Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2022–23

Cryptographie à clé publique – Devoir 2

17/02/2023

Consignes :

1. à rendre par email avant le vendredi 10/03/2023 (exceptionnellement 3 semaines) ;
2. le code doit être commenté ;
3. il est conseillé d'utiliser `python` et sa bibliothèque externe `cryptodome` et ses fonctions `getPrime, isPrime` si besoin, mais tout autre langage (standard) est accepté. Pour l'installation de `cryptodome`, suivre :
`https://pycryptodome.readthedocs.io/en/latest/src/installation.html`

Exercice 1. Implantation du chiffrement ElGamal sur les courbes elliptiques.

Dans cet exercice, on souhaite implanter le système de chiffrement ElGamal dans le groupe des points d'une courbe elliptique. Les 5 premières questions consistent à implanter les fonctions de manipulation de points de courbes elliptiques. Les questions 6 à 9 sont elles consacrées au chiffrement ElGamal.

Note. Si vous utilisez un logiciel de calcul formel (`sagemath` ou `magma`), veuillez ne pas utiliser directement les fonctions associées aux courbes elliptiques dans la partie 1. Le but est que vous les implantiez par vous-même.

Première partie.

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 $\mathbb{Z}/100\mathbb{Z}$), dont un générateur est 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 ici $\mathcal{O}$, si c'est le point à l'infini (qui est le "zéro" du groupe additif). Par exemple, cette valeur pourra être simplement stockée en machine comme l'entier 0, ou comme la chaîne de caractères `"zero"` ; on se souviendra que c'est une convention pour représenter le neutre du groupe.

Question 1.– Implanter deux fonctions

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

Question 2.– 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 3.– 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 4.– Implanter un algorithme `add(P, Q, a, p)` qui retourne la somme des points `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 5.– 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*.

Deuxième partie.

On suppose que sont donnés publiquement, dans une variable `param`, les paramètres su système de chiffrement ElGamal, à savoir :

— les valeurs de p, a, b ;
— un générateur G d'un sous-groupe cyclique $\mathbb{G}$ des points de la courbe elliptique ;
— l'ordre r du groupe $\mathbb{G}$.

Question 6.– En utilisant la connaissance du générateur G, de l'ordre r ainsi que la fonction de multiplication rapide implantée plus haut, écrire une fonction `random_point(param)` qui produit un point aléatoire de la courbe $E_{a,b}(\mathbb{F}_p)$.

Question 7.– Écrire une fonction `keygen(param)` qui produit un couple de clefs publique/privée à partir du nombre premier p, du générateur G et de l'ordre r du groupe.

Question 8.– Écrire une fonction `encrypt(M, pk, param)` qui chiffre un message `M`, donné sous la forme d'un point de la courbe, avec la clé publique `pk`.

Question 9.– Écrire une fonction `decrypt(C, sk, param)` qui déchiffre un chiffré `C`, donné sous la forme d'un couple de points de la courbe, avec la clé privée `sk`.

Question 10.– Pratique : dans le fichier accessible en ligne à l'adresse suivante :

`https://www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/docs/CP/devoir/EC_elgamal.txt`

vous trouverez des valeurs de p, a, b, G et r, ainsi qu'un chiffré $C = (C_1, C_2)$ sous la forme de deux points de la courbe $E_{a,b}(\mathbb{F}_p)$.

Déchiffrer le chiffré C et donner l'abscisse du message obtenu.