-1)$. Montrer qu'il existe un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre $\frac{\varphi(n)}{d}$. Dans la suite on suppose de plus que $p > 3$ et $q > 3$ et $\text{pgcd}(p-1, q-1) = 2$.
3. Soit α un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre $\frac{\varphi(n)}{2}$ et $a \in \{0, 1, \ldots, \frac{\varphi(n)}{2} - 1\}$ le logarithme de α^n en base α. Montrer que $n - a = \varphi(n)$.
4. Ecrire un algorithme qui prend pour entrées n et a et qui renvoie les facteurs p et q de n.
5. Montrer que le coût de votre algorithme est polynomial en la taille de n. On utilisera une méthode dichotomique pour le calcul de la racine carré dans $\mathbb{Z}$.