Master 1	Spécialité : SI	TP Outils Mathématique pour la Cryptographie

Travail Pratique : Chiffrement Simplifié Elamal ECC

Travail demander

- ⌦ Programmer toutes les fonctions de base ECC.
- ⌦ Tester le chiffrement et déchiffrement ElGamal ECC.
- ⌦ Vérifier chaque étape et comprendre le rôle de chaque opération.
- ⌦ Un **rapport clair et structuré**.
- ⌦ Proposer un protocole de comparaison entre RSA et ElGamal ECC
- ⌦ Optionnel : Interface graphique de protocole de comparaison RSA et ElGamal ECC

1. Préparation

1) Choisir un petit corps premier $p < 1000$
2) Définir une courbe elliptique $y^2 = x^3 + ax + b \bmod p$
3) Condition pour éviter les points singuliers :$4a^3 + 27\,b^2 \not\equiv 0\ mod\ p$
4) Choisir un point générateur $\boldsymbol{P}$ appartenant à la courbe.
5) Définir la clé privée $\boldsymbol{d_A}$et calculer sa clé publique $\boldsymbol{Q_A = d_A P}$.
6) Choisir un message $\boldsymbol{M}$ représenté par un point sur la courbe.

2. Implémentation des fonctions ECC

Programmer en C (Dev C++) les fonctions suivantes :

1) Vérification qu'un point appartient à la courbe : bool Is_on_curve(Point P, int a, int b, int p);
2) Addition de deux points : Point Point_add(Point P, Point Q, int a, int p);
   Formules sur un corps premier $\mathbb{F}_p$:
   Si $P = (x_1, y_1)$et $Q = (x_2, y_2)$avec $P \neq Q$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$$
$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

3) Doublement d'un point : Point Point_double(Point P, int a, int p);
   Si $P = Q$(doublement) :

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$$
$$x_3 = \lambda^2 - 2x_1 \bmod p$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

4) Multiplication scalaire : Point Scalar_mult(int k, Point P, int a, int p); C'est l'addition répétée :

$$kP = \underbrace{P + P + \cdots + P}_{k \text{ fois}}$$

3. Chiffrement Elamal ECC

1. Choisir un entier aléatoire k.
2. Calculer $C_1 = kP$.
3. Calculer $C_2 = M + kQ_A$.

4. Afficher le couple chiffré (C_1, C_2).

4. Déchiffrement

1. utiliser la clé privée $d_A$pour calculer : $M_{dechiffre}$ = C_2 - d_A C_1
2. Vérifier que $M_{dechiffre} = M$.
3. Afficher le résultat et un message de validation.

5. Rapport et analyse

- Répondre aux questions :
    1. Quelle est la difficulté de retrouver $k$ou d_Aà partir de C_1et C_2?
    2. Comparer ce chiffrement ECC avec RSA en termes de **taille des clés et sécurité**.
    3. Décrire comment les opérations ECC (addition et multiplication de points) sont utilisées dans le chiffrement et le déchiffrement.

Exemple pédagogique

- Courbe : $y^2 = x^3 + 2x + 3 \bmod 97$
- énérateur : $P = (3,6)$
- Clé privée Alice : $d_A = 7$
- Clé publique : $Q_A = 7P = (80,10)$*(à calculer par l'étudiant)*
- Message : $M = (10,20)$
- Bob choisit $k = 3$
- Chiffrement :
    - $C_1 = 3P$
    - $C_2 = M + 3Q_A$
- Déchiffrement : $M = C_2 - 7C_1 = (10,20)$

Les étudiants doivent calculer toutes les coordonnées intermédiaires et vérifier que le message déchiffré correspond au message original.