Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Feuille de TD 4

18/02/2022

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/clef-publique.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

Exercice 1. $(\star)$ ElGamal : application directe.

En guise d'exercice d'application, on considère le cryptosystème d'ElGamal « brut » dans le groupe multiplicatif $\mathbb{F}_p^\times$ où $p = 19$.

Alice produit la clé privée $a = 5$.

Question 1.– Quelle est la clé publique ?

Question 2.– Chiffrer le message $m = 10$ avec l'aléa $k = 7$.

Question 3.– Déchiffrer $c = (12, 7)$ avec la clé privée d'Alice.

Exercice 2. $(\star)$ Attaque sur l'homomorphie du chiffrement d'ElGamal.

Question 1.– Démontrer que le chiffrement d'ElGamal dans sa version « brute », présenté dans un groupe $(\mathbb{G}, \cdot)$, est homomorphe. Autrement dit, démontrez que si m et m' sont deux clairs de chiffrés $c = (c_1, c_2)$ et $c' = (c'_1, c'_2)$, alors un chiffré possible de $m \cdot m'$ est $(c_1 \cdot c_2, c'_1 \cdot c'_2)$.

Application. Bob souhaite acheter une maison à Clara. Pour cela, il doit transmettre au notaire une promesse d'achat, sur laquelle il inscrit la somme qu'il souhaite payer à Clara.

On suppose que le notaire utilise le chiffrement ElGamal « brut », dans le groupe multiplicatif $\mathbb{F}_p^\times$, pour sécuriser la valeur entière (en euros) que Bob souhaite inscrire sur sa promesse de vente.

Ajoutons que la valeur du nombre premier p a été choisie suffisamment grande pour que le logarithme discret dans $\mathbb{F}_p^\times$ soit irrésoluble.

Question 2.– Supposons que Clara arrive à intercepter le message de Bob. Comment peut-elle le modifier pour faire croire au notaire que Bob souhaite payer 2 fois plus que la somme initialement prévue ?

Question 3.– Que proposeriez-vous au notaire pour empêcher cela ?

Exercice 3. $(\star\star)$ Une variante du chiffrement ElGamal.

Dans cet exercice, on se place dans le corps $\mathbb{F}_p$, avec p premier, et on considère g un générateur de $\mathbb{F}_p^\times$.

On s'intéresse à une variante du chiffrement ElGamal. La clé privée est toujous un élément aléatoire $a \in \mathbb{Z}/(p-1)\mathbb{Z}$, et la clé publique est toujours $\alpha = g^a$. En revanche, l'espace des clairs du système est $\mathbb{F}_p$, et celui des chiffrés est $\mathbb{F}_p \times \mathbb{F}_p^\times$. Enfin, l'algorithme de chiffrement est le suivant.

Algorithme 1 : Algorithme de chiffrement

Entrée : un message $m \in \mathbb{F}_p$, une clé publique α
Sortie : un chiffré $c = (c_1, c_2) \in \mathbb{F}_p^\times \times \mathbb{F}_p$

1 Choisir aléatoirement $r \in \mathbb{Z}/(p-1)\mathbb{Z}$.
2 Calculer $c_1 = g^r \mod p$.
3 Calculer $c_2 = \alpha^r + m$.
4 Retourner $c = (c_1, c_2)$.

Question 1.– Décrire précisément l'algorithme de déchiffrement associé (entrées, sortie, étapes), ainsi que sa complexité en fonction de p.

Question 2.– Supposons que Bob réutilise le même aléa à chaque chiffrement. Présenter une attaque contre le système en indiquant le mode d'attaque utilisé (c'est-à-dire, les moyens de l'attaquant).

Question 3.– Pourriez-vous instancier ce cryptosystème dans le groupe de points d'une courbe elliptique (au lieu de $\mathbb{F}_p$) ? Justifier : si oui, préciser les changements à effectuer ; si non, donner les obstacles.

Exercice 4. 💻 (⋆) Implantation de *baby-step giant-step.*

Question 1.– Implanter l'algorithme de calcul de logarithme discret dit « pas de bébé – pas de géant », dans le groupe multiplicatif d'un corps fini $\mathbb{F}_p^\times$.

Question 2.– Trouver les logarithmes discrets de $y \in \mathbb{F}_p^\times$ en base g pour les valeurs de p, g et y suivantes :

p	g	y
101	2	78
10007	5	8804
1000003	2	832469
100000007	5	29220559
10000000019	2	9521998688
1000000000039	3	855427796771

Jusqu'à quelle valeur de p le temps de calcul du logarithme discret par l'algorithme « pas de bébé – pas de géant » reste-t-il raisonnable sur votre machine ?

Et pour la recherche exhaustive ?

Exercice 5. 💻 (⋆⋆) Opérations sur une courbe elliptique.

Dans cet exercice, on se donne une courbe elliptique $E_{a,b}$ sur $\mathbb{F}_p$ d'équation de Weierstrass

$$y^2 = x^3 + ax + b\,.$$

À titre d'exemple et pour tester les fonctions implantées, on pourra utiliser $p = 89$ et $(a, b) = (1, 1)$, qui donne un groupe $E_{a,b}(\mathbb{F}_p)$ cyclique d'ordre $n = 100$ (donc isomorphe à $\mathbb{Z}/100\mathbb{Z}$) et de générateur le point $P = (27, 24)$.

Le but est d'obtenir une implantation (non-optimisée) du groupe des points rationnels de la courbe.

Un point rationnel de la courbe sera représenté sous la forme suivante :

— un couple (x, y) d'entiers modulo p si c'est un point situé dans le plan affine,
— une valeur facilement identifiable, notée `inf`, si c'est le point à l'infini. Par exemple, cette valeur pourra être simplement 0 (mais on se souviendra que c'est une convention pour représenter le point à l'infini).

Question 1.– Implanter deux fonctions

— `zero()` qui construit le point à l'infini `inf`, et
— `is_zero(P)` qui teste si `P` est le point à l'infini.

Question 2.– Implanter un algorithme `find_points(a, b, p)` qui retourne la liste des points rationnels de la courbe $E_{a,b}$. Cette fonction pourra avoir une mauvaise complexité algorithmique (par exemple $O(p^2)$).

Question 3.– Implanter un algorithme `random_point(L)` qui retrourne un point rationnel aléatoire tiré uniformément sur la courbe. La fonction prendra en entrée (un pointeur vers) la liste précalculée `L` des points de la courbe.

Question 4.– Implanter un algorithme `neg(P, p)` qui retourne l'opposé du point `P` pour la loi de groupe de $E_{a,b}(\mathbb{F}_p)$.

Question 5.– Implanter un algorithme `double(P, a, p)` qui retourne le double du point `P` pour l'opération de groupe de $E_{a,b}(\mathbb{F}_p)$.

Question 6.– Implanter un algorithme `add(P, Q, a, p)` qui retourne la somme de `P` et `Q` pour l'opération d'addition du groupe $E_{a,b}(\mathbb{F}_p)$. On prendra garde au cas où `P` et `Q` sont égaux, et au cas où `P` ou `Q` est le point à l'infini.

Question 7.– Implanter un algorithme `fast_mult(P, m, a, p)` qui calcule le multiple d'ordre `m` du point `P` dans le groupe $E_{a,b}(\mathbb{F}_p)$, en utilisant la méthode *double-and-add*.

Question 8.– Implanter un algorithme `ord(P, a, p, primes)` qui calcule l'ordre du point `P` dans le groupe $E_{a,b}(\mathbb{F}_p)$. Pour cela, on supposera avoir à disposition la liste `primes` des nombres premiers qui divisent l'ordre du groupe $E_{a,b}(\mathbb{F}_p)$.