Aix-Marseille Université
Préparation à l'agrégation: Option C
http://iml.univ-mrs.fr/~kohel/tch/Agreg/

Arithmétique d'ElGamal et de RSA

Exercices

Structure de $(\mathbb{Z}/N\mathbb{Z})^*$

1. Montrer que $a = 5$ est un élément primitif du groupe $(\mathbb{Z}/23\mathbb{Z})^*$, et remplir la table ci-dessous des valeurs.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
a^k																							

Résoudre le logarithme discret $\log_a(b)$ pour $b = 7$.

2. Résoudre le logarithme discret $\log_a(b)$ pour $a = 5$ et $b = 7$ dans $(\mathbb{Z}/17\mathbb{Z})^*$ en utilisant le méthode de Pohlig-Hellman.

3. Montrer que $(\mathbb{Z}/13\mathbb{Z})^* \cong (\mathbb{Z}/12\mathbb{Z}, +) \cong (\mathbb{Z}/3\mathbb{Z}, +) \times (\mathbb{Z}/4\mathbb{Z}, +)$. Expliciter ces isomorphismes avec un élément primitif mod13 et des éléments d'ordre 3 et 4.

ElGamal

4. Pour chaque p dans $\{101, 103, 107\}$ et a dans $\{2, 3, 5\}$, déterminer si a est un élément primitif de $\mathbb{F}_p^*$.

5. Soit donée (a, a^x, a^y) égal dans le tableau ci-dessous :

p	a	a^x	a^y
101	2	50	55
103	5	70	99
107	2	20	72

Vérifier que $x = 49$ dans les trois cas, et trouver a^{xy}.

6. Pour $(p, a, a^y) = (103, 5, 99)$, déterminer y en utilisant le méthode de pas de bébé, pas de géant. Idem pour $(p, a, a^y) = (107, 2, 72)$.

7. Pour $(p, a, a^y) = (101, 2, 55)$, déterminer y en utilisant le méthode de Pohlig–Hellman.

RSA

8. Soit $n = 19 \cdot 23 = 437$, et $(n, e) = (437, 17)$ une clé publique RSA. Trouver le chiffrement de $m = 11$. **Indication :** Commencer par remplir la table ci-dessous.

i	0	1	2	3	4
2^i	1	2	4	8	16
m^{2^i}	11				

9. Trouver la clé privée d en utilisant la factorisation de n.

10. Pour deux entiers n_1 et n_2, mettre $r = \text{ppcm}(n_1, n_2)$ et $s = \text{pgcd}(n_1, n_2)$. Montrer que $\mathbb{Z}/r\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ est une injection, et que le noyau de

$$\mathbb{Z}/n_1n_2\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

est $r\mathbb{Z}/n_1n_2\mathbb{Z}$.

11. Trouver $d_1 = e^{-1} \bmod (p-1)$ et $d_2 = e^{-1} \bmod (q-1)$, pour $(p, q) = (19, 23)$. Comment est-ce qu'on sait qu'il existe d tel que

$$d_1 = d \bmod (p-1) \text{ et } d_2 = d \bmod (q-1)?$$

12. Décrire l'algorithme pour déchiffrement de $c = 83$ en utilisant (d_1, p) et (d_2, q), et montrer comment retrouver le message m.

Factorisation

13. Le cible quadratique utilise les expressions de la forme $x^2 - n$ pour factoriser n. Retrouver la factorisation de $n = 437$ avec les valeurs de la table ci-dessous.

x	$x^2 - 437$
17	$-148 = -4 \cdot 37$
20	-37
21	4

14. Trouver la factorisation de $n = 5938201$ avec les donnés suivants (avec x autour de $\sqrt{n} = 2436.84...$) :

x	$x^2 - n$
2427	$-47872 = -1 \cdot 2^8 \cdot 11 \cdot 17$
2435	$-8976 = -1 \cdot 2^4 \cdot 3 \cdot 11 \cdot 17$
2437	$768 = 2^8 \cdot 3$