UNIVERSITE MOHAMMED V ÉCOLE NATIONALE SUPÉRIEURE
D'INFORMATIQUE ET D'ANALYSE DES SYSTÈMES
ENSIAS - RABAT

FILIÈRE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Projet Cryptographie

Elliptic Curve Integrated Encryption Scheme (ECIES) with AES

Soutenu par :
SABIR YASSINE
AMAR ILYAS
HAYAR CHAIMA

Sous l'encadrement de :
M. BELKASMI MOSTAFA
M. EL GAABOURI ISMAIL

Année Universitaire 2022 - 2023

Résumé

Ce projet porte sur l'étude de la cryptographie sur les courbes elliptiques et son utilisation pour l'échange de clés pour un contexte de cryptographie symétrique, comme AES dans notre étude. Nous avons commencé par explorer les concepts fondamentaux des courbes elliptiques, les opérations qui peuvent être réalisées sur celles-ci et le problème du logarithme discret. Ensuite, nous avons examiné la cryptographie sur les courbes elliptiques, les clés AES et le protocole de Diffie-Hellman comme un moyen d'échanger les clés AES de manière sécurisée. Nous avons également discuté des applications pratiques de la cryptographie sur les courbes elliptiques ainsi que l'expérience que nous avons mené. Finalement, nous conclurons quant aux résultats de notre simulation.

Table des matières

Introduction générale **4**

1 Étude générale **5**

1.1 **Les courbes elliptiques** 5

1.1.1 Définition 5

1.1.2 Les opérations sur les courbes elliptiques 5

1.1.3 Problème du logarithme discret sur les courbes elliptiques . 6

1.2 Utilisation de la cryptographie sur les courbes elliptiques pour échanger les clés AES 7

1.2.1 la cryptographie sur les courbes elliptiques 7

1.2.2 Elliptic Curve Integrated Encryption Scheme 7

1.2.3 Les clés AES 8

1.2.4 Le protocole de Diffie-Hellman sur les courbes elliptiques . . 9

1.2.5 Les applications de ECIES 10

1.2.6 Les attaques courantes sur les implémentations spécifiques d'ECIES 11

2 Expérience **11**

3 Résultats **12**

Conclusion **15**

Bibliographie **16**

Liste des figures

1 L'addition dans une courbe elliptique 6
2 Les étapes du processus de chiffrement AES 8
3 Illustration du protocole de Diffie-Hellman sur les courbes elliptiques 10
4 Illustration du mode de fonctionement CBC de AES 12
5 Initialisation de l'expérience 13
6 Échange de clé entre les deux clients 13
7 Échange de données (cryptés) entre les deux clients 14

Introduction générale

La cryptographie à courbes elliptiques est une technique de cryptographie asymétrique qui repose sur la difficulté de résoudre le problème du logarithme discret dans le groupe de points d'une courbe elliptique sur un corps fini. Elle permet notamment de réaliser des échanges de clé et des signatures numériques avec une sécurité similaire à celle des systèmes RSA et DSA, tout en nécessitant des clés plus courtes et donc des calculs moins coûteux en termes de ressources.

L'échange de clé basé sur les courbes elliptiques est un protocole cryptographique qui permet à deux parties de générer une clé de chiffrement commune à partir d'une information publique échangée de manière sécurisée. Ce protocole est utilisé dans de nombreux systèmes cryptographiques, tels que SSL/TLS, SSH et IPSec, pour établir une communication sécurisée entre deux parties.

Dans ce rapport, nous allons explorer les courbes elliptiques et leur utilisation en cryptographie. Dans un premier temps, nous introduirons les courbes elliptiques et les opérations qui peuvent être effectuées sur ces courbes. Ensuite, nous aborderons le problème du logarithme discret sur les courbes elliptiques. Dans un second temps, nous expliquerons comment la cryptographie sur les courbes elliptiques peut être utilisée pour échanger les clés AES, qui est un algorithme de chiffrement symétrique largement utilisé. Nous présenterons également le protocole de Diffie-Hellman sur les courbes elliptiques. Ainsi, nous discuterons des applications de la cryptographie sur les courbes elliptiques dans divers domaines. En outre, nous discuterons brièvement des différentes attaques possibles sur la cryptographie avec les courbes elliptiques. Et finalement nous discuterons l'expérience et les résultats obtenus.

1 Étude générale

1.1 Les courbes elliptiques

1.1.1 Définition

On appelle courbe elliptique, toute courbe plane d'équation $y^3 = x^2 + ax + b$, ou le discriminant $-(4a^3 + 27b^2)$ de $x^3 + ax + b$ est non nul. On rajoute à cette courbe un point à l'infini noté O.

1.1.2 Les opérations sur les courbes elliptiques

Parmi les opérations qu'on peut effectuer sur les points d'une courbe elliptique on trouve **l'addition**, on fait on peut définir une opération d'addition sur les points d'un courbe elliptique C, de telle sort $(C, +)$ soit un groupe commutatif.

Soient P et Q deux points distincts d'un courbe elliptique C (différents du point à l'infini O), on définit $P+Q$, le résultat de l'addition des deux points P et Q, en traçant la droite (PQ) qui passe par P et Q, deux cas peuvent se produire :

- **La droite coupe la courbe C en un troisième point :** dans ce cas Le symétrie de ce troisième point par rapport à l'axe des abscisses $((\Delta) : x = 0)$est $P + Q$.
- **La droite ne coupe la courbe C qu'en P et Q :** ceci n'est possible que si la droite (PQ) est parallèle à l'axe des ordonnées$((\Delta) : y = 0)$. On définit alors $P + Q = O$ (point à l'infini).

Pour le cas si $P = Q$, on considère la tangente à la courbe C en P, et on définit $P + P$ comme ci-dessus. Enfin, on prolonge la définition de l'addition en posant $P + O = O + P = P$

On peut alors prouver que l'opération d'addition définit une loi de groupe sur la courbe elliptique. On peut d'ailleurs effectuer les calculs, pour obtenir les coordonnées de $P + Q$ en fonction de celles de P et de Q. Si $P(x_1, y_2)$, $Q(x_2, y_2)$

et $P + Q(x_3, y_3)$, on a :

$$\begin{cases} x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) \end{cases} \tag{1}$$

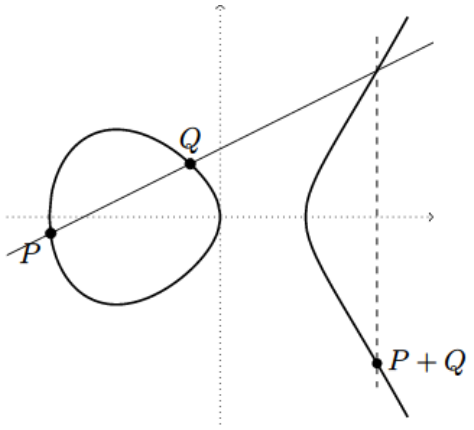

FIGURE 1 – L'addition dans une courbe elliptique

1.1.3 Problème du logarithme discret sur les courbes elliptiques

Soit n un entier naturel et P un point d'une courbe elliptique, on définit le point nP du courbe elliptique par :

$$\begin{cases} n \times P = O & sin = 0 \\ n \times P = \sum_{i=1}^{n} P = P + ... + P \ (nfois) & \text{sinon} \end{cases} \tag{2}$$

Le problème du logarithme discret sur les courbes elliptiques consiste à trouver l'exposant secret n tel que $Q = n \times P$, où P est un point générateur connu et Q un point quelconque sur la courbe elliptique. Autrement dit, il s'agit de trouver la clé privée n à partir de la clé publique Q et du point générateur P.

Le problème du logarithme discret sur les courbes elliptiques est considéré comme difficile à résoudre en pratique, même pour des attaquants avec des ressources importantes, ce qui en fait une base solide pour les algorithmes de cryptographie à clé publique. Les courbes elliptiques sont souvent utilisées dans les protocoles de sécurité tels que le chiffrement de clé publique, la signature numérique et les échanges de clés sécurisés.

1.2 Utilisation de la cryptographie sur les courbes elliptiques pour échanger les clés AES

1.2.1 la cryptographie sur les courbes elliptiques

La cryptographie sur les courbes elliptiques est une technique de cryptographie qui utilise les propriétés mathématiques des courbes elliptiques pour sécuriser les communications. Contrairement à d'autres techniques cryptographiques, la cryptographie sur les courbes elliptiques utilise des clés de chiffrement plus petites et offre une plus grande efficacité des calculs. De plus, elle résiste bien aux attaques grâce à la difficulté de résoudre le problème du logarithme discret sur les courbes elliptiques. Dans ce chapitre, nous allons examiner les principes fondamentaux de la cryptographie sur les courbes elliptiques, discuter de ses avantages et de ses limites, et donner un exemple d'application pratique de cette technique pour protéger les données.

1.2.2 Elliptic Curve Integrated Encryption Scheme

ECIES est une extension de l'algorithme ECC(Elliptic Curve Cryptography) qui utilise à la fois des schémas de chiffrement à clé publique et symétriques pour offrir une sécurité accrue et une efficacité supérieure. La clé de session générée aléatoirement est chiffrée à l'aide de l'algorithme ECC en utilisant la clé publique du destinataire, puis la clé de session chiffrée est envoyée au destinataire, qui peut la déchiffrer à l'aide de sa clé privée correspondante. La clé de session est ensuite utilisée pour chiffrer et déchiffrer les données échangées entre les deux parties à l'aide de schémas de chiffrement symétrique tels que AES dans notre cas.

Les schémas de chiffrement à clé publique sont plus lents que les schémas de chiffrement symétrique car ils impliquent des calculs mathématiques plus complexes. Cela les rend coûteux en temps et en ressources pour chiffrer et déchiffrer de grandes quantités de données. ECIES utilise la clé publique du destinataire pour chiffrer une clé de session aléatoire, qui est ensuite utilisée pour chiffrer et déchiffrer les données échangées. Cela offre une sécurité renforcée tout en garantissant une plus grande efficacité en utilisant les schémas de chiffrement symétrique.

1.2.3 Les clés AES

L'Advanced Encryption Standard (AES) est un algorithme de chiffrement symétrique utilisé pour sécuriser les données. AES est largement utilisé dans les applications commerciales et gouvernementales pour protéger les informations sensibles.

Le chiffrement AES fonctionne en prenant des blocs de données de taille fixe (128 bits) et en appliquant une série d'opérations de substitution, de permutation, de mélange et d'ajout de clé pour produire un texte chiffré. Il est considéré comme l'un des algorithmes de chiffrement les plus sûrs disponibles, grâce à sa structure complexe et à la taille de sa clé de chiffrement. Il se compose de quatre étapes principales :

1. SubBytes : Substitution non linéaire où chaque octet est remplacé par un autre via une table.
2. ShiftRows : Permutation où chaque ligne de l'état est soumise à une permutation circulaire de longueur variable.
3. MixColumns : Mélange sur les colonnes via une transformation linéaire.
4. AddRoundKey : Chaque octet de l'état est combiné avec la clé de ronde.

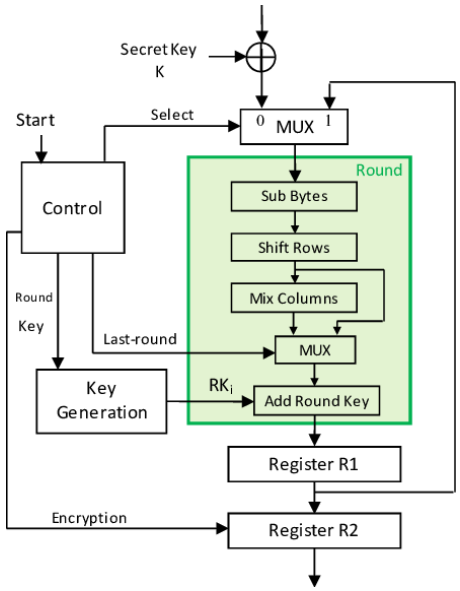

FIGURE 2 – Les étapes du processus de chiffrement AES

1.2.4 Le protocole de Diffie-Hellman sur les courbes elliptiques

Le protocole de Diffie-Hellman est un algorithme de cryptographie à clé publique qui permet à deux parties de s'échanger une clé de chiffrement symétrique sur un canal de communication non sécurisé. Le protocole utilise les propriétés mathématiques des nombres premiers et des groupes de nombres pour sécuriser l'échange de clés.

Le protocole de Diffie-Hellman sur les courbes elliptiques est une version du protocole de Diffie-Hellman qui utilise des courbes elliptiques pour échanger des clés symétriques AES.

Dans ce protocole, on choisie une courbe elliptique sue lequel en prend un point G quelconque, ensuite Alice génère une clé privée aléatoire (d_A), puis détermine sa clé publique (Q_A), tel que $Q_A = d_A \times G$
G et Q_A sont donc des points sur la courbe elliptique. Alice envoie ensuite Q_A à Bob. Ensuite, Bob génère : $R = r \times G$ et $S = r \times Q_A$
où r est un nombre aléatoire généré par Bob.

Alice reçoit R. Elle est alors en mesure de déterminer la même clé de cryptage avec :

$$S = d_A \times R$$

ce qui revient à dire :

$$S = d_A \times (r \times G)$$
$$S = r \times (d_A \times G)$$
$$S = r \times Q_A$$

et qui est identique à la clé générée par Bob.

Le protocole de Diffie-Hellman sur les courbes elliptiques est considéré comme sûr car il est difficile pour un attaquant d'intercepter les échanges de clés et de déterminer la clé de chiffrement commune sans connaître les nombres aléatoires choisis par les parties.

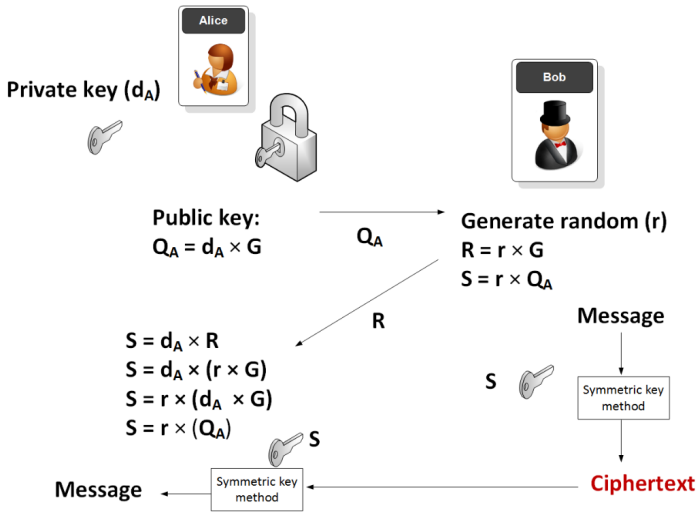

FIGURE 3 – Illustration du protocole de Diffie-Hellman sur les courbes elliptiques

1.2.5 Les applications de ECIES

ECIES est souvent utilisé dans des applications où la sécurité est une priorité, comme la sécurité des réseaux sans fil, des communications satellitaires et des transactions financières en ligne. Voici quelques exemples d'applications courantes de ECIES :

— **Messagerie instantanée sécurisée :** ECIES peut être utilisé pour sécuriser les communications entre les utilisateurs de messagerie instantanée en utilisant la cryptographie à clé publique pour échanger des clés de session sécurisées.

— **Transactions financières :** ECIES est utilisé pour sécuriser les transactions financières en ligne, notamment pour les portefeuilles de crypto-monnaie et les échanges de crypto-monnaie.

— **Sécurité des réseaux sans fil :** ECIES peut être utilisé pour protéger les données transmises sur les réseaux sans fil, tels que les réseaux Wi-Fi, contre les attaques de piratage.

— **Communications satellitaires :** ECIES est utilisé pour sécuriser les communications satellitaires, qui sont souvent utilisées pour les opérations militaires et gouvernementales sensibles.

En général, toutes les applications qui nécessitent une communication sécurisée peuvent utiliser ECIES pour protéger les données transmises.

1.2.6 Les attaques courantes sur les implémentations spécifiques d'ECIES

La cryptographie sur les courbes elliptiques est considérée comme l'une des méthodes de cryptographie les plus sûres et les plus efficaces. Cependant, comme pour toute technologie de sécurité, il existe des risques potentiels d'attaques. Bien qu'il n'y ait pas de failles connues dans la cryptographie sur les courbes elliptiques utilisée par le schéma de chiffrement ECIES, certaines attaques peuvent être menées sur les implémentations spécifiques d'ECIES.

L'une des attaques les plus courantes est l'attaque par canaux cachés, qui exploite les fuites d'informations qui se produisent lorsqu'un système de cryptographie est exécuté sur une machine physique. Cette attaque peut être utilisée pour extraire des informations sur les clés privées utilisées dans le système. D'autres attaques potentielles incluent l'attaque par injection de fautes, qui vise à altérer les données transmises afin de récupérer des informations sensibles, et l'attaque par analyse de côté, qui utilise des techniques d'analyse pour extraire des informations à partir de comportements non intentionnels d'un système.

Ces attaques soulignent l'importance de maintenir les systèmes d'ECIES à jour et de suivre les meilleures pratiques de sécurité. Cela peut inclure l'utilisation de clés suffisamment longues et complexes, la protection des clés privées avec des mesures de sécurité adéquates, et la mise en place de mesures de sécurité pour empêcher les fuites d'informations ou l'injection de fautes.

2 Expérience

Dans notre expérience, nous avons choisi d'utiliser le type **P256** des courbes elliptiques pour l'échange de clé. Ce type de courbe est calculé dans un domaine fini modulo $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, et défini par l'équation $y^2 = x^3 - 3x + b$, où b est un nombre premier d'environ 2^{256}. Cette courbe est souvent utilisée en cryptographie en raison de sa sécurité, de sa performance et de sa compatibilité

avec les normes de sécurité les plus strictes.

En ce qui concerne la méthode de chiffrement utilisée, nous avons choisi le mode CBC (Cipher Block Chaining) de l'algorithme AES (Advanced Encryption Standard). Dans ce mode, chaque bloc de données est chiffré en utilisant une clé secrète et le bloc précédent de chiffrement, ce qui rend le chiffrement plus sûr en empêchant la répétition des blocs chiffrés.

L'un des avantages du mode CBC est qu'il fournit une protection contre les attaques par analyse différentielle en rendant difficile la prédiction de l'effet du chiffrement sur les blocs suivants. De plus, le mode CBC est facile à implémenter et à utiliser, et il est largement pris en charge par les différents systèmes et plateformes de cryptographie.

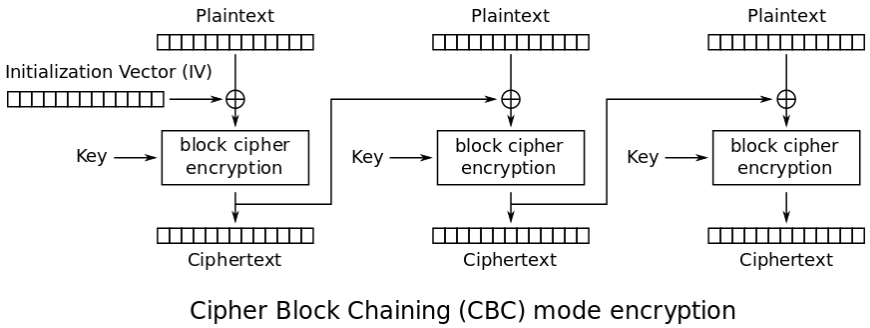

FIGURE 4 – Illustration du mode de fonctionement CBC de AES

L'expérience consiste à échanger une clé commune de manière sécurisée entre deux utilisateurs, Bob et Alice. Cette clé partagée est ensuite utilisée pour chiffrer et déchiffrer les données échangées entre les deux parties en utilisant l'algorithme de chiffrement AES.

3 Résultats

Dans notre expérience, nous avons réussi à échanger une clé de manière sécurisée entre deux utilisateurs, Bob et Alice. Cette clé partagée a ensuite été utilisée pour chiffrer et déchiffrer des messages entre les deux parties. Grâce à ce protocole, nous avons pu garantir la confidentialité des données échangés entre les deux utilisateurs Bob et Alice.

1. On commence par exécuter le code du serveur, la console à gauche pour le serveur, les deux consoles à droit pour les deux clients .

FIGURE 5 – Initialisation de l'expérience

2. Une fois le deuxième client se connecte l'échange de clés s'effectue et on arrive assez rapidement au point ou les deux clients possèdent la même clé qui serait un abscisse d'un point sur la courbe **P256**

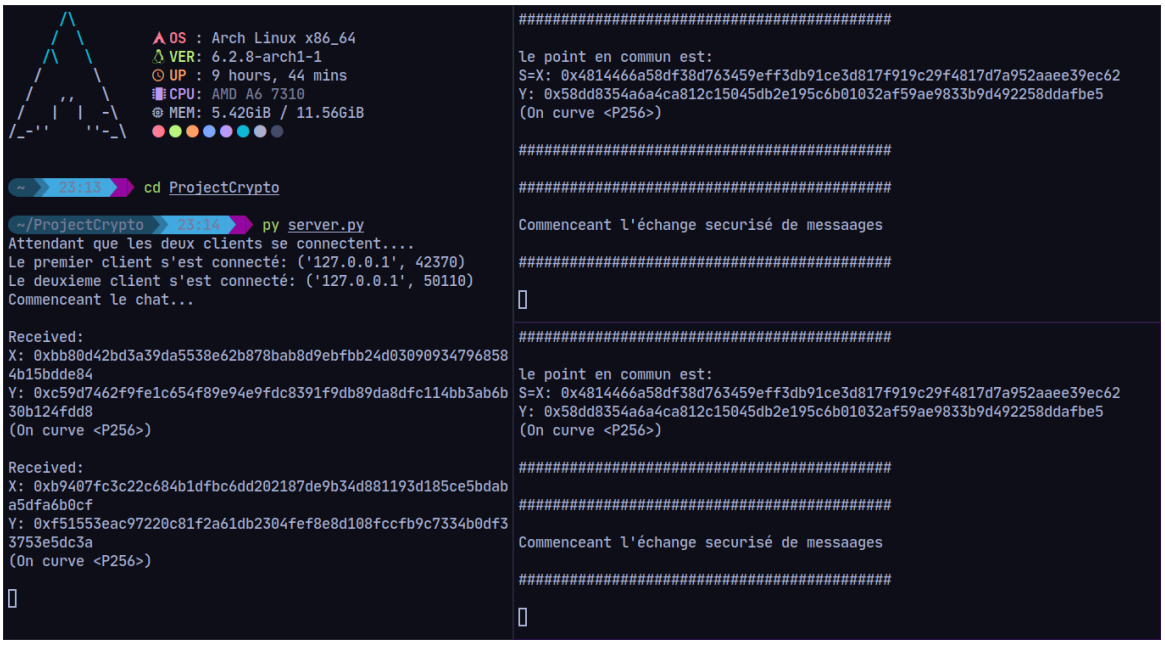

FIGURE 6 – Échange de clé entre les deux clients

3. Voilà, les données sont bien échangées entre les deux utilisateurs. On remarque que même si les données passent par le serveur avant d'arriver à leur destination, le serveur ne peut pas les comprendre puisqu'elles sont chiffrées et que le destinataire est le seule qui peut les déchiffrer.

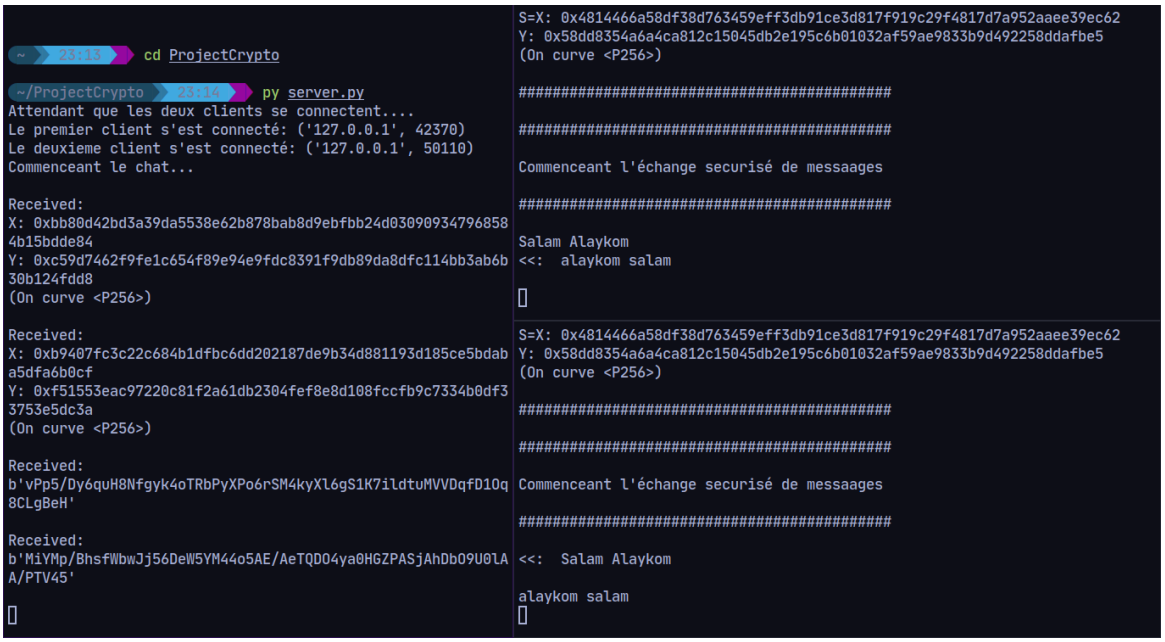

FIGURE 7 – Échange de données (cryptés) entre les deux clients

NB. le serveur ici peux être vu comme le domaine public

Conclusion

En conclusion, l'utilisation des courbes elliptiques pour l'échange de clés est une technique de cryptographie moderne et efficace qui offre un niveau de sécurité élevé. Elle est largement utilisée dans les systèmes de communication pour protéger la confidentialité des données échangées. Les avantages des courbes elliptiques résident notamment dans leur efficacité, leur sécurité, leur résistance aux attaques de type brute-force, ainsi que dans leur faible consommation de ressources.

Cependant, l'émergence de l'informatique quantique pose un défi pour la sécurité des systèmes de communication basés sur les courbes elliptiques, car elle peut potentiellement briser les clés de chiffrement. Ainsi, les chercheurs travaillent activement sur le développement de nouvelles techniques de cryptographie post-quantique pour protéger les systèmes de communication contre les attaques de l'informatique quantique.

En somme, les courbes elliptiques sont une technique de cryptographie essentielle pour l'échange de clés dans les systèmes de communication modernes. Cependant, il est important de continuer à surveiller l'évolution de la technologie quantique et de développer des techniques de cryptographie post-quantique pour assurer la sécurité des systèmes de communication à l'avenir.

Bibliographie

[1] https ://www.bibmath.net/crypto/index.php ?action=affiche&quoi= complements/courbelliptique

[2] https ://theses.hal.science/tel-03663532/document

[3] https ://asecuritysite.com/ecc/ecc3

[4] https ://cryptopp.com/wiki/Elliptic_Curve_Integrated_Encryption_Scheme

[5] https ://core.ac.uk/download/pdf/36042967.pdf

[6] M. Belkasmi(2022-2023) *"Cryptographie et Codes"*ENSIAS page : 34-39

[7] https ://www.educative.io/answers/what-is-cbc