SORBONNE UNIVERSITÉ

Cryptographie basée sur les Courbes Elliptiques

Version du 9 avril 2022

TME

1 Notations

Soit p un nombre premier, $\mathbb{F}_p$ désigne le corps à p éléments. Dans ce TME, vous manipulerez des courbes $\mathcal{E}$ définies sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + ax + b$. Une telle courbe sera représentée par un triplet (p, a, b) où p est un nombre premier et $a, b \in \mathbb{F}_p$. Un point $P := (x, y)$ sera représenté par un couple (x, y) et le point à l'infini $\mathcal{O}$ sera représenté par le tuple vide $()$.

2 Questions

Question 1. Écrire une fonction `est_elliptique` qui prend en entrée une courbe $\mathcal{E} = (p, a, b)$ et renvoie `True` si cette courbe est elliptique et `False` sinon.

Question 2. Écrire une fonction `point_sur_courbe` qui prend en entrée un point P et une courbe $\mathcal{E}$ et renvoie `True` si le point P se trouve sur la courbe $\mathcal{E}$ et `False` sinon.

Question 3. Écrire une fonction `symbole_legendre` qui prend en entrée un entier a et un premier p et renvoie le symbole de Legendre de a mod p. Ce symbole est donné par l'expression $a^{\frac{p-1}{2}}$ mod p. Expliquer pourquoi.

Question 4. Écrire une fonction `cardinal` qui prend en entrée une courbe $\mathcal{E}$ et renvoie le nombre de points de cette courbe. Votre fonction doit être suffisament efficace pour passer le test 3.

Question 5. Écrire une fonction `liste_points` qui prend en entrée une courbe $\mathcal{E}$ et renvoie la liste des points de $\mathcal{E}$ (point à l'infini compris). On pourra utiliser que, lorsque p premier est congru à 3 mod 4, une racine carrée de a mod p est donnée par $a^{\frac{p+1}{4}}$ mod p. Vérifier ce résultat.

Question 6. Rappeler le théorème de Hasse. Écrire une fonction `cardinaux_courbes` qui prend en entrée un premier p et renvoie un dictionnaire dont les clés sont les cardinaux possibles pour une courbe elliptique définie sur $\mathbb{F}_p$. On associe à une clé c le nombre de courbes elliptiques définies sur $\mathbb{F}_p$ de cardinal c.

La fonction `dessine_graphe`, avec en entrée un premier p, utilise votre fonction `cardinaux_courbes` pour dessiner l'histogramme des cardinaux des courbes elliptiques définies sur $\mathbb{F}_p$.

Question 7. Écrire une fonction `est_egal` qui prend en entrée deux points P_1 et P_2 ainsi qu'un premier p et renvoie `True` si ces points sont égaux sur $\mathbb{F}_p$ et `False` sinon.

Question 8. Écrire une fonction `addition` qui prend en entrée deux points P_1 et P_2 ainsi que la courbe elliptique $\mathcal{E}$ à laquelle ils appartiennent et renvoie le point $P_1 + P_2$.

Question 9. Écrire une fonction `multiplication_scalaire` qui prend en entrée un entier k, un point P et la courbe elliptique $\mathcal{E}$ à laquelle il appartient et renvoie le point $[k]P$. Votre fonction doit être suffisament efficace pour passer le test 7.

Question 10. Écrire une fonction `ordre` qui prend en entrée un point P, la courbe elliptique $\mathcal{E}$ à laquelle ce point appartient, le cardinal N de la courbe et la factorisation de N en produits de facteurs premiers et renvoie l'ordre du point P dans le groupe de points de la courbe $\mathcal{E}$. On pourra utiliser la fonction `factor` qui prend en entrée un entier N et renvoie une liste de couples (p, a_p) où p est un diviseur premier de N et a_p est la valuation p-adique de N.

Question 11. Écrire une fonction `point_aleatoire_naif` qui prend en entrée une courbe $\mathcal{E}$ et renvoie un point (x, y) de $\mathcal{E}$ choisi aléatoirement. Cette fonction devra choisir x et y au hasard jusqu'à obtenir un point de la courbe. Estimer le nombre de points à tirer avant de trouver un point de la courbe $\mathcal{E}$. En déduire la complexité de votre fonction. Lancer votre fonction sur la courbe

$$\mathcal{E} = (360040014289779780338359, 11723570195835808591986 7, 18575864837248358617992)$$

Commenter.

Question 12. Améliorer la complexité de la fonction ci-dessus dans une nouvelle fonction `point_aleatoire`. Vous pourrez vous limiter aux courbes définies sur $\mathbb{F}_p$ pour p congru à 3 mod 4 et utiliser le calcul de racines carrées présenté précédemment. Donner la complexité de votre nouvelle fonction. Tester sur la courbe ci-dessus.

Question 13. Utiliser la fonction précédente et la fonction `ordre` pour écrire une fonction `point_ordre` qui prend en entrée une courbe $\mathcal{E}$, son cardinal N, la factorisation de son cardinal et un premier n divisant N et retourne un point d'ordre n.

Question 14. Application au protocole de Diffie-Hellman. Programmer l'échange de clé Diffie-Hellman. Pour cela, coder deux fonctions `keygen_DH` et `echange_DH`. La première prendra en argument une courbe $\mathcal{E}$, un entier n et un point d'ordre n et génèrera une clé publique et une clé privée pour l'échange Diffie-Hellman. `echange_DH` prend en entrée une clé secrète d'Alice, une clé publique de Bob ainsi que la courbe $\mathcal{E}$ et calcule la clé commune Diffie-Hellman.

Question 15. Etant donnés le premier $p = 24830176302272902765201974756837501232 3$ et la courbe $\mathcal{E} : y^2 = x^3 + x$ sur $\mathbb{Z}/p\mathbb{Z}$ de cardinal $N = 24830176302272902765201974756837501232 4$ dont la factorisation est donnée par $[(2, 2), \ (620754407556822569130049368920937530 81, 1)]$, trouver un bon point P pour un échange de clé Diffie-Hellman. Expliquer pourquoi ce point est bien et comment il a été trouvé.