D31: Protocoles cryptographiques
TD n 3: El Gamal / ECC

Exercice 1. Généralités

1. Sur quel problème repose la sécurité des cryptosystèmes ECC et El Gamal?
2. Pour les deux systèmes n'utilisent ils pas les mêmes tailles de clés à sécurité équivalentes?
3. Quel taille de corps de base doit-on choisir pour obtenir une sécurité de 192 bits avec ECC.

Exercice 2. Cryptosystème El Gamal

On considère le groupe $(\mathbb{Z}/23\mathbb{Z})^*$.

1. Quel est l'odre du sous groupe engendré par $\alpha = 3$?
2. On considère comme paramètres publics $\alpha = 3$ et $\beta = 18$. Quels sont les paramètres privés du systèmes? Chiffré les messages $m_1 = 2$ et $m_2 = 12$ en utilisant les entiers (supposés) générés aléatoirement $r_1 = 4$ et $r_2 = 10$.

Exercice 3. Cryptosystème ECC

On considère la courbe $E : y^2 = x^3 + x + 6$ définie sur $\mathbb{F}_{13}$.

1. Calculer la clé privée du système dont les paramètres publics sont:
   i. $P = (2, 4), Q = (9, 9)$
   ii. $P = (2, 9), Q = (9, 4)$
   iii. $P = (12, 2), Q = (4, 10)$.
2. Décompresser les points:
   i. $R = (11, 0)$
   ii. $R = (4, 1)$
   iii. $R = (12, 0)$

Exercice 4. Algorithme de Shanks

On considère un groupe cyclique $G =< \alpha >$ d'ordre n. Soit $\beta = \alpha^k$ pour un certain $k < n$.

1. Décrire à l'aide de l'algorithme de Shank comment trouver k en $O(\sqrt{n})$ étapes.
2. On suppose maintenant que l'on connait deux entiers s et t tels que $0 < s \leq k \leq t < n$. Modifier l'algorithme de Shank afin de retrouver k en $O(\sqrt{t-s})$ étapes.

Soit p un nombre premier. On considère maintenant une courbe elliptique E définie sur $\mathbb{F}_p$ d'ordre $\#E$ premier.

3. Montrer que $\log_P(-P) = \#E - 1$.
4. Donner un algorithme calculant $\#E$ en $O(p^{1/4})$ étapes (penser aux bornes sur le nombre de points d'une courbe).