Initiation à la cryptographie

Travaux Dirigés de cryptographie n°6

—TELECOM Nancy 2A ISS—

1 Cryptographie sur les groupes

▸ **Exercice 1.** Chiffrement ElGamal

Le protocole de chiffrement ElGamal repose sur un groupe G cyclique d'ordre N. Soit g un générateur fixé de ce groupe. Bob génère les clés de la façon suivante :

(i) Il choisit $b \in \mathbb{Z}/N\mathbb{Z}$ au hasard et il en fait sa clé secrète $K_s = b$.

(ii) Il publie sa clé publique $K_p = g^b$.

Pour chiffrer un message $m \in G$, Alice tire $k \in \mathbb{Z}/N\mathbb{Z}$ et calcule g^k et $s = K_p^k$; le chiffré de m est alors $C = (g^k, m \cdot s)$.

1. Expliquer comment Bob peut déchiffrer le message.
2. Alice est fainéante : elle choisit d'utiliser plusieurs fois le même k. Quelles pourraient être les conséquences d'une telle paresse ? (On suppose qu'Eve connaît le message clair m d'un chiffré envoyé par Alice.)
3. Que pouvez vous dire de la malléabilité du chiffrement ElGamal ?

▸ **Exercice 2.** Exponentiation

Soit G un groupe. On souhaite s'intéresser à des opérations dans G. L'unité de mesure choisie est le produit dans G. On dit donc que le coût pour calculer le produit de a et b dans G est 1. De même, le coût pour calculer a^2 est 1.

Les entiers x et y, dans ce qui suit, sont des entiers de k bits.

— Par la méthode naïve consistant à multiplier a par lui-même x fois, quel est le coût du calcul de a^x ?

— Par la méthode d'exponentiation rapide, quel est le coût du calcul de a^x (donner une expression faisant apparaître séparément les carrés et les produits) ?

— Quel est le nombre de chiffres de l'écriture de x en base 4 ? Après le précalcul des grandeurs $\{1, a, a^2, a^3\}$, comment peut-on optimiser le calcul de a^x en l'exprimant à l'aide de produits et de puissances 4-èmes ?

— Soient a et b deux éléments de G. On souhaite calculer $a^x b^y$ plus efficacement qu'en calculant séparément les deux puissances. Montrer qu'on peut économiser la moitié des calculs de carrés. (On peut commencer en réfléchissant au calcul de $a^9 b^{14}$, par exemple. À titre d'indice, cet élément de G peut être calculé à partir de $a^4 b^7$ au moyen d'un produit et d'un carré).

▸ **Exercice 3.** Courbe elliptique

Un courbe elliptique est l'ensemble des solutions d'une équation du type $y^2 = x^3 + ax + b$, où les coefficients, ainsi que les solutions recherchées, appartiennent à un corps fini. On manipule ici un petit exemple sur $\mathbb{Z}/5\mathbb{Z}$, qui est un corps : on peut effectuer dedans des additions (modulo 5) et des produits (modulo 5). En outre, chaque élément non nul possède un inverse.

1. Quels sont les éléments de $\mathbb{Z}/5\mathbb{Z}$? Pour chacun, donner deux entiers de $\mathbb{Z}$ représentant ce même élément de $\mathbb{Z}/5\mathbb{Z}$.

2. Pour chaque élément de $\mathbb{Z}/5\mathbb{Z}$, calculer son carré dans $\mathbb{Z}/5\mathbb{Z}$. Combien le carré prend-il de valeurs distinctes sur $\mathbb{Z}/5\mathbb{Z}$?
3. Pour chaque élément de $\mathbb{Z}/5\mathbb{Z}$, calculer $f(x) = x^3 - 1$. En déduire les solutions de l'équation

$$y^2 = x^3 - 1 \tag{E}$$

(il y a 5 solutions distinctes).

4. Quelle est l'équation de la droite Δ passant par les points de coordonnées $(0, 2)$ et $(1, 0)$?
5. Soit (x, y) un point de la droite Δ satisfaisant aussi l'équation (E). L'abscisse x est alors solution d'une équation qu'on notera P. Quelle est cette équation (l'écrire – c'est une équation de degré 3).
6. Que peut-on dire de la somme des racines de P ? Connaissez-vous déjà es racines ? En déduire une nouvelle.
7. Si on « dessine » les points solution de (E), la droite Δ ressemble-t-elle à une droite ? Faire un dessin plus convaincant sur une feuille à petits carreaux, en répétant plusieurs fois un carré de côté 5 dans lequel vous aurez placé les points (ainsi, le «même» point a vocation à apparaître plusieurs fois sur votre dessin).

▸ **Exercice 4.** El Gamal plus rapide

On rappelle le système de chiffrement d'El Gamal. Pour fixer les idées, on se place dans le groupe $G = (\mathbb{Z}/p\mathbb{Z})^*$, où p est un nombre premier de 2048 bits. On note g un générateur de G. La clé secrète d'Alice est un entier $s \in [0, p-1]$, et sa clé publique est $h = g^s$. Le chiffré, calculé par Bob, d'un message $m \in G$ est la paire d'éléments : (mh^r, g^r), où r est un nombre aléatoire choisi par Bob.

— Combien d'opérations modulo p au maximum sont nécessaires pour calculer g^r ? Combien sont nécessaires en moyenne.
— Donner des exemples de value de r pour lesquelles le coût de calcul de g^r est nettement plus rapide (on ne se limitera pas à $0, 1, 2$).
— Bob n'a pas envie de passer trop de temps à chiffrer. Est-il pertinent de lui suggérer l'usage des «meilleures» valeurs de r ci-dessus ? Si non, pourquoi ? Si oui, dans quelles limites ?