République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohammed Seddik Ben Yahia de Jijel
Faculté des Sciences Exactes et informatique
Département d'Informatique

Mémoire de fin d'étude

pour l'obtention du diplôme de master en informatique

Option : ***Réseaux et Sécurité***

Titre

Modèle de cryptographie à base des courbes elliptiques pour les réseaux mobiles

Présenté par :
Kissoum Karima.
Guendouzi Halima.

Encadré par :
Bouachiba Fouad

Promotion :2019.

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohammed Seddik Ben Yahia de Jijel
Faculté des Sciences Exactes et informatique
Département d'Informatique

Mémoire de fin d'étude

pour l'obtention du diplôme de master en informatique

Option : *Réseaux et Sécurité*

Titre

Modèle de cryptographie à base des courbes elliptiques pour les réseaux mobiles

Présenté par :
Kissoum Karima.
Guendouzi Halima.

Encadré par :
Bouachiba Fouad

Promotion :2019.

⁕ *Remerciements* ⁕

Nous tenons à remercier en premier lieu le dieu , qui nous a donné la force et la patience pour terminer ce Modeste travail.

Mes remerciements s'adressent aussi à **Mr Bouachiba Fouad** , qui nous a fait orienter notre travail.

Nous tenons à remercier très sincèrement l'ensemble des membres du jury qui nous a fait le grand honneur d'accepter d'examiner notre travail.

Nous remercions nos trés chers parents pour leur amour,leurs sacrifices et leur encouragements.

Enfin,nous adressons mes plus sincères remerciements à tous qui nous ont toujours soutenu et encouragé de prés ou de loin au cours de la réalisation de ce mémoire.

⁎ Dédicaces⁎

Je dédié Ce modeste travail

A mes trés chers parents

Pour leur sacrifices et leur encouragements,Merci pour votre compréhension, et votre soutien permanent.Merci d'avoir toujours été là.

Ames frères et soeurs,
A mes collègues et toute mes chères amies,

A mes proches,

A toutes les personnes qui nous ont apportés de l'aide.

GUENDOUZI HALIMA

⁎ Dédicaces⁎

Ce modeste travail est dédié :

A mes chers parents qui nous ont soutenus et encouragés durant toute notre scolarité,

Ames frères et soeurs,
A mes proches,

A mes amis(e),

A toutes les personnes qui nous ont apportés de l'aide.

Kissoum karima

RÉSUMÉ

Aujourd'hui,La protection des données sensibles dans les terminaux ayant des ressources limitées est devenue une problématique qui incite beaucoup d'intérêts.Plusieurs solutions sont proposées dans la littérature. Cependant La majorité de celles-ci ne prennent pas en considération des contraintes imposées par ce type de réseaux. En effet, ces contraintes présentent un obstacle crucial devant la plupart des solutions existantes.D'un autre côté, la technologie de la cryptographie basée sur les courbes elliptiques utilise des clés relativement petites et est mathématiquement très efficace, qui la rend idéale pour des petits dispositifs des communications utilisées aujourd'hui.

Afin d'assurer la protection des données sensibles échangées au sein des réseaux mobiles en tenant compte la capacité des ressources limitées de ses terminaux, Nous avons proposé un modèle de cryptographie basé sur les courbes elliptiques qui permet aux applications sollicitant un niveau de sécurité de choisir la(les) méthode(s) de chiffrement approprie(s) selon les ressources disponibles. Ainsi, Nous avons développé un mini chat, comme un cas d'application de notre modèle, qui utilise des courbes elliptiques pour la génération des clés et le chiffrement de données.

L'efficacité de notre modèle dépend de deux paramètres : la durée nécessaire au traitement des données et le niveau de sécurité fourni par l'application en fonction des ressources disponibles. Les résultats obtenus encouragent la continuité de notre travail.

Mots clés :Sécurité,Réseaux mobiles,Cryptographie,Courbes Elliptiques,Terminaux mobiles,Chat.

ABSTRACT

Today,the protection of sensitive data in mobile networks and its terminals with limited resources has become a problem that incites many interests. Several solutions are proposed in the literature. However, the majority of these do not take into consideration the constraints imposed by this type of network. Indeed, these constraints present a crucial obstacle to most existing solutions.On the other hand, cryptography technology based on elliptic curves uses relatively small keys and is mathematically very efficient, making it ideal for small communications devices used today.

In order to ensure the protection of sensitive data exchanged within mobile networks taking into account the capacity of the limited resources of its terminals, we have proposed a cryptography model based on elliptic curves which allows applications requiring a security level to choose the appropriate encryption method (s) according to available resources. Thus, we developed a mini chat, as an application case of our model, which uses elliptic curves for key generation and data encryption.

The effectiveness of our model depends on two parameters : the time required to process the data and the level of security provided by the application depending on available resources. The results obtained encourage the continuity of our work.

Keywords :Security, Mobile networks, Elliptic Curves Cryptography, Mobile Terminals,Messanger.

Table des matières

Liste des tableaux

Table des figures

Liste des abréviations

AES Advanced Encryption Standard

CPU Computer Processing Unite

CBC Cipher Block Chaining

CFB Cipher FeedBack

CDMA Code Division Multiple Access

CTR CounTer

DES Data Encryption Standard

DSA Digital Signature Algorithm

DDoS Distributed Denial Of Service

DoS Denial Of Service

DLP Discret Logarithm Problem

DL Discrete Logarithm

DH Diffie-Hellman

ECB Electronic Code Book

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

ECDH Elliptic Curve Diffie-Hellman

FDMA Frequency Division Multiple Access

GnuPG GNU PrivacyGuard

GF(p) Corps Fini (Galois Field) premier à p éléments

GF(2n) Corps Fini (Galois Field) binaire à 2n éléments

GSM Global System for Mobile communication

GPRS General Packet Radio Service

IV Initialization Vector

IDE Integrated Development Envirenment

JDK JAVA Developement Kit

LTE Long Terme évolution

MD5 Message Digest5

NIST National Institute of Standards and Technology

OFB Output FeedBack

PDA Personal Digital Assistant

PGP Petty Good Privacy

PGCD Plus Grand Commun Diviseur

PKC Public Key Cryptography

RSA Rivest Shamir Adleman

RC4 Rivest Cipher 4

RIPEMD-160 Ripe Message Digest

SHA Secure Hach Algorithm

TDMA Time Division Multiple Access

UML Unified Modeling Language

UMTS Universal Mobile Telecommunications Service

WPAN Wireless Personal Area Network

WMAN Wireless Metropolitan Area Network

WLAN Wireless Local Area Network

WMAN Wide Area Network

W-CDMA Wide Code Division Multiple Access

WEP Wide Equivalent Privacy

XOR eXclusive OR

Introduction générale

L'évolution dans le domaine de la communication sans fils et l'informatique mobile gagne de plus en plus de popularité.

De nos jours, l'utilisation des terminaux mobiles aux ressources limitées augmente et ces terminaux travaillent principalement avec des données sensibles. Par conséquent, la sécurité des données est devenue cruciale pour les producteurs et les utilisateurs .

La nécessité de protéger les communications a existé depuis l'antiquité dans plusieurs domaines qui vont du domaine militaire au domaine commercial.Pour cela plusieurs méthodes ont été utilisées jusqu'à l'apparition de la cryptographie moderne. Il existe de nos jours deux grands modes de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Plusieurs recherches sont effectuée et plusieurs protocoles ont été conçus pour le chiffrement des données transmises. Les protocoles existants sont basés soit sur la cryptographie symétrique, soit sur la cryptographie asymétrique ou bien sur les deux.Les méthodes symétriques ont plusieurs faiblesses de sécurité malgré qu'ils soient compatibles avec des contraintes dans les dispositifs mobiles, les méthodes asymétriques sont plus sécurisés que les symétriques, mais ils sont très gourmands en matière de ressources,actuellement ces ressources sont très limitées dans une unité mobile .Où les méthodes hybrides consistent à fournir un compromis entre la sécurité et le coût.

Afin d'établir un mécanisme de sécurité efficace,il est nécessaire de limiter le nombre d'instruction de l'algorithme de sécurité .Pour cela ,des cryptosystèmes aujourd'hui sont orientés vers la cryptographie basé sur les courbes elliptiques.Elle est émergée comme alternative aux systèmes cryptographiques asymétriques traditionnels. Plusieurs recherches ont montré que cette technique de cryptographie est mieux adaptée aux dispositifs mobiles sans fils contraints en ressources.

L'objectif de notre projet, est de proposer un modèle de cryptographie destiné aux réseaux mobiles plus précisément pour les terminaux mobiles.Ce modèle offre une amélioration d'une part dans le niveau de sécurité et d'autre part dans le temps de chiffrement et de génération des clés.

Ce mémoire est structuré autour de cinq chapitres :

- Le premier chapitre est une introduction aux réseaux mobiles ,il présente les obstacles et les mécanismes de base de la sécurité dans les réseaux mobiles.
- Le deuxième chapitre discutera les principaux concepts cryptographiques et les techniques de cryptographie moderne existantes.
- Ensuite,la notion de cryptographie à courbes elliptiques, et quelques protocoles basés sur cette dernière sont abordés dans le troisième chapitre .
- Le quatrième chapitre s'occupe de la conception du modèle proposé.
- Le cinquième chapitre présenter des outils logiciels pour une implémentation d'un chat comme un cas d'application du modèle.

Enfin nous cloturonts ce mémoire par une conclusion générale et des perspectives pour une amélioration future.

Chapitre 1

La sécurité dans les réseaux mobiles

1.1 Introduction

Les réseaux mobiles sont actuellement déployés à travers le monde. Ceci est dû à leurs caractéristiques : Installation simple et facile, absence de câblage ,les utilisateurs se déplacent librement au sein de la zone de couverture du réseau.

La sécurité est une fonction incontournable des réseaux mobiles.Elle empêche les personnes de lire ou modifier les messages destinés aux autres, ou des individus qui essaient d'utiliser des services en ligne auxquels ils ne sont pas autorisée à accéder. C'est pour cela qu'un ensemble des moyens sont mis en oeuvre pour minimiser la vulnérabilité d'un système contre des menaces .

Dans ce chapitre nous allons faire une étude sur les réseaux et les terminaux mobiles ,ensuite nous allons présenter la sécurité dans les réseaux mobiles ,Ainsi les obstacles et les attaques liées à ces derniers.

1.2 Généralité sur les réseaux et les terminaux mobiles

1.2.1 Introduction aux réseaux mobiles

Les réseaux mobiles sont des réseaux sans fil dans lesquels au moins deux terminaux peuvent communiquer sans liaison filaires.Grâce a ce type de réseau,un utilisateur (abonné) a la possibilité de rester connecté au réseau tout en se déplaçant dans un périmètre géographique plus au moins étendu ,c'est la raison pour laquelle on parle de **"mobilité"**.

Ces réseaux sont basés sur une liaison utilisant des ondes radioélectriques et utilisant l'interface radio comme support de transmission[1].

1.2.2 Évolution des réseaux mobiles

1.2.2.1 Première génération (1G)

La premier génération de téléphone mobile (noté 1G) a vu le jour dans les années 80.Elle est basée sur une transmission analogique avec une modulation de fréquences.Elle est constituée d'appareils relativement volumineux,utilisant une faible bande passante.Cette norme ne permet que la transmission de la parole .La zone de couverture est divisée en cellule de tailles différentes[2].

On y retrouve essentiellement les standards suivants :

— **AMPS**(Advanced Mobile Phone System) apparu aux USA,constitue le premier standard des réseaux de 1G,il possédé de faibles mécanismes de sécurité rendant possible le piratages des lignes téléphoniques.

— **TACS**(Total Access Communication System) est la version européenne de standard AMPS utilisant une bande de fréquence de 900 MHz.

— **ETACS**(Extended Total Access Communication System) est une version améliorée du standard TACS ,il a été développé au Royaume−Uni et permet l'utilisation d'un nombre plus important de canaux de communications.

1.2.2.2 Deuxième génération(2G)

La deuxième génération (noté 2G) à marqué une rupture avec la 1G grâce au passage de l'analogique au numérique .La norme permet la transmission de la parole et des données simultanément.Elle offre la possibilité aux utilisateur de partage le même canal de transmission ,ceci est possible grâce à l'utilisation de mécanisme de division de fréquence FDMA et le mécanisme de division de temps TDMA [1].

on y retrouve les standards suivants :

— **D-AMPS**(Digital AMPS) compatible avec AMPS lancé par une groupe américain.

— **GSM** : lancé par une groupe européenne,s'est vite imposé leader des réseaux de téléphonie mobile à l'échelle mondiale .Ce standard a vite données naissance à ce qu'on l'appelle la génération 2.5 .C'est le réseau GPRS qui permet la transmission des données par paquets.

1.2.2.3 Troisième génération (3G)

Elle a été introduite vers la fin des années 90,suite au besoin des utilisateurs d'intégrer le multimédia dans les applications de mobiles. les spécifications IMT 2000(International Mobiles Telecommunication for the year 2000) de l'union internationale de télécommunication UIT définissent les caractéristiques de la 3G[1].

un réseau de troisième Génération doit permettre :

— Une transmission à haut débit des données.

— Une compatibilité mondiale.

— Une compatibilité avec les réseaux de 2G.
La principale norme 3G utilisé en Europe est UMTS utilisant le codage W-CDMA.

1.2.2.4 Quatrième génération(4G)

La quatrième génération , qui se base sur la technologie **"Long Terme Evolution"** (LTE),commence a émerger, permet des débits beaucoup plus élevés pouvant aller jusqu'à 100 Mb/s,soit 3 ou 4 fois plus rapides que ceux de la 3G.La migration progressive vers la 4G se fera à un coût inférieur à celui qu'ont nécessité les réseaux précédent ,puisqu'elle implique davantage de modification logicielles que matérielles.les internautes pourront envoyer des fichier lourdes sans problème depuis leur portable et les utilisateur de téléphone intelligente,se connecter plus rapidement au web et y naviguer sur la toile en mode accélérer, en plus de pouvoir visionner des vidéos HD, envoyer des courriels avec des pièces jointes, télécharger des films,etc [1].

1.2.2.5 Cinquième génération(5G)

Ces derniers temps,on entend parler de la cinquième génération. Cette technologie de base a un but pas différente de la quatrième génération mais les différences sont architecturales qui sont définit comme suit[2] :

— L'introduction de Cloud.
— Utilisation fort de la virtualisation.
— Les plates formes d'altitude.

1.2.3 Classification des réseaux mobiles

Les réseaux mobiles peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Au vu de ce critère il existe quatre catégories : les réseaux personnels WPAN , les réseaux locaux WLAN , le réseau métropolitain WMAN et les réseaux étendus WWAN . Le second critère est l' infrastructure. Par rapport à ce critère on peut diviser en deux catégories :réseaux avec infrastructure,réseaux sans infrastructure

1.2.3.1 Selon la zone de couverture

1. **Les réseaux personnels sans fil (WPAN)[3] :**
Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN concerne les réseaux sans fil de faible portée : de l'ordre de quelques dizaines de mètres à usage personnel. Ce type de réseau sert généralement à relier les périphériques personnels (imprimante, téléphone portable, appareils domestiques, etc.) à un ordinateur sans liaison filaire ou bien permettre une liaison sans fil entre deux machines très peu distantes.

Il existe plusieurs technologies permettant la mise en oeuvre de tels réseaux qui sont :

- **Bluetooth :**
  La norme Bluetooth (pris en charge par IEEE 802.15.1) est une technologie de moyen débit, elle permet d'atteindre un débit maximal théorique de 1Mbps. à basse consommation énergétique. Bluetooth utilise la bande de fréquence 2.4 GHz avec une couverture entre 10 et 30 mètres.

FIGURE 1.1 – Technologie Bluetooth.

- **ZigBee** : La norme IEEE 802.15.4 orientée très faible consommation énergétique, qui rend cette technologie bien adaptée à des petits appareils électroniques (appareils électroménagers, jouets, ...), et plus particulièrement aux réseaux de capteurs. La pile proposée par l'IEEE et la ZigBee qui a pour objectif de promouvoir une puce offrant un débit relativement faible (100Kbps environ) mais à un coût très bas, et une consommation électrique extrêmement réduite.

FIGURE 1.2 – Technologie Zigbee.

- **Liaisons infrarouges :** La technologie infrarouge ou IrDA est également utilisée dans ce type de réseaux. Cette technologie est cependant beaucoup plus sensible que Bluetooth aux perturbations lumineuses et nécessite une vision directe entre les éléments souhaitant communiquer, ce qui la limite bien souvent à un usage de type télécommande.

2. **Les réseaux locaux sans fil WLAN**[3]
   Depuis le développement des normes qui offrent un haut débit, les réseaux locaux sans fil ou Wireless Local Area Network (WLAN) sont généralement utilisés à l'intérieur d'une entreprise, d'une université, mais également chez les particuliers.

   Ces réseaux sont principalement basés sur les technologies suivantes :

- **IEEE** 802.11, **WiFi (Wireless Fidelity) :** IEEE 802.11 est un standard de réseau sans fil local proposé par l'organisme de standardisation Américain IEEE. La technologie 802.11 est généralement considérée comme la version sans fil de 802.3 (Ethernet). La technologie 802.11 a connu beaucoup d'évolutions, notamment la 802.11.a et la 802.11.b qui proposent une amélioration de la norme initiale.
- **Hiperlan 1 & 2 :**
  Élaboré par l'ETSI (European Telecommunications Standards Institut), Hiperlan est exclusivement une norme européenne. La technologie de Hiperlan exploite la bande de fréquence de 5Ghz et les débits changent selon la version, ainsi : Hiperlan1 apporte un débit de 20 Mbit/s et Hiperlan2 offre un débit de 54 Mbit/s sur une portée d'action semblable dans celui de la Wi-Fi (100 mètres).

3. **Les réseaux métropolitains sans fil**[4] **:**

   Le réseau métropolitain sans fil est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La norme 802.16 est généralement appelée Wimax.La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres. Le MAN est utilisé généralement dans les universités, les campus ou dans les villes. Le support physique d'interconnexion utilisé dans les WMAN est habituellement la fibre optique.

4. **Les réseaux sans fil étendus (WWAN)**[4] **:**

   Le réseau étendu sans fil est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil.

   - **GSM :** C'est une norme établie en commun par les opérateurs européens depuis 1982, ayant pour objectif le développement d'un système de téléphonie mobile permettant des communications outre-mer.
     Le GSM se distingue par plusieurs spécificités, le premier est l'aspect numérique du réseau, qui offre une qualité supérieure grâce à sa résistance aux interférences. La deuxième spécificité du réseau de GSM réside dans sa configuration cellulaire.

   - **GPRS** :C'est une technologie de radiocommunication par commutation de paquets pour les réseaux de GSM. Les connexions des services de GPRS sont toujours ouvertes afin d'offrir aux utilisateurs des terminaux mobiles une disponibilité de réseau identique à celle qu'ils pourraient atteindre par des réseaux d'entreprise. Le GPRS offre une connectivité d'IP de bout en bout, du terminal GPRS jusqu'à n'importe quel réseau IP. Les terminaux peuvent être intégrés efficacement aux réseaux Internet. La vitesse est quatre fois supérieure à celle du GSM.

   - **UMTS** : l'UMTS désigne une nouvelle norme de téléphonie mobile. Le prin-

cipe de l'UMTS consiste à exploiter une bande de fréquences plus grande pour faire transmettre plus des données et donc obtenir un débit plus important. En théorie, il peut atteindre 2 Mb/s. La norme d'UMTS exploite de nouvelles bandes de fréquences situées entre 1900 et 2200 MHz. Cette technologie permet de faire passer des données simultanément et offre alors des débits nettement supérieurs à ceux atteints par le GSM et le GPRS.

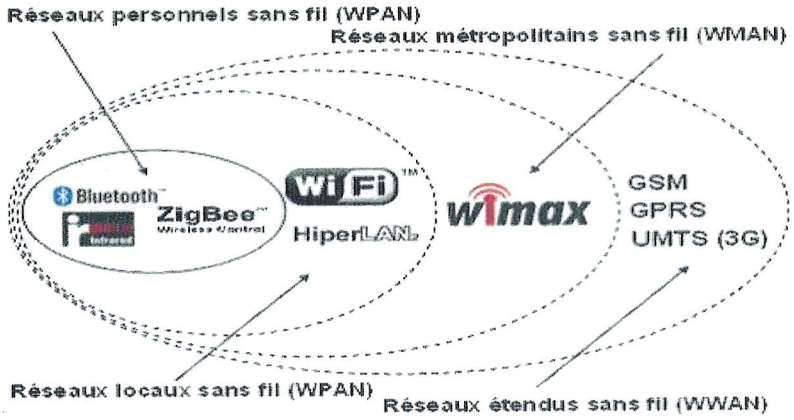


FIGURE 1.3 – Différentes technologies des réseaux mobiles.

1.2.3.2 Selon l'infrastructure

1.2.3.2.1 Réseau avec infrastructure(cellulaire) :

Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques sur une zone de couverture déterminée par la taille du réseau.

Le modèle de système intégrant des sites mobiles et qui a tendance à se généraliser, est composé de deux ensembles d'entités distinctes :

- Les " sites fixes " d'un réseau de communication filaire classique (wired network).
- Les "sites mobiles" (Wireless network).

Certains sites fixes, appelés stations de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites mobiles ou unité mobile (UM) localisés dans une zone géographique limitée, appelée cellule comme le montre la figure suivante[5].

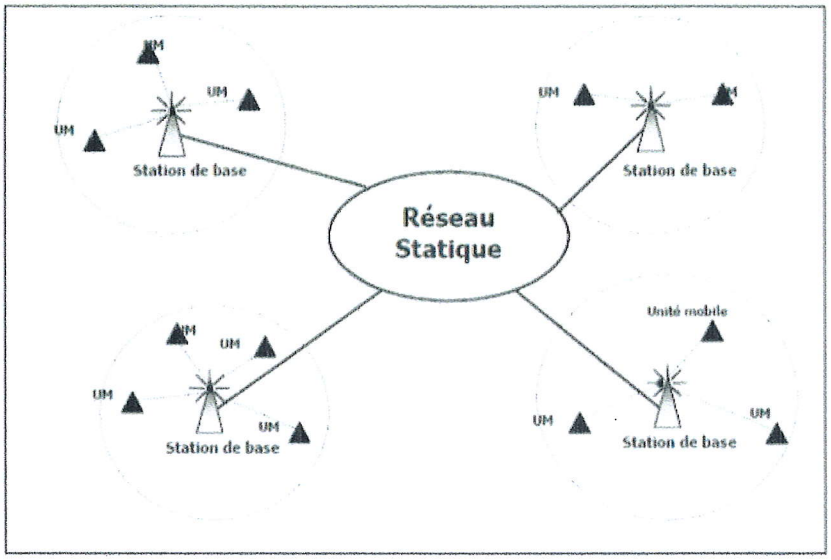


FIGURE 1.4 – Le modèle du réseau mobile avec infrastructure.

- A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages.
  Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire.
- Une unité mobile ne peut être à un instant donné directement connectée qu'à une seule station de base. Elle peut communiquer avec les autres sites à travers la station à laquelle elle est directement rattachée

1.2.3.2.2 Réseaux sans infrastructure fixe(Ad Hoc) :

Le modèle du réseau mobile sans infrastructure préexistante ne comporte pas l'entité « site fixe ». Tous les sites du réseau sont mobiles et communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil.

L'absence de l'infrastructure ou d'un réseau filaire composé de station de base, oblige les unités mobiles (UM) à se comporter comme des routeurs qui participent à la découverte et à la maintenance chemins pour les autres hôtes du réseau. Ce type de réseau est appelé : Ad Hoc [6].

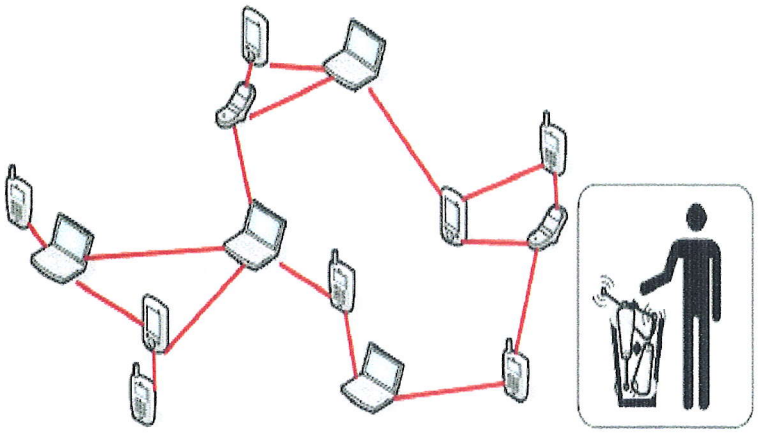


FIGURE 1.5 – Le modèle du réseaux mobiles sans infrastructure

1.2.4 Type des Terminaux mobiles

Un Terminal mobile est un appareil portable permettant le traitement et l'échange de données.Aujourd'hui beaucoup de mobiles différents existent. De nouveaux types d'appareils furent conçus pour répondre à certaines exigences des utilisateurs. Par exemple, les PDA doivent être compacts et posséder une longue autonomie, alors que les lecteurs multimédia mobiles ont besoin d'un grand espace de stockage, d'un processeur rapide et, dans le cas d'un lecteur vidéo, d'un grand écran. Combiner ces différents dispositifs dans un seul appareil n'est pas toujours possible, c'est pourquoi plusieurs types d'appareils mobiles distincts existent aujourd'hui.Dans ce qui suit nous présentons quelque types des terminaux mobiles :

1.2.4.1 PDA

Les PDA sont des appareils de la taille d'un téléphone mobile, mais possédant généralement un large écran tactile à la place d'un écran plus petit. et offrant la possibilité de réaliser des calculs, de stocker et de récupérer de l'information pour un usage personnel ou professionnel [7].

1.2.4.2 Smartphone

Un téléphone intelligent est une combinaison entre un PDA et un téléphone mobile. Smartphones offrent à l'utilisateur les fonctions complètes d'un téléphone mobile ordinaire, mais ajouter un planificateur de jour, la navigation Web et une infinité d'applications.Des exemples de smartphones sont le BlackBerry ,Sumsung et iPhone.

1.2.4.3 Micro portable

Est un ordinateur personnel ,Il est plus léger et leur dimensions limitées permettent un transport facile.Il intègrent une unité centrale, un écran dépliable, une souris, ainsi que

certains périphériques.

1.2.4.4 Tablette PC

Une tablette PC est une ardoise électronique dispose d'un écran tactile et ne possède pas de clavier. La majorité des tablettes sont construites en utilisant des composants standards d'ordinateurs personnels, et donc font tourner un système d'exploitation commun aux ordinateurs personnels.

1.3 La sécurité des réseaux mobiles

En premier lieu ,il est important d'éclaircir la notion de sécurité avant de passer à la sécurité des réseaux mobiles :

1.3.1 Sécurité informatique

Plusieurs définitions de la sécurité sont trouver dans la littérature . Le dictionnaire de l'académie française définit la sécurité comme suit « Sécurité. n.f. Confiance, tranquillité d'esprit qui résulte de l'opinion, bien ou mal fondée,qu'on n'a pas à craindre de danger».

La sécurité informatique est l'ensemble des politiques et des mécanismes de protection et de contrôle mis en oeuvre pour réduire les vulnérabilités d'un système contre les menaces pour éviter les erreurs, afin d'assurer le bon fonctionnement de tel système[8].

1.3.2 Objectifs de la sécurité

Les objectifs ou les services fournis par la sécurité peut résumé dans les six (6) points suivants :

1.3.2.1 Confidentialité

La confidentialité est particulièrement nécessaire pour la transmission des données sensibles et constitue une des exigences pour aborder les problèmes de protection de la vie privée des utilisateurs des réseaux de communication.

La confidentialité permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conservation ou surtout de son transfert[8].

1.3.2.2 L'intégrité

Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission.Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission. Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du système

(intégrité du système) et de l'information (intégrité des données). Dans le réseau sans fil, le message peut être modifié pour des raisons non malicieuses, telles que la corruption du paquet au niveau de la propagation radio. Cependant, le risque qu'un noeud malicieux modifie le paquet est toujours présent. En fait, ce service peut être appliqué de manière indirecte avec des protocoles de sécurité qui assurent la confidentialité ou l'authentification[?].

1.3.2.3 La disponibilité

La disponibilité permettant de maintenir le bon fonctionnement du système informatique. C'est un ensemble des mécanismes garantissant que les ressources (les données et les services opérationnels) sont accessibles, même en cas d'événements perturbants tels que des pannes de courant, des catastrophes naturelles,etc.

Elle signifie que le réseau est disponible pour assurer ses services aux parties communicantes lorsque ceci est nécessaire.

1.3.2.4 Non répudiation

Fournir des éléments de preuve (en temps réel ou a posteriori) sur :

1.La réalité de certaines actions.

2.Les tentatives d'actions non autorisées[8].

les données publiées de façon authentique sont certifiées, et leur auteur ne peut pas nier les avoir publiées, il en assume la responsabilité[9].

1.3.2.5 L'authentification

L'une des mesures les plus importantes de la sécurité, elle consiste à assurer l'identité d'un utilisateur. L'authentification correspond à la vérification de l'identité d'une entité, elle permet donc de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué et y a pas d'usurpation d'identité. Sans l'authentification, un noeud malicieux peut facilement usurper l'identité d'un autre noeud dans le but de bénéficier des privilèges attribués à ce noeud ou d'effectuer des attaques sous l'identité de ce noeud et de nuire à la réputation du noeud victime[?].

1.3.3 Les obstacles de sécurité dans les réseaux mobiles

Un réseau mobile est un réseau spécial qui a plusieurs contraintes comparativement au réseau traditionnel. A cause de ces contraintes, il est très difficile d'appliquer directement les approches de sécurité existantes pour les cas des réseaux mobiles. Donc, pour développer des mécanismes de sécurités utiles tout en empruntant les idées depuis les techniques de sécurité courantes, il est nécessaire de connaitre et comprendre ces contraintes premièrement.

1. **Les ressources limitées :**

Toutes les approches de sécurité exigent une certaine quantité de ressources pour les implémenter, y compris l'espace mémoire, capacité de traitement et l'énergie pour actionner l'unité mobile. Cependant,ces ressources sont très limitées dans une unité mobile. Ces ressources limitées ont un impact important sur la sécurité du terminal.

- **Espace mémoire et de stockage limité :**

  Un mobile est un dispositif minuscule avec seulement un peu de capacité mémoire et d'espace de stockage. Afin d'établir un mécanisme de sécurité efficace, il est nécessaire de limiter le nombre d'instructions de l'algorithme de sécurité. Avec une telle limitation, le logiciel établi pour le mobile doit également être tout à fait petit[10].

- **Limitation de puissance d'énergie :**

  Est la plus grande contrainte aux possibilités des unités mobiles. Par conséquent, la charge de la batterie prise avec l'unité mobile doit être conservée pour prolonger la vie du noeud. En mettant en application une fonction ou un protocole cryptographique dans un noeud mobile, l'impact du code de sécurité supplémentaire sur l'énergie doit être considéré.En ajoutant la sécurité à un noeud mobile, nous sommes intéressés par l'impact de la sécurité sur la durée de vie d'un noeud (c.-à-d., sa durée de vie de la batterie). La puissance supplémentaire consommée par des noeuds mobiles dus à la sécurité est liée au traitement exigé pour des fonctions de sécurité (par exemple, chiffrage, déchiffrage, signature de données, vérification des signatures)[10].

2. **L'utilisation de l'interface sans fil**

   Le médium sans fil est très vulnérable par sa nature, beaucoup plus vulnérable que le médium filaire.

   Le médium sans fil permet un accès libre de tout acteur : la lecture, l'injection, la suppression et la modification des données sont possibles dans la plupart des configurations.Il ne permet pas de limiter le cercle des acteurs impliqués dans le traitement des données envoyées.Pour un attaquant le medium sans fil est souvent plus attractif, car il ne nécessite pas de la présence physique de l'attaquant. Bien équipé, il est capable de monter des attaques contre les vulnérabilités naturelles du medium en restant en dehors du domaine attaqué (parking lot attack).

   Pour résoudre les problèmes existant, un certain nombre de mécanismes sont implémentés pour empêcher toute écoute clandestine ainsi que toute tentative d'accès non autorisé [10].

3. **La mobilité**

   Compare a un environnement statique, ce nouvel environnement mobile permet aux unités de calcul une libre mobilité et ne pose aucune restriction sur la localisation des

noeuds. La mobilité représente en effet un problème connu pour la sécurité .Donc la sécurité de la mobilité doit être traitée avec une prudence élevée. Le problème c'est que les mécanismes de sécurité interviennent souvent en même temps que les mécanismes typiques de mobilité comme le changement de cellule[8].

1.3.4 Attaques sur les réseaux mobiles

En raison de l'architecture massive d'un réseau mobile, il existe une variété d'attaques qui peuvent atteindre l'infrastructure d'un réseau ; les attaques peut classer sur les réseaux mobiles dans les catégories suivantes :

1.3.4.1 Attaques sur les unités mobiles

Les unités mobiles sont exposées à des attaques que les ordinateurs. La sécurité des unités mobiles est plus complexe que la sécurité des ordinateurs à cause de leurs propres caractéristiques. L'unité mobile peut s'exposer à plusieurs risques comme :

1. **Perte :**

   Si un appareil est perdu ou volé, sa confidentialité est cassée. Son intégrité peut être endommagée si l'appareil réapparaît après une période de temps. Dans ce cas, quelqu'un peut avoir installé un logiciel espion (spyware) ou avoir causé une détérioration matérielle qui peut avoir abîmé l'intégrité de l'appareil[11].

2. **Attaques par déni de service :**

   C'est l'attaque la plus nocive qui peut réduire et nuire à l'infrastructure en entier. Ceci est provoqué par l'envoi des données excessives au réseau. Plus le réseau peut manipuler ces données, il en résulte, que les utilisateurs ne pourront plus accéder aux ressources du réseau. D'autres attaques DoS plus spécifiques contre des appareils mobiles peuvent utiliser le fait que ces appareils tournent sous batteries. Dans ce cas, le but de l'attaque est de décharger le plus vite possible les batteries de la cible[12].

3. **Virus :**

   Les virus, vers et chevaux de Troie, sont des menaces pour les appareils mobiles, de la même manière qu'ils le sont pour les ordinateurs. Les vers peuvent avoir un coût s'ils se répandent en utilisant un service pour lequel l'utilisateur est facturé, comme le MMS par exemple. Dans ce cas, un vers s'envoyant lui-même à des centaines d'unités mobiles peut causer un dommage substantiel au propriétaire de l'appareil infecté. D'autre type de virus peut facilement outrepasser les mécanismes de sécurité configurés seulement pour détecter des attaques externes. Les virus peuvent aussi placer un cheval de Troie sur l'appareil, permettant le vol des données ou l'enregistrement des activités d'un utilisateur, en envoyant périodiquement des rapports[10].

4. **L'usurpation de l'identité :**

L'usurpation de l'identité (en anglais, Spoofing ou Impersonation), dans ce type d'attaques, l'attaquant essaie de prendre l'identité d'un autre noeud mobile afin de pouvoir recevoir ses messages ou d'avoir des priviléges qui ne lui sont pas accordés[13].

1.3.4.2 Attaques sur l'interface radio

L'interface radio par leur nature plus vulnérable aux attaques que l'interface filaire. Le support de transmission étant partagé. Quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise. De plus, si une personne malveillante est assez bien équipée, cette dernière n'a pas besoin d'être située dans la zone de couverture. Il lui suffit d'utiliser une antenne avec ou même sans l'aide d'un amplificateur pour accéder au réseau[10].

Il existe un grand nombre d'attaques différentes qui influencent la connectivité d'une cible :

1. **Attaque par interposition (Man In The Middle Attack) :**

   C'est une attaque dangereuse qui touche la confidentialité et l'intégrité des informations, elle est désigné aussi écoute clandestine des transmissions sans fil pour objectif d'extraire des informations confidentielles. Un attaquant peut se reposer entre une unité mobile et un point d'accès et intercepter les messages entre eux[14]. Les attaques sur l'interface radio par interposition peuvent être :

   — **Passive :** l'attaquant écoute seulement les communications entre le dispositif mobile et la station de base pour extraire des informations confidentielles comme les noms d'utilisateurs et mots de passe présente dans toutes les communications sans fil.

   — **Active** :en plus de l'écoute, l'attaquant injecte ou modifie les données transmisses[15].

2. **Dénie de service :**

   Un noeud peut très bien saturer le médium en émettant des trames de contrôle ou de données et empêcher ainsi les autres noeuds de communiquer.

1.3.4.3 Attaque sur les points d'accès

1. **Dénie de service :**

   Un attaquant peut acheter un équipement de station de base BTS et l'installe. Le terminal mobile se reliera au BTS attaquants, s'il a les caractéristiques de l'opérateur et un meilleur signal que la vraie station de base. La fausse station de base se pose entre les unités mobiles et la station de base d'origine et intercepte les communications sans être découvert. L'attaquant pourrait envoyer un signal "occupé" à l'unité mobile chaque fois qu'il demande un service. Aussi, il est possible que le BTS réponde à une demande de service par un message interdisant la station mobile d'accéder au canal

dans un temps spécifique. Cette attaque peut être considérée comme déni de service puisqu'elle dénie les utilisateurs légitimes d'employer le réseau[16].

2. **Détournement d'une session**

Un utilisateur malveillant peut détruire une session déjà établie et peut agir comme une station de base.

1.3.4.4 Attaques sur le réseau du coeur

Le réseau du coeur est considéré la base des réseaux de mobiles. Il représente la base des fonctionnalités des unités mobiles, comme la fonctionnalité téléphonique ou de suivi d'emails. Donc, une attaque réussie sur le coeur réseau peut bloquer totalement le réseau de mobile[10].

1. **Dénie de service distribué :**

   Le but principal d'une attaque de type dénie de service distribué DDoS est de rendre un serveur public incapable de fournir des services aux utilisateurs légitimes. Une station de base peut être une cible typique d'une telle attaque de DDoS. Come les virus informatique ne concernent pas seulement les ordinateurs, ils touchent même les réseaux informatiques comme les réseaux de mobiles, donc lis sont considérés le moyen principale pour réaliser ce type d'attaque.

   Un attaquant équipé par des virus peut envoie des paquets de commande à tout les noeuds de réseau pour demander des services de réseau coeur. Avec la limitation des capacités de traitement des requêtes des demandes ; la cible sera immédiatement bloqué et par conséquence le réseau sera bloqué[10].

   Quand le réseau du coeur stocke des informations vitales pour la sécurité comme les mots de passe des utilisateurs, les clés...etc , on distingue d'autre forme d'attaque comme :

2. **l'attaque par force brute :**

   Généralement les mots de passe de la plupart des logiciels sont stockés, cryptés dans un fichier. Pour obtenir un mot de passe, il suffit de récupérer ce fichier et de lancer un logiciel de brute force craking. Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumériques + symboles), de manière à trouver au mois un mot de passe valide. Cette attaque se base sur le fait que n'importe quel mot de passe est crackable. Ce n'est qu'une histoire de temps. Mais la puissance des machines double tous les deux ans[10].

1.3.5 Mécanismes de bases pour la sécurité

Pour assuré la sécurité au sein des réseaux mobiles ,il existe plusieurs mécanisme tel-que :

1.3.5.1 La cryptographie

La cryptographie est la science d'écriture et de lecture de messages codés. En effet, elle joue un rôle essentiel dans toutes les communications sécurisée en chiffrant un message dit texte clair ,pour obtenir un texte dit crypté, à l'aide d'une clé en utilisant des moyens matériels ou logiciels conçus à cet effet. la cryptographie est un traitement fait sur une donnée qui sera transmise à un destinataire, à travers un canal peu sur en présence d'adversaire.

En fonction du nombre de clés utilisées, nous distinguons deux familles de cryptographie, la cryptographie symétrique nécessite que les systèmes de chiffrement et de déchiffrement disposent de la même clé, tandis que la cryptographie asymétrique ou à clés publiques considère deux clés complémentaires une clé publique et autre privée ,le premier pour le chiffrement et l'autre pour le déchiffrement[6].

Dans le chapitre suivant, nous expliquerons ce concept plus en détail.

1.3.5.2 L'antivirus

Les antivirus visent à détecter des fichiers contenant un code malicieux. De tels fichiers utilisent généralement une faille du système pour exécuter le code malicieux et se propager.Les antivirus reposent principalement sur une base de signatures et vérifient que les fichiers ne présentent pas ces signatures.

Des mécanismes d'analyse heuristique sont également présents, visant à détecter des comportements suspects.Néanmoins, étant donnée la grande variété de virus, ces heuristiques sont peu efficaces.

1.3.5.3 Firewall

Un pare-feu (appelé aussi coupe-feu ou firewall en anglais), est un système permettant de protéger un terminal des intrusions provenant du réseau (ou bien protégeant un réseau local des attaques provenant d'Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante. Un système pare-feu fonctionne sur le principe du filtrage de paquets. Il analyse les en-têtes de chaque paquet (datagramme) échangé entre une machine du réseau local et une machine extérieure.

La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue)[10].

1.4 Conclusion

La sécurité au sein des réseaux mobiles et sans fils reste un challenge ,car ils héritent le problème de sécurité à cause de la présence de support sans fil sans oublie les caractéristiques

physiques des unités mobiles comme la limité d'énergie et les ressources de traitement.

Nous avons présenté dans ce chapitre une généralité sur les réseaux mobiles et quelque mécanismes de base de sécurité, qu'ils ne sont pas tous applicables dans les réseaux mobiles à cause des contraintes de ces derniers.

Alors, il faut concevoir des mécanismes de sécurité spécifiques aux réseaux mobiles, tout en respectant ces propres caractéristiques.

Chapitre 2

La cryptographie

2.1 Introduction

Dés que les hommes apprirent à communiquer,ils durant trouver des moyennes d'assurer la confidentialité d'une partie de leur communications cela signifie que l'origine de la cryptographie remonte sans doute aux origines de l'homme .En effet,la cryptographie ou l'art de chiffrer est devenu aujourd'hui une science à part entière.Au croisement de mathématique,de l'informatique,et parfois même la physique,on la retrouve quand il y a échange des données "sensibles".

Dans ce chapitre nous allons présenter une introduction générale à la cryptographie moderne, en passant par des notions et des terminologies , puis nous allons expliquer le fonctionnement des méthodes de chiffrement symétrique et asymétrique.

Nous allons aussi donner une description de quelques fonctions qui est utilisés avec le chiffrement symétrique et asymétrique pour garantir l'intégrité et l'authenticité des données.

2.2 Définition

Le terme cryptographie vient en effet de deux mots grecs : Kruptus qu'on peut traduire comme secret et Graphein pour écriture. Ainsi la cryptographie est l'art de dissimuler une information écrite en clair (plain text) en cryptogramme (cipher text) pour qu'elle soit incompréhensible que par son destinataire légitime par le biais d'une clé appelé « clé de chiffrement» (processus de chiffrement). Pour rendre l'information à nouveau intelligible par le biais d'une clé appelé « clé de déchiffrement » le processus inverse est appliqué (processus de déchiffrement)[17].

2.3 Terminologies et Notations

1.3.1 Terminologies [18]

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.
- **Cryptographie :** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.
- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Chiffrement/Déchiffrement :** Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message ou qui le reçois. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.
- **Texte en clair :**c'est le message à protéger(à chiffrer).
- **Texte chiffré :**Appelé également cryptogramme, le texte chiffré est le résultat de l' application d'un chiffrement à un texte clair.
- **Clé :** Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, ...).
- **Cryptosystème :**Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

1.3.2 Notatios

En cryptographie, la propriété de base est que [18] :

$$M = D_k(E_k(M))$$

où

- M représente le texte clair.
- C est le texte chiffré tel que C=$E_k(M)$.
- K est la clé de chiffrement(dans le cas d'algorithme symétrique),E_k et D_k dans le cas d'algorithme asymétrique.
- E(x) est la fonction de chiffrement.
- D(x) est la fonction de déchiffrement.

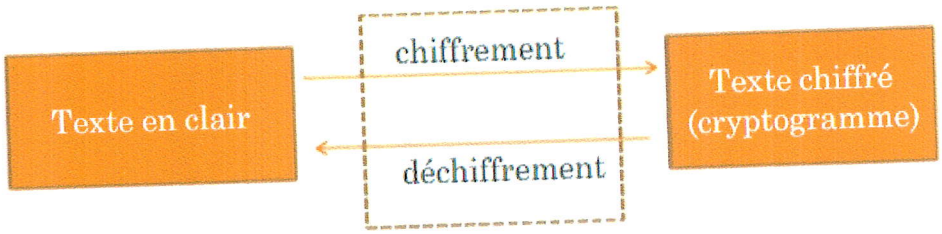


FIGURE 2.1 – Une représentation d'un cryptosystème.

2.4 Principes de cryptographie

1.5.1 Principe de Kerckhoffs

Le principe de Kerckhoffs est une idée de bonne pratique de la cryptographie qui dit que : La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé.En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît K, le déchiffrement est immédiat [19].

2.5 Objectifs de cryptographie

Les principaux objectifs à garantir par l'application de la cryptographie sont[20] :

- **Confidentialité :**
  Les messages ne peuvent être déchiffrés que par le destinataire.
- **Intégrité :**
  Les messages ne peuvent être modifiés par un tiers non autorisé.
- **Authentification :**
  L'identité des différents participants peut être vérifiée.
- **Non-répudiation :**
  L'expéditeur ne peut nier avoir émis le message et le destinaire ne peut nier l'avoir reçu.

2.6 Techniques de cryptographie

2.6.1 Cryptographie symétrique

Dans la cryptographie symétrique ou conventionnelle, les clés de chiffrement et de déchiffrement sont identiques :c'est la clé privé qui doit être connue exclusivment par les communicants.On parle de cryptographie symétrique lorsque deux ou plusieurs personnes

utilisant une même clé pour crypter et décrypter des messages[21].

A chaque clé K sont associées une fonction de chiffrement E_k et une fonction de déchiffrement D_k. L'expéditeur chiffrer le texte clair m pour obtenir le texte chiffré c = E_k(m) et envoie "c" au destinataire.

Le destinataire rétablit le texte en clair m en calculant m = D_k(c).

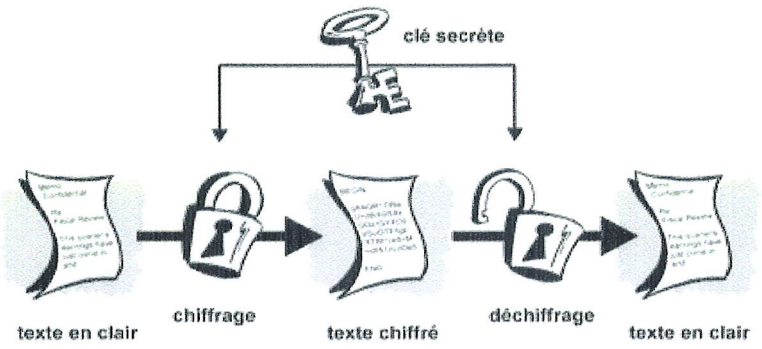


FIGURE 2.2 – Chiffrement symétrique

On distingue deux types d'algorithmes de chiffrement symétriques, le chiffrement par flux(le cryptage de "Stream ")et le chiffrement par bloc :

☞ **Chiffrement par flux :**

Le chiffrement par flux traite les données au fur et à mesure de leurs arrivées. Il se présente classiquement sous la forme d'un générateur de nombres pseudo-aléatoires dont la sortie est couplée via un XOR avec l'information à chiffrer. Le chiffrement se fait bit par bit, octet par octet ou bloc par bloc. Toutefois, le XOR n'est pas la seule opération possible.

L'opération d'addition est également envisageable (par exemple, addition entre deux octets, modulo 256). Notons aussi, qu'un chiffrement par flux peut être réalisé par un chiffrement par bloc utilisant les modes opératoires CTR, ou OFB.

La sécurité d'un système de chiffrement par flux repose essentiellement sur les caractéristiques du générateur pseudo-aléatoire utilisé[22].

Comme exemple d'algorithmes de chiffrement par flux :

— **A5 :** utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.

— **RC4 :**le plus répandu, conçu par Ronald Rivest, utilisé notamment par le protocole WEP

— un algorithme récent de Eli Biham E0 utilisé par le protocole Bluetooth.

☞ **Chiffrement par bloc :**

Dans un algorithme de chiffrement par bloc(en anglais block cipher), chaque message clair est découpé en blocs de taille fixe de même longueur. La taille typique des blocs est 64 bits.Les blocs sont ensuite chiffrés les uns après les autres. Les algorithmes de chiffrement par blocs peuvent être utilisés suivant différents modes ECB,CBC, CFB ou OFB.

1. **Mode ECB : [5][23]**

   Ce mode, dictionnaire de codes, est le plus simple des modes. Il revient à crypter un bloc indépendamment des autres ; cela permet de crypter suivant ordre aléatoire (bases de données, etc...) mais en contre-partie, ce mode est très vulnérable aux attaques.L'avantage de ce mode est qu'il permet le chiffrement en parallèle des différents blocs composant un message. L'inconvénient de ce mode est qu'un même bloc de texte en clair sera toujours chiffré en un même bloc de texte chiffré.

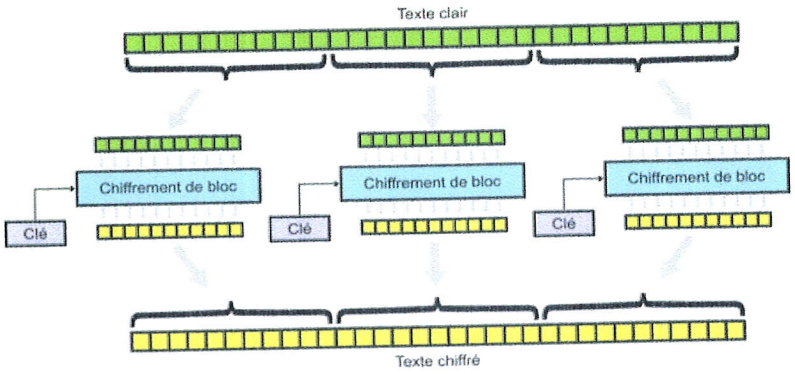


FIGURE 2.3 – Mode ECB :

— **Chiffrement :** Chaque bloque clair mi est chiffré indépendamment et donne un bloc chiffré ci=E_k(mi).

— **Déchiffrement :** Chaque chiffré est déchiffré indépendamment pour donner le clair correspondant mi=D_k (ci).

2. **Mode CBC :** Dans ce mode, on applique sur chaque bloc un OU exclusif avec le chiffrement du bloc précédent avant qu'il soit lui-même chiffré. De plus, afin de rendre chaque message unique, un vecteur d'initialisation (IV) est utilisé.

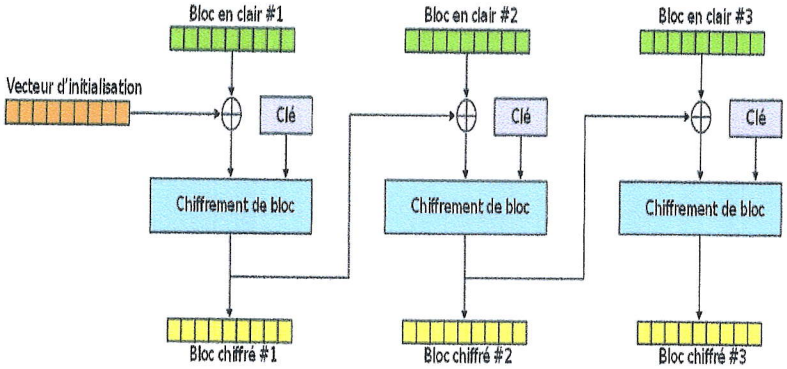


FIGURE 2.4 – Mode CBC

— **Chiffrement :** un vecteur d'initialisation IV est généré aléatoirement. ci = $E_k(mi \oplus$(ci - 1)). Le vecteur IV est transmis avec les blocs chiffrés.
— **Déchiffrement :** mi = $D_k(ci) \oplus$(ci - 1)

3. **Mode CFB :**

Le message est ajouté à la sortie du bloc chiffré. Le résultat sert de feedback pour l'étape suivante. Le registre peut utiliser un nombre quelconque de bits : 1, 8, 64 bits (le plus souvent 64). Il est utilisé pour le chiffrement par flux ainsi que pour l'authentification.

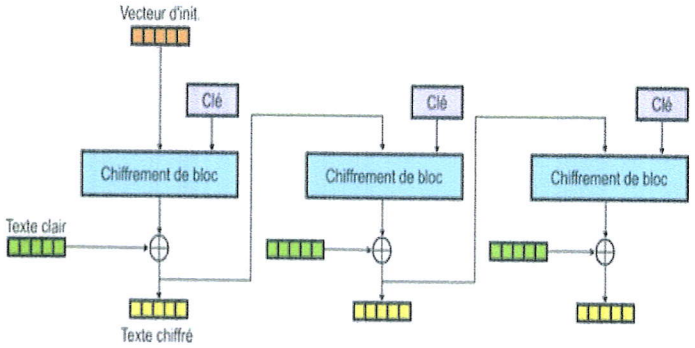


FIGURE 2.5 – Mode CFB

— **chiffrement :**un vecteur d'initialisation IV est généré aléatoirement. ci=$ri \oplus mi$, ou $r1 = E_k(IV)$ et pour $i \geq 2, ri = E_k$(mi1$\oplus$ri-1). Le vecteur IV est transmis avec les blocs chiffrées.
— **déchiffrement :** mi=$ci \oplus$ri.

4. **Mode OFB :** Le feedback est indépendant du message. Tout le mécanisme est donc indépendant des blocs mi et ci. C'est une variante d'un chiffrement de Vernam avec réutilisation de la clé et de l'IV. Il est utilisé dans le cadre de chiffrement de flux sur un canal bruyant.

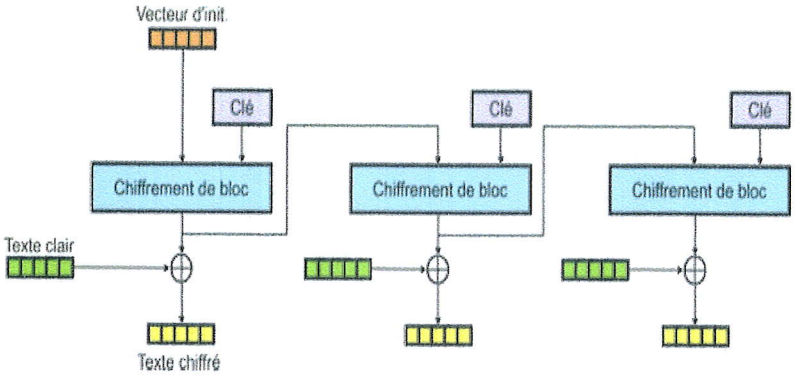


FIGURE 2.6 – Mode OFB

— **Chiffrement** :un vecteur d'initialisation IV est généré aléatoirement.
ci = $ri \oplus$mi , ou r0 = IV et pour $i \geq 1$, ri =0 E_k(ri-1). Le vecteur IV est transmis avec les blocs chiffrés.

— **Déchiffrement** : mi = $ci \oplus$ri.

Pour cette catégorie, nous allons présenter deux algorithmes très connus DES et AES :

DES(Data Encryption Sandard)[24]

Le gouvernement américain a adopté, en 1977, la fonction DES (Data Encryption Standard) comme algorithme de chiffrement standard officiel.

c'est un algorithme de chiffrement par blocs qui agit sur des blocs de 64 bits. C'est un chiffre de Feistel à 16 rondes.qui fonctionne avec une clé de 56 bits. Généralement, celle-ci est représentée sous la forme d'un nombre de 64 bits, mais un bit par octet est utilisé pour le contrôle de parité. Les sous-clefs utilisées par chaque ronde ont une longueur de 48 bits .

L'algorithme DES permet d'effectuer des combinaisons, des substitutions et des permutations entre le texte en clair et la clé de chiffrement, en s'assurant que les opérations peuvent être inversées. Sa sécurité repose spécialement sur ses tables de substitutions non linéaires très efficaces pour perturber les informations.

Les grandes lignes de l'algorithme sont :

✔ **Phase 1 :Préparation - Diversification de la clé**

On diversifie la clé K, c'est-à-dire qu'on fabrique à partir de K , 16 sous-clés K_1,...,K_{16} à 48 bits. Les K_i sont composés de 48 bits de K, pris dans un certain ordre.

✔ **Phase 2 :Permutation initiale**

Pour chaque bloc de 64 bits X du texte, on calcule une permutation Y=P(X). Y est représenté sous la forme Y=G_0 D_0, G_0 étant les 32 bits à gauche de y, D_0 les 32 bits à droite.

✔ **Phase 3 :Itération - schéma de Feistel**

On applique 16 tours d'un même schéma de Feistel. A partir de G_{i-1} D_{i-1} (pour i de 1 à 16), on calcule G_iD_i en posant :

$G_i = D_{i-1}$;

$D_i = G_{i-1} \oplus f(D_{i-1}, K_i)$.

où $\oplus$ est le "ou exclusif" bit à bit, et f est une fonction de confusion, suite de substitutions et de permutations.

✔ **Phase 4 : Permutation finale** On applique à G_{16} D_{16} l'inverse de la permutation initiale. $Z=P_1(G_{16}\ D_{16})$ est le bloc de 64 bits chiffré à partir de x.

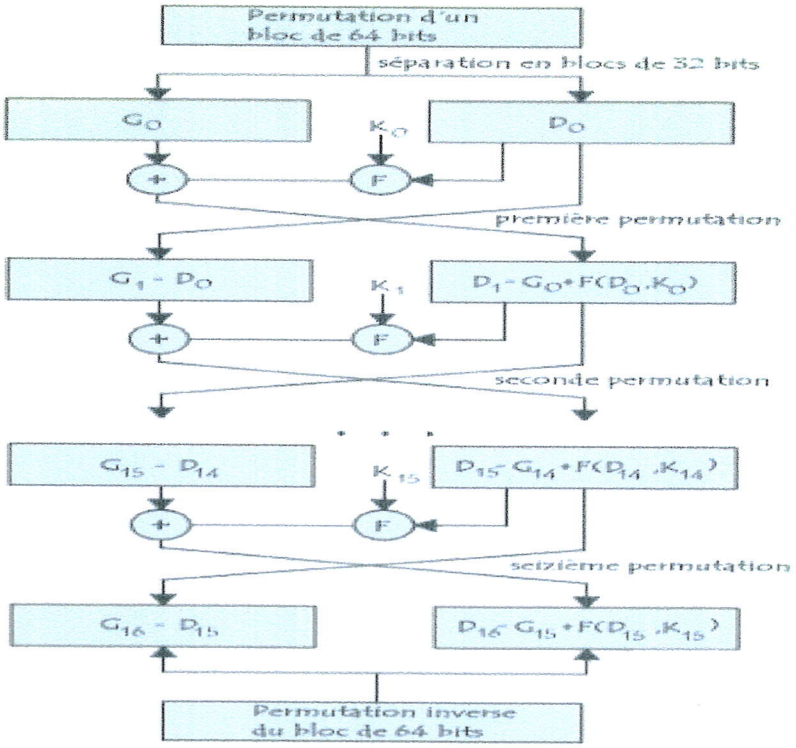


FIGURE 2.7 – Résumé de fonctionnement DES

AES (Advanced Encryption Standard)

En Janvier 1997, NIST (National Institute of Standards and Technology) lance un appel d'offre international pour remplacer le vieillissant DES : il en résulte 15 propositions. Parmi ces 15 algorithmes, 5 furent choisis pour une évaluation plus avancée en avril 1999 : MARS, RC6,Rijndael, Serpent et Twofish. Finalement, en octobre 2000 la NIST élit Rijndael comme nouveau standard qu'on nomme aussi AES (Advanced Encryption Standard)[25].

-Principe de AES :

AES est un chiffrement par bloc symétrique pouvant contenir des blocs de taille 128 bits, des clés de chiffrement 128, 192 et 256 bits. L'algorithme AES utilise une fonction ronde qui est comparé de quatre transformations différentes orientées octet telles que : Sub byte, Shift row, Mix column,Add round key. Le nombre de tours à utiliser dépend de la longueur de la clé, 10 tours pour 128 bit clé, 12 tours pour la clé 192 bits et 14 tours pour les clés 256 bits[26].

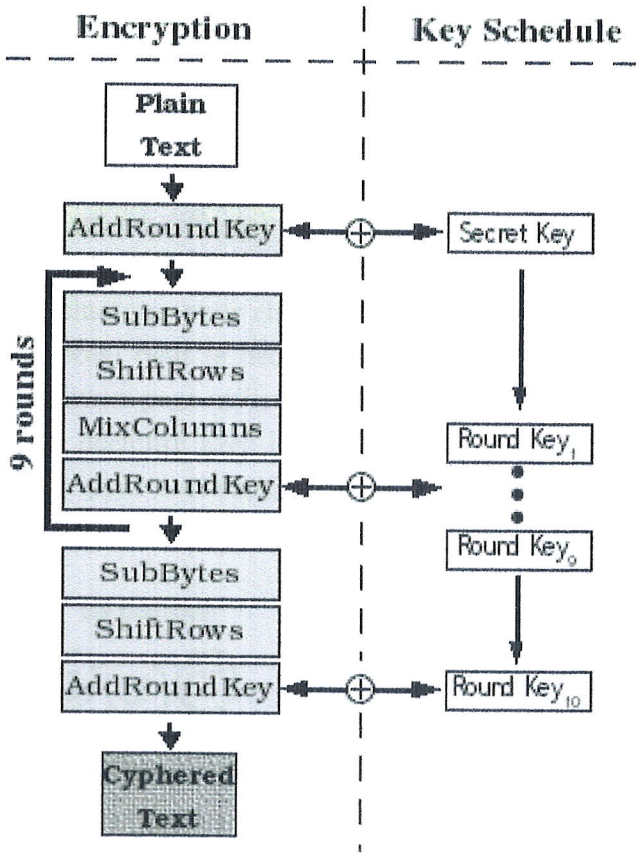


FIGURE 2.8 – Résumé de fonctionnement AES

- **SubBytes :** Chaque entrée est remplacée par un autre mot de 8 bits donnée par un tableau de correspondance.
- **ShiftRows :** Les entrées sont décalées suivant un décalage circulaire à gauche d'un nombre de cases dépendant de la ligne.
- **MixColumns :** Chaque colonne est remplacé par un autre colonne obtenu en transformant la colonne en un polynôme et en multipliant par un polynôme fixé.
- **AddRoundKey :** Chaque entrée est remplacé par le XOR entre cette entrée et l'entrée correspondant dans une matrice 4*4 construit à partir de la clé.

— DSA (Digital Signature Algorithm).
— RSA (Rivest, Shamir et Adleman).

Diffie-Hellman [27]

Parallèlement à la découverte du principe de la cryptographie à clé publique,Diffie et Hellman n'ont pas construit de système de chiffrement, mais ils ont proposé une construction pour une primitive différente : l'échange de clef. Le problème est le suivant : Alice et Bob veulent s'échanger un message crypté en utilisant un algorithme nécessitant une clé K. Ils veulent s'échanger cette clé K, mais ils ne disposent pas de canal sécurisé pour cela. Le protocole d'échange de clés de Diffie et Hellman répond à ce problème lorsque K est un nombre entier. Il repose sur l'arithmétique modulaire, et sur le postulat suivant :

Étant donnés des entiers p,a,x, avec p premier et $1 \leq a \leq p-1$:
— il est facile de calculer l'entier $y=a^x$ (modp).
— si on connait $y=a^x$ (mod p),a et p, il est très difficile de retrouver x.

Retrouver x connaissant a^x (mod p), a et p s'appelle résoudre le problème du logarithme discret. Comme pour la factorisation d'entiers, c'est un problème pour lequel on ne dispose pas d'algorithme efficace. Expliquons maintenant comment Alice et Bob peuvent s'échanger une clé secrète par le protocole de Diffie-Hellman. Ils font des actions en parallèle, que l'on décrit dans le tableau suivant :

	Alice	Bob
Étape 1 :	Alice et Bob choisissent ensemble un grand nombre premier p et un entier $1 \leq a \leq p-1$. Cet échange n'a pas besoin d'être sécurisé.	
Étape 2 :	Alice choisit secrètement x_1.	Bob choisit secrètement x_2.
Étape 3 :	Alice calcule $y_1 = a^{x_1} \pmod{p}$.	Bob calcule $y_2 = a^{x_2} \pmod{p}$.
Étape 4 :	Alice et Bob s'échangent les valeurs de y_1 et y_2. Cet échange n'a pas besoin d'être sécurisé.	
Étape 5 :	Alice calcule $y_2^{x_1} = (a^{x_2})^{x_1} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Bob.	Bob calcule $y_1^{x_2} = (a^{x_1})^{x_2} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Alice.

FIGURE 2.10 – Principe du Diffie-Hellman

À la fin du protocole, Alice et Bob sont donc en possession d'une même clé secrète K, qu'ils ne se sont pas échangés directement. Si quelqu'un a espionné leurs conversations, il connait p,a, y_1 et y_2. Il ne peut pas retrouver K comme le font Alice ou Bob, car il lui manque toujours l'une des informations nécessaires, à savoirx_1 ou x_2. Et il ne peut pas retrouver x_1 connaissant y=a^{x1} (mod p), a et p, puisque la résolution du logarithme discret est un problème difficile.

RSA [17]

L'algorithme RSA a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman.Le principe de base de RSA et de considérer un message comme un grande nombre entier et de faire des calcules dessus pour le chiffrer.Il repose sur la factorisation en nombres premiers d'un entier ,son fonctionnement est le suivant :

- Générer aléatoirement deux nombres premiers (p et q),puis les multiplier pour générer le nombre n.
- Déterminer φ(n) : φ(n)=(p-1)*(q-1).
- Choisi un entier naturel e premier avec φ(n) et strictement inférieure à φ(n)

- Calculer l'entier naturel d qui est strictement inférieure à φ(n) et e* d≡ 1(mod φ(n)).
- le couple (e,n) est la clé publique du chiffrement,alors que le couple (n,d) est sa clé privée.
- pour chiffrer un texte, nous calculons c avec :c=m^e mod n.
- pour déchiffrer un texte chiffré, nous calculons m avec :m=c^d mod n où m est le message en claire et c le message chiffré.

Avant d'être chiffré, le message original doit être décomposé en série d'entier M de valeurs comprises entre 0 et n-1 .

L'algorithme 1 décrit l'étape de création des clés de RSA.

Algorithme 1 : Génération de clés avec RSA

```
Sortie : Clé publique (n,e) et clé privé d générées
Début
Sélection au hasard de deux nombres premiers p et q ;
Calculer n=p * q et φ(n) =(p-1)*(q-1) ;
choisi un entier e tel que 1< e<φ(n) et le PGCD (e,φ(n))=1 ;
calculer d tel que 1< d<φ(n) et e*d ≡1 (mod φ(n)) ;
Fin
```

L'algorithme 2 décrit l'étape de chiffrement de message avec RSA.

Algorithme 2 : Chiffrement avec RSA

```
Entrée :(n,e) et m // la clé publique et le texte clair m∈[0,n-1]
Sortie :c //le texte chiffré
Début
Calculer c=m^e ;
Fin
```

L'algorithme 3 décrit l'étape de déchiffrement de message crypté avec RSA.

Algorithme 3 : Déchiffrement avec RSA

```
Entrée :(n,d) et c // la clé privé et le texte chiffré c
Sortie :m //le texte clair
Début
Calculer m=c^d ;
Fin
```

Les inconvénients de chiffrement RSA[28] :

Les inconvénients de RSA sont comme suit :

-Génération de clés très lente.

-Signature et décryptage lents, qui sont peu délicate à mettre en ouvre en toute sécurité

Courbes Elliptiques : Il s'agit d'un concept proposé en 1985 par deux chercheurs Miller et Koblitz, de façon totalement indépendante. Ce type de cryptographie, toujours basé sur le modèle asymétrique, permet aussi bien de chiffrer que de signer. On utilise souvent l'abréviation ECC, pour Elliptic Curve Cryptography. Les clés utilisées sont plus courtes pour une sécurité égale ou supérieure aux autre méthodes asymétrique[29]. cette méthode,elle sera détaillée dans le Chapitre suivant.

Avantages et Inconvénients de chiffrement asymétrique :

Avantages	Inconvenants
Usage à long terme des paires de clés	lent à l'exécution en raison de la charge de calcul élevée
Authentification de la clé publique	Taille de clé généralement grande
Signature électronique Des messages	Sécurité conditionnelle
2 n clés seulement pour n partenaires	

TABLE 2.2 – Avantages et Inconvénients de chiffrement asymétrique

2.6.2.1 Fonctions de hachage

Une bonne cryptographie doit pouvoir offrir une garantie de l'intégrité des informations.En effet, il ne doit pas être possible de pouvoir modifier les informations crypté de façon totalement transparent, un processus de vérification de l'intégrité du message doit être mise en place ,Ce processus est réalisé par une fonction de hachage[21].
Une fonction de hachage est une fonction qui prend en entrée un élément de taille arbitraire finie et renvoyant un élément de longueur fixée [24].

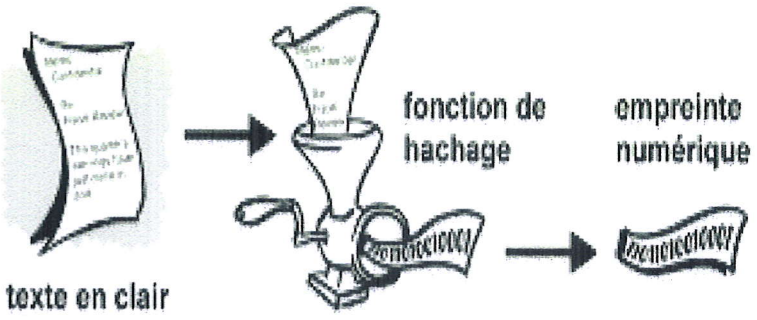


FIGURE 2.11 – Principe du hachage

Deux caractéristiques (théoriques) importantes sont les suivantes[30] :
— Ce sont des fonctions unidirectionnelles :
A partir de H(M) il est impossible de retrouver M.
— Ce sont des fonctions sans collisions :
A partir de H(M) et M il est impossible de trouver $M' \neq$ M tel que H(M') = H(M).

Les algorithmes de hachage le plus utilisé actuellement sont :
— **MD5** (MD signifiant Message Digest) .
— **SHA-1** SHA-1(Secure Hash Algorithme1).
— **SHA-2** (Secure hash Algorithme2).
— **RIPEMD-160** (Ripe Message Digest).

2.6.2.2 Signature numérique

C'est un code électronique unique qui permet de signer un message codé. Cette signature permet d'identifier l'origine du message (assurée la fonction d'authentification) : elle a la même fonction qu'une « signature à la main ».
Pour réaliser la signature électronique, avant d'envoyer un message, il faut calcule d'abord l'empreinte (hache) du message. Il chiffre ensuite cette empreinte par un algorithme asymétrique avec la clé privée de l'utilisateur. Ce résultat est appelé signature électronique. Avant l'envoi, cette signature est ajoutée au message, qui devient un message signé. C'est la clé privé qui permet de signer, et la clé publique qui permet de vérifier cette signature [21].
La figure suivante montre le déroulement de cette opération.

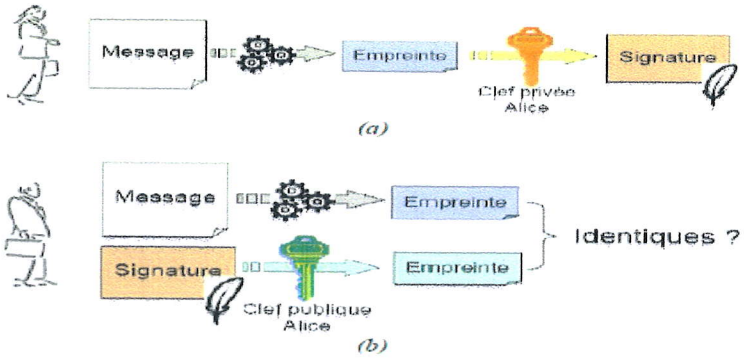


FIGURE 2.12 – a) Signature. b) Vérification.

Quand le destinataire reçoit l'information, il peut aussi la passer par la même fonction de hachage, déchiffrer la somme de contrôle qui accompagne le message et comparer les deux sommes. Si elles correspondent, l'information n'a pas été modifiée. Lorsque la somme de contrôle originale est conservée, on peut toujours vérifier l'information pour détecter d'éventuelles modifications.

2.6.3 Cryptographie hybride

La cryptographie hybride a été introduite pour profiter des avantages des deux techniques précédemment citées, en fait cette technique bénéficie de la cryptographie asymétrique par sa rapidité de traitement des données et de la cryptographie asymétrique par sa puissance de chiffrement.

Le principe est assez simple, l'échange des clés pour un chiffrement symétrique est effectué grâce à la cryptographie à clé publique, et les données à échanger sont chiffrées en utilisant un algorithme de chiffrement symétrique, cela rend la communication assez rapide[31].

Les plus classiques de ces logiciels sont :

— **GnuPG (GNU PrivacyGuard).**

— **PGP (Petty Good Privacy).**

2.7 Cryptographie quantique

La cryptographie quantique, plus correctement nommée distribution quantique de clés,désigne un ensemble des protocoles permettant de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information. Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles[32].

2.8 Conclusion

Nous avons présenté dans ce chapitre une vue globale sur la cryptographie moderne en mettant le point sur les concepts de base et les méthodes de chiffrement symétriques et asymétriques utilisé . ce qui nous donne une base pour passer au troisième chapitre où nous allons s'intéresser au cryptographie à base des courbes elliptiques.

Chapitre 3

Cryptographie basée sur les courbes elliptiques

3.1 Introduction

Au cours des dernières années, un sujet sur la théorie des nombres et la géométrie algébrique appelé courbes elliptiques a trouvé un champ d'application en cryptographie.

Nous allons présenter dans ce chapitre un rappel sur les groupes, les définitions de base et les règles sur les courbes elliptiques.Ainsi une description des attaques connue sur la cryptographie à base des courbes elliptiques pour éviter d'avoir une mauvaise implémentation de cette dernière.

3.2 Généralité

Avant de présenter les courbes elliptiques, nous étudions d'abord les notions mathématiques dont nous avons besoin pour comprendre son fonctionnement.

3.2.1 Groupe

En mathématique, un groupe est un couple (E, .) où E est un ensemble et "." est une loi de composition interne qui combine deux éléments a et b de E pour obtenir un troisième élément a.b . Il faut que la loi satisfasse les quatre axiomes ci-dessous[33].

— Fermeture : $\forall(a, b) \in$ E : a.b $\in$ E
— Associativité : $\forall(a, b) \in$ E : (a . b) . c = a . (b . c)
— Élément neutre : $\exists e \in$ E : a . e = e . a = a
— Symétrique : $\forall a \in$ E, $\exists$ b $\in$ E : a . b = b . a = e

Groupe abélien : Un groupe abélien, ou un groupe commutatif, est un groupe dont la loi de composition interne est commutative. Un ensemble E est un groupe commutatif lorsque[33] :

$\forall$(a, b) $\in$ E : a . b = b . a

Groupe cyclique : Un groupe fini G est cyclique si tout élément du groupe peut s'exprime sous forme d'une puissance ou d'un multiple d'un élément particulier g, appelé le générateur du groupe, c'est-à-dire G = <g> = g^n : n $\in$ Z* . Par exemple si G = g^0, g^1, g^2, g^3, g^4, g^5 etg^6 = g^0, alors G est un groupe cyclique. Tout groupe cyclique est abélien car $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$. L'ordre d'un élément e d'un groupe cyclique est le nombre entier n positif le plus petit tel que ne = 0 (en notation additive) ou e^n = 1 (en notation multiplicative). Reprenons le même groupe G du paragraphe précédent, par exemple l'ordre de l'élément g^2est 3 car l'élément neutre du groupe est $g^0 = 1$ et $(g^2)^3 = g^6 = 1$[33].

3.2.2 Corps

Un corps est un ensemble E muni de deux lois de composition, notée respectivement (+) et (·). Il faut que les deux lois satisfassent les conditions suivantes :

— Le couple (E, +) forme un groupe abélien, il existe un élément neutre, noté 0, tel que :
$\forall a \in$ E | a + 0 = 0 + a = a

— Le couple $(E/0, .)$ forme aussi un groupe abélien dont l'élément neutre est 1 ,
$\forall a \in$ E | a · 1 = 1 · a = a

— La multiplication (.) est distributif pour l'addition, c'est-à-dire :
$\forall(a, b, c) \in$ E | a · (b + c) = a · b + a · c et (b + c) · a = b · a + c · a

Autrement dit, un corps est un anneau dont les éléments non nuls forment un groupe abélien pour la multiplication[33].

3.2.3 Corps fini

Un corps fini F est un corps qui contient un nombre fini d'éléments. L'ordre ou cardinal de F est le nombre d'éléments de F. Si F est un corps fini, F contient p^m éléments, où p est premier et m >=1 [34].

Pour étudier la cryptographie sur les courbes elliptiques, il faut que nous comprenions les deux types de corps ci-dessous :

3.2.3.1 Corps premier

Un corps est un corps premier, noté indices : $\mathbb{F}_P$ lorsque l'ordre du corps q = p^n et p est un nombre premier. Le corps est constitué des nombres entiers $\{0, 1, 2, ..., p-1\}$, et $\forall a \in \mathbb{Z}$, a mod p donne le reste unique r qui est compris entre [0, p-1][33].

3.2.3.2 Corps binaire

Un corps fini de l'ordre 2^n est un corps binaire, noté $\mathbb{F}_{2^n}$, qui peut être construit en utilisant une représentation polynomiale. Les éléments du corps sont des polynômes binaires dont les coefficients $a_i \in \{0,1\}$et les degrés sont inférieurs à n. C'est-à-dire $\mathbb{F}_{2^n} = \{a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + ... + a_1 z + a0 : a_i \in \{0,1\}\}$[35].

3.3 Présentation des courbes elliptiques

dans cette section nous allons passer à la définition des courbes elliptiques avec l'ensemble d'opérations que nous pouvons effectuer sur elles.

3.3.1 Equation de Weierstrass

Une courbe elliptique sur $\mathbb{K}$, définie comme l'ensemble des solutions du plan projectif P_2 (|) de l'équation de Weierstrass suivante.

E : F (x ; y ; z) = $y^2z + a_1xyz + a_3yz^2 - x3 - a_2x^2z - a_4xz^2 - a_6z^3$.

où les coefficients a1 ; a2 ; a3 ; a4 et a6 sont dans $\mathbb{K}$[36].

pour alléger les notations, nous allons écrire l'équation de Weierstrass avec coordonnées non homogènes : X = x/z et Y = y/z.

E : $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.

3.3.2 Définition des courbes elliptiques

Soit K un corps fini, on appelle courbe elliptique sur K une courbe dans le plan projectif,cubique et sans points singuliers, et munie d'un point distingué qui jouera un rôle particulier :élément neutre.

Elle est donc définie par un polynôme irréductible homogène en trois variables à coefficient dans K . Par un changement de variables homographique, on peut toujours se ramener à une équation dite de Weierstrass :

$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$;

Avec $a_1; a_2; a_3; a_4; a_5; a_6 \in K$

En caractéristique différente de 2 et 3, on peut considérer une équation plus simple pour la courbe E, à savoir, une équation sous forme de Weierstrass :

$E : Y^2 = X^3 + AX + B$

avec un extra-point ϑ , où les constantes A et B doivent satisfaire :

$4A^3 + 27B^2 \neq 0$

La courbe elliptique E est l'ensemble des points (x,y) $\in$ K2 satisfaisant cette équation et d'un point imaginaire ϑ appelé point à l'infini.[37]

La Figure suivante illustre deux exemples de courbes elliptiques :

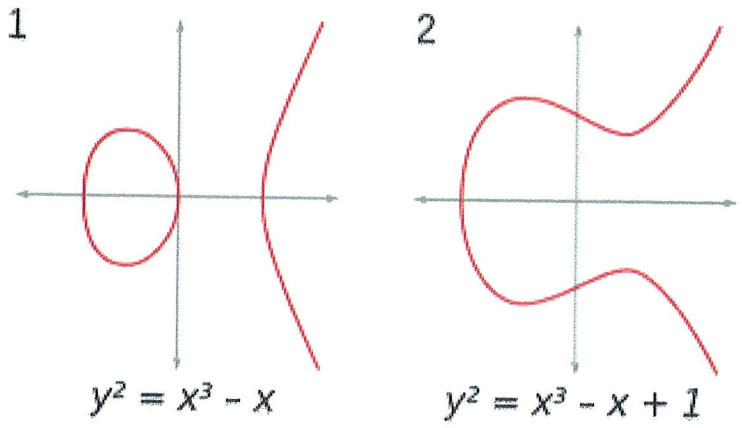


FIGURE 3.1 – Exemples des courbes elliptiques

3.3.3 Multiplication de point

Les modèles cryptographiques basés sur ECC se fondent sur la multiplication scalaire des points des courbes elliptiques. étant donner un nombre entier k et un point p $\in E(F_p)$, la multiplication scalaire est le processus d'ajouter p à elle-même k fois [35].

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

La multiplication scalaire des points des courbes elliptiques peut être calculée efficacement en utilisant l'algorithme doublement-et-addition(double and add) qui représentée dans l'algorithme(4).

- Supposons que P est un point sur une courbe elliptique qui est définie sur un corps premier, notée $E(F_p)$, pour calculer kP où k est un nombre entier positif de longueur l bits, nous représentons k en binaire $k = \sum_{i=0}^{l-1} k_i 2^i$, et ensuite nous parcourons k du bit de poids faible au bit de poids fort[33].

Algorithme 4 : Algorithme doublement-et-addition pour calculer $Q = kP$

```
Données :k = Σ_{i=0}^{l-1} k_i 2^i et P∈ E(F_p)
Résultat : Q = kP
Début
Q ⟵ ∞ ;
pour i de 0 à l − 1 faire
    si k_i = 1 alors
        Q ⟵ Q + P;
    P ⟵ 2P;
retourner Q
```

3.3.4 Problème du logarithme discert sur les courbes elliptiques

Soit G un groupe (note additivement) cyclique fini d'ordre n engendré par un élément P.

Soit H =< P > le sous-groupe engendré par P, alors :

$\forall Q \in H, \exists n \in \mathbb{N} : Q = nP$

Cet entier n est appelé le logarithme discret de Q en base P et nous le noterons $log_p(Q)$. Le problème du logarithme discret dans un groupe consiste donc à retrouver l'entier n à partir de la donnée publique (H, P, Q). La sécurité des protocoles basé sur les courbes elliptiques repose sur la résolution de ce problème.

Usuellement ce problème est plutôt présenté pour un groupe noté multiplicativement ce qui donne :

Soit G un groupe (noté multiplicativement) cyclique fini d'ordre N engendré par un élément g.

Soit h un élément de G. Comme G est un groupe cyclique engendré par g, il existe un unique entier n compris entre 1 et N tel que h = gn. Cet entier n est appelé le logarithme discret de h en base g et nous le noterons $log_g(h)$.

Maintenant nous faisons la correspondance entre les courbes elliptiques et le logarithme discret tel que : Soit E une courbe elliptique définie sur F_p.

Soit P et Q deux points de E(F_p) tels que Q = nP. En résumé, le problème du logarithme discret revient donc à déterminer un entier n tel que Q = nP[38].

3.3.5 Nombre de points sur une courbe elliptique

Il existe une méthode naïve pour observer que le nombre de points d'une courbe elliptique a une borne maximale. Pour un x donné il existe au maximum 2 points avec des cordonnées opposées solutions de l'équation$E_{GF(p)}$. Nous pouvons donc affirmer qu'il y aura $2p + 1$ points au maximum sur la courbe. On connait depuis 1933 des bornes plus précises pour le nombre de points sur une courbe elliptique grâce au théorème de Hasse. On notera $\sharp E a_4, a_6, p$ le nombre de points d'une courbe elliptique, aussi nommé ordre de la courbe elliptique.

Le théorème de Hasse assure que :

$$\text{p +1 - 2 } \sqrt{p} \leq \sharp E_{a_4,a_6,} \leq \text{ p +1 +2 } \sqrt{p}$$

$\sharp E_{a_4,a_6,}$ =Nombre de points

L'ordre de la courbe $E_{-12,20,37}$ est donc compris entre 26 et 50 points.L'ordre exact de cette courbe est 47 . Il faut connaitre l'ordre d'une courbe elliptique pour deux raisons.Tout d'abord ce nombre intervient dans les protocoles cryptographiques et dans

la procédure de génération de clé secrète. De plus, pour des nombres de points particuliers, la complexité du problème du logarithme discret peut être réduite (exemple : $\sharp Ea_4, a_6, p = p$) ; ces courbes doivent donc être évitées pour sélectionner uniquement des courbes plus sûres[35].

3.4 Arithmétiques sur les courbes elliptiques

Soit E(K) :$y^2 = x^3 + ax + b$ une courbe elliptique, alors E(K) est un groupe pour la loi de composition suivante :
— P+$\vartheta = \vartheta + P = PpourtoutP \in$ E(K).
— $\vartheta + \vartheta = \vartheta$
Les cas où ϑ est un des deux termes de l'addition de deux points de E(K) ayant été traités, nous allons nous intéresser au cas où celui-ci n'est aucun des deux termes de l'addition.
Les formules permettant le calcul des coordonnées de l'opposé d'un point s'expriment ainsi :

Opposé d'un point :
Soit (x_P, y_P) les coordonnées non-homogènes d'un point P de E(K). Alors son opposé Q = -P a pour coordonnées :

$$\begin{cases} x_Q = x_P \\ y_Q = -y_P - a_1 x_p - a_3 \end{cases}$$

3.4.1 Addition des points

1ér Cas :
Prenons deux points P et Q sur cette courbe. En général, la courbe passant par P et Q recoupe la courbe en un troisième point de coordonnées (x, y). Son symétrique (x, -y) est lui aussi sur la courbe et on le désigne par P+Q pour signifier qu'il est construit à l'aide de P et Q. La chose surprenante est que cette opération "+" possède toutes les propriétés de l'addition des nombres. C'est-à-dire que l'on peut faire tous les calculs de type addition, soustraction et division avec un reste entier que nous faisons sur la droite des nombres réels sur cet courbe elliptique [39][33].
Règles de l'addition
Soient P = $(x_1; y_1)$ et $Q = (x_2; y_2)$ deux points sur E :
— Le point $(x_1; -y_1)$ est l'opposé du point P et il est noté -P.
— Si Q $\neq P$ et $Q \neq -P$, alors le point $R = P + Q = (x_3; y_3)$ est défini par :

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ Y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

— Si P = Q, alors le point$2P = (x_3; y_3)$ est définit par :

$$\begin{cases} x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ Y_3 = \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

— Si$x_1 = x_2$ mais $y_1 \neq y_2$, alors $R = \vartheta$.

— Si $P = Q$ et $y_1 = 0$, alors $R = \vartheta$.

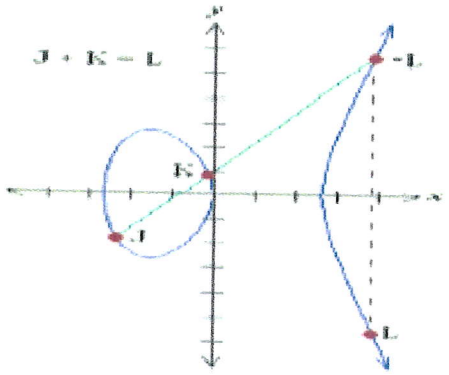


FIGURE 3.2 – Représentation de l'addition de P et Q

2 iéme Cas :

Si K = -J la droite passant par ces deux points dessinée se croise à un point à l'infini ϑ. D'où J + (-J) = ϑ. Un négatif d'un point est le symétrique de ce point en ce qui concerne l'axe des abscisses, La figure suivante est une l'illustration de ce cas .

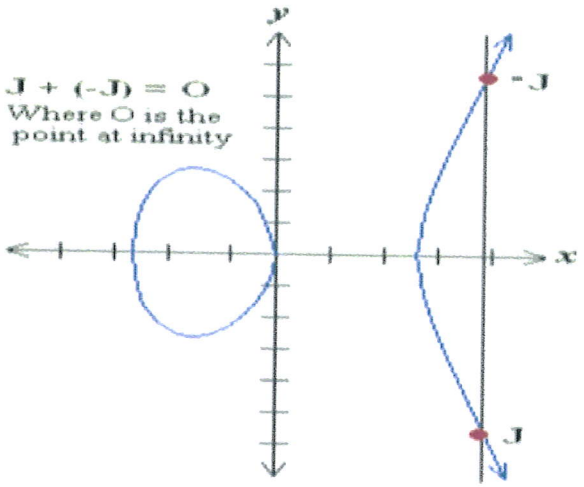


FIGURE 3.3 – Représentation du 2ième cas de l'addition de J et K.

3.4.2 Doublement de point

1er Cas :

Si la coordonnée du point J n'est pas le zéro alors la ligne de tangente à J croisera la courbe elliptique à exactement encore un point -L. Le symétrique du point L. En ce qui concerne l'axe des abscisses donne le point L, qui est le résultat du doublement du point J. Ainsi L = 2J. Comme le montre la figure suivante :

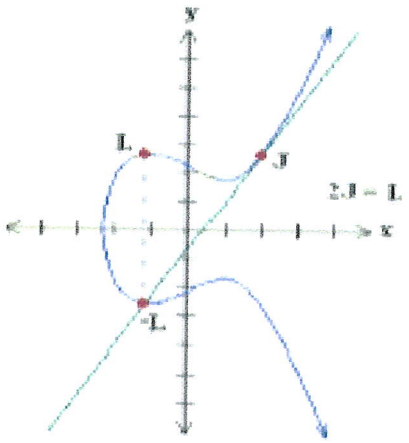


FIGURE 3.4 – Représentation du 1ér cas du doublement de point.

2ième Cas : Si la coordonnée du point J est le zéro alors la tangente à ce point se croise à un point à infini ϑ. De là $2J = \vartheta$ quand $YJ = 0$. La figure suivante illustre le doublement de point dans ce cas-là [33].

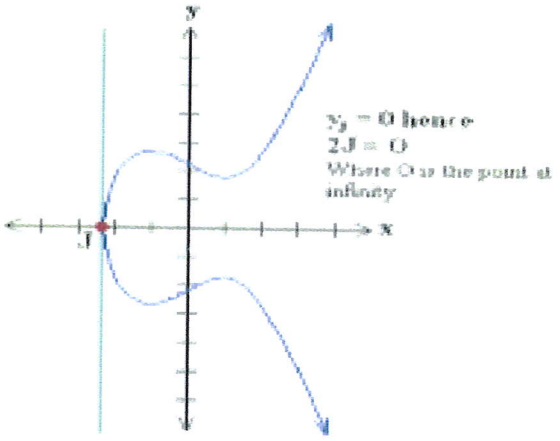


FIGURE 3.5 – Représentation du 2ième cas du doublement de point.

3.5 Cryptosystème basé sur les courbes elliptiques

3.5.1 Protocole d'échange de clés de Diffie-Hellmann

Alice et Bob veulent avoir une clé en commun pour s'échanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux. La méthode de Diffie-Hellmann permet justement de fair cela (en général on utilise cette méthode avec des groupes $\mathcal{U}_n$, mais nous présentons cette méthode adaptée pour les courbes elliptiques)[40].

1. Alice et Bob choisissent une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ tel que le logarithme discret soit difficile a résoudre. Il choisissent aussi un point $P \in E(\mathbb{F}_q)$ tel que le sous-groupe généré par P ait un ordre de grande taille. (En général, la courbe E et le point P sont choisis de manière a ce que l'ordre soit un grand nombre premier.)
2. Alice choisit un nombre entier secret a, calcule $P_a = aP$ et envoie P_a a Bob.
3. Bob choisit un nombre entier secret b, calcule $P_b = bP$ et envoie Pb a Alice.
4. Alice calcule aP_b = abP .
5. Bob calcule bPa = baP.
6. Alice et Bob utilisent une méthode quelconque connue pour extraire une clé secréte de abP . Par exemple, ils peuvent utiliser les derniers 256 bits de la premiére coordonnée de abP comme clé, ou ils peuvent hacher une des coordonnées de abP avec une fonction de hachage pour laquelle ils se sont mis d'accord.

La figure suivante illustre l'application de la méthode de Diffie-Hellman aux courbes elliptiques.

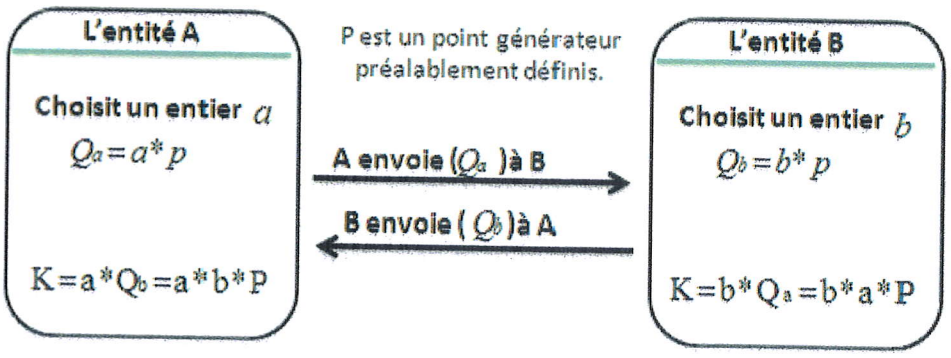


FIGURE 3.6 – Application de la méthode de Diffie-Hellman aux courbes elliptiques.

3.5.2 La méthode d'ElGamal

Alice veut envoyer un message secret à Bob. Tout d'abord, Bob fabrique une clé publique de la manière suivante. Il choisit une courbe elliptique E définie sur un corps fini F_q de telle manière que le problème du logarithme discret soit plus difficile 'a résoudre sur $E(\mathbb{F}_q)$ que sur $\mathbb{F}_q$. Il choisit aussi un point P sur E tel que l'ordre de P soit un grand nombre premier. Il choisit un nombre entier secret s et calcule B = sP. La courbe E, le corps fini Fq et les points P et B sont la clé publique de Bob. La clé secréte de Bob est s. Pour envoyer le message, Alice fait comme suit [34].

1. Elle télécharge la clé publique de Bob.
2. Elle transforme son message en un point M $\in E(\mathbb{F}_q)$.
3. Elle choisit un nombre entier secret k et calcule $M_1 = kP$.
4. Elle calcule $M_2 = M + kB$.
5. Elle envoie$M_1 et M_2$'$aBob$. Bob déchiffre le message en calculant
   $M = M_2 - sM_1$.
   Nous avons cette égalité parce que :
   $M_2 - sM1 = (M + kB) - s(kP) = M + k(sP) - skP = M$.
   Pour récupérer le texte en clair.

3.5.3 Signature électronique d'ElGamal

[41]

Les courbes elliptiques peuvent aussi être utilisées pour la signature électronique : Comment prouver à Bob que le message a bien été envoyé par Alice ?

L'idée est de joindre au message une signature électronique, l'équivalent de l'autographe dans le monde physique, qui certifie au destinataire l'identité de l'expéditeur.

Supposons donc qu'Alice envoie un message à Bob et qu'elle veuille signer électroniquement son message. Si elle utilise la signature ElGamal voici comment elle doit s'y prendre.

Alice doit tout d'abord créer une clé publique. Pour cela, elle choisit une courbe elliptique E définie sur un corps fini F_q , de manière que le problème du logarithme discret soit difficile sur E(F_q). Elle choisit aussi un point $A \in E(F_q)$, tel que l'ordre n de A est un grand nombre premier. De plus, elle choisit un nombre secret a et calcule B = aA. Finalement, Alice choisit encore deux fonctions, une fonction de hachage H :$\mathbb{N} \to \mathbb{N}$ et une fonction

$f : E(F_q) \to \mathbb{Z}$

Par exemple, si q est un nombre premier, elle peut prendre f(x, y) = x(mod q). L'information publique d'Alice est (E, F_q, A,B,H, f). Elle garde secret le nombre a. Pour signer son document, Alice fait comme suit :

1. Elle représente son document sous forme d'un nombre entier m et le hache, c'est à-dire calcule H(m) (n étant un grand nombre premier,$H(m) \leq n$. Si tel n'est pas le cas, on sépare le message en morceaux $m_1, ..., m_k$ tels que chaque $H(m_i) \leq n, 1 \leq i \leq k$.).
2. Elle choisit un nombre entier k avec PGCD(k, n) = 1 et calcule R = kA.
3. Elle calcule $s \equiv k$ - 1(H(m) - af(R))(mod n).

Le message signé est (m, s,R). Si Alice veut garder son message secret, elle peut par exemple le crypter avec le ECC ou RSA et utiliser le message crypté au lieu de m. Pour vérifier l'authenticité de la signature d'Alice, Bob procède de la manière suivante :

1. Il télécharge l'infor mation publique d'Alice.
2. Il calcule $V_1 = f(R)B + sRetV_2 = H(m)A$.
3. Si $V_1 = V_2$alors la signature est valide.

3.6 Utilisation de la cryptographie a base des courbes elliptiques

3.6.1 Efficacité de la courbe elliptique

Les courbes elliptiques fournissent de bons candidats de groupes car [42] :
— Elles forment un groupe, avec $\sharp E \sim O(p)$
— On dispose d'une arithmétique efficace.
— Pas de meilleure attaque connue que les attaques génériques.
— Clés plus faciles à générer et plus petites qu'avec RSA.

3.6.2 Équivalence entre RSA et ECC

Des travaux existants montre l'équivalence des tailles des clés offrant le même niveau de sécurité.Le tableau ci-dessous compare la taille des clés utilisées en cryptographie dans RSA et ECC :

taille de clé	
RSA	ECC
1024	160
2048	224
3072	256

TABLE 3.1 – Comparaison entre ECC et RSA

Nous remarquons que la cryptographie basée sur les courbes elliptiques permet d'utiliser des clés de taille moyenne comparativement à celles du RSA tout en fournissant les mêmes performances [33].

3.6.3 Des applications qui utilise ECC

De nos jours, plusieurs protocoles et plateformes utilisent la cryptographie à base des courbes elliptiques à cause de sa rapidité et sa sécurité. Parmi celle ci :

1. **TLS** Le protocole de sécurisation d'échange sur internet () utilise la ECC dans la phase "Handshake" pour l'agrément sur la clé à utiliser pour chaque session.
2. Smart Cards A coté de RSA, les nouvelles smart-card support la ECC.
3. Passport biométrique La ECC est utilisée pour construire la clé de session.
4. Bitcoin : ECC est utilisée pour la signature Transport Layer Security électronique pendant les transactions des paiement avec Bitcoin,la courbe utilisé par Bitcoin c'est Secp256k1 avec l'équation : $y^2 = x^3 + 7$ [41].

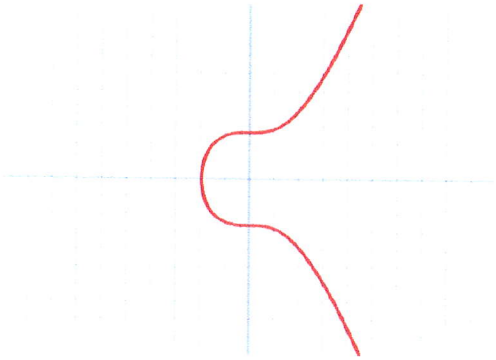


FIGURE 3.7 – La courbe Secp256k1 utilisé par Bitcoin

3.6.4 Quelques travaux similaires

Dans ce contexte, de nombreux travaux ont été élaborés afin d'introduire la cryptographie à base des courbes elliptiques pour les réseaux mobiles. dans ce qui suit, nous allons présenter quelques approches, qui sont conçues pour les réseaux mobiles en utilisant la méthode ECC.

1. **Protocole de P.G.Rajeswari et K.Thilagavathi :**
   Ce protocole d'authentification a été proposé par **P.G.Rajeswari et K.Thilagavathi** [43]. Ces deux auteurs proposent un simple protocole pour l'établissement de communications sécurisées entre la station de base et les noeuds des réseaux mobiles. Le protocole proposé est nouveau pour le schéma d'authentification, simple et efficace. Il est conçu en utilisant un schéma de cryptographie à clé publique très familier, la cryptographie à courbe elliptique, puis il est dédié aux réseaux mobiles pour l'authentification de la station de base. L'utilisation de ce protocole dans les réseaux de téléphonie mobile permettra uniquement à la station de base autorisée d'accéder au noeud et, par conséquent, les informations seront refusées aux oreilles indiscrètes lorsqu'ils essaieront de pirater ou d'abuser du noeud.

2. **une technologie de** "$FengXu, XuanZhou, DanZhou, ShushengPeng$" **:**
   dans un système ZigBee "$FengXu, XuanZhou, DanZhou, ShushengPeng$"[44] proposent une technologie simple de cryptage et d'authentification ECC ,est présentée entre un noeud terminal et un ordinateur hôte. Cette méthode permet non seulement d'économiser de l'énergie et des frais de stockage, mais également de réduire la charge informatique du réseau, améliore la sécurité des données et réduit les risques de sécurité liés au cryptage, à la distribution et à l'échange de clés.
3. **Présentation de Wenbo Shi et Peng Gong :**
   Wenbo Shi et Peng Gong [45] propose Un nouveau protocole d'authentification d'utilisateur pour les Réseaux de capteurs sans fil utilisant la cryptographie à courbes elliptiques . Avant d'émettre une requête à un noeud de capteur, chaque utilisateur doit s'enregistrer auprès de la passerelle de manière sécurisée afin qu'ils puissent accéder aux données des capteurs en temps réel. Sur l'utilisateur réussi demande d'enregistrement, le noeud de passerelle personnalise une puce carte pour chaque utilisateur enregistré. Ensuite, un utilisateur peut soumettre son interroger de manière authentique et accéder aux données du réseau de capteurs à tout moment pendant une période configurable par l'administrateur.

3.7 Les attaque sur la cryptographie à base des courbes elliptiques

Puisque le cryptage des messages avec des courbes elliptiques se base sur la difficulté de résoudre le problème du logarithme discret en un temps raisonnable généralement, il est important de savoir dans quels cas nous pouvons le résoudre rapidement pour éviter ces cas là.

3.7.1 Baby step Geant step

C'est l'une des méthodes générales les plus rapides de résolution du journal discret EC problème. Cette méthode, développée par D. Shanks, (En fait, il peut être appliqué à un groupe arbitraire.) L'algorithme fonctionne dans environ $\sqrt{N}$ heure et $\sqrt{N}$ espace,où$N = \sharp E(F_q)$. Ce n'est pas assez rapide pour être pratique[46].
Problème : Trouver k tel que kP = Q sur E $(F_q), avec \sharp E(F_q)$= N, en supposant que un tel k existe.
Algorithm :

1. Choisissez un entier m > $\sqrt{N}$
2. Calculer mP.
3. For i = 0 to i = m - 1 calculer (et stocker) iP

4. For j = 0 to j = m - 1 caluler (et stocker) Q - jmP.
5. Triez les listes des étapes 3 et 4 de manière cohérente.
6. Comparez les listes des étapes 3 et 4 jusqu'à une paire i, j telle que iP = Q - jmP est trouvé
7. Retourne k ≡ i + jm (mod N).

3.7.2 L'attaque MOV

Les travaux menés en 1993 par Menezes, Okamoto et Vanstone, qui ont donné leurs noms à l'attaque MOV, montrent que le problème du logarithme discret sur$E(F_p)$ peut être ramené à celui du logarithme discret dans $(F_p^k)^*$. En particulier dans le cas de courbes super singulières, il peut être ramené à celui du logarithme discret sur (F_p^k) avec k 2 1, 2, 3, 4, 6, généralement k = 2. Cela induit un risque car la réduction à un tel problème se fait en temps polynomial en O(logp), et la résolution du problème du logarithme discret est alors réalisable par un algorithme probabiliste sous-exponentiel [41].

3.7.3 Force brute

L'attaque par force brute consiste à calculer P, 2P, ..., jusqu'à ce qu'on trouve k. Au pire des cas l'attaque nécessite n opérations (l'ordre de la courbe).
En 1996 une attaque sur un système cryptographique basé sur les EC de clé de 120 bits a été esquissée et réalisée après 3 ans. L'attaque était basée sur un matériel dédié qui peut faire 25 million d'opérations en parallèle. Le coût de construire cette machine était de $ 10 million et le temps nécessaire pour obtenir la clé était 32 jours [41].

3.7.4 Attaque par cannaux cachés

Les attaques par canaux cachés profitent des fuites d'information involontairement divulguées par un dispositif de cryptage. Ces fuites peuvent être utilisées pour lancer différents types d'attaques telles que l'analyse simple de l'énergie (SPA : Simple Power Analysis) et l'analyse différentielle de l'énergie (DPA : Differential Power Analysis). SPA analyse un seul tracé de la consommation d'énergie durant l'exécution de l'algorithme, tandis que DPA est un ensemble d'analyses statistiques à travers plusieurs tracés issus de 66 l'exécution.L'exécution d'un algorithme de chiffrement par un processeur peut laisser échapper de nombreuses informations en rapport avec la clé de chiffrement. Ces informations peuvent être le temps de calcul, la consommation d'énergie, le rayonnement électromagnétique, voire même le son émis par le processeur[47].

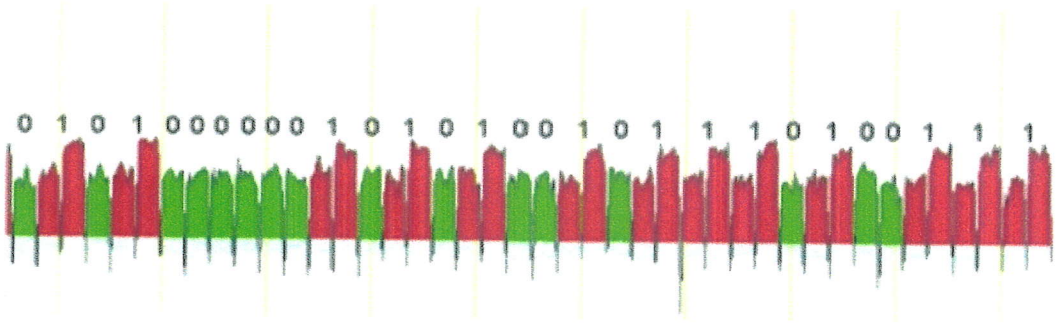


FIGURE 3.8 – Analyse des bits par canaux cachés.

Puisque le chiffrement d'un point avec les courbes elliptiques (la multiplication d'un point k fois où k est la clé) est une succession de doublements et d'addition de points dont l'enchaînement dépend directement de la clé, cette dernière peut être extraite.
Pour éviter ces attaques, on peut :
— Adapter les algorithmes des chaînes d'additions euclidiennes ou différentielles [41].
— Rajouter de l'aléa pour masquer la clé.
Il faut remarquer qu'aucune attaque par analyse des temps de calcul n'est possible sur les cryptosystémes ECC si toutes les opérations s'effectuant a tous les niveaux de hiérarchie (opérations modulaires, opérations de points, multiplication scalaire, protocole cryptographique) s'exécutent a temps constant, et ce, quelque soit la valeur de la clé[48].

3.8 Conclusion

Dans ce chapitre, nous avons présenté la cryptographie sur les courbes elliptiques ainsi que l'ensemble de termes mathématiques indispensables pour comprendre son fonctionnement.d'aprés équivalence representé dans le chapitre entre RSA et ECC ,nous pouvons remarquer que ECC est un cryptosystème plus attractif.

La difficulté actuel est de mentionner que la mise en oeuvre de Le cryptosystème à base des courbes elliptiques est difficile,nécessitant beaucoup de théories mathématiques.Dans le chapitre suivant, nous présentons notre modèle qui nous permet d' améliorer le niveau de sécurité au sein des terminaux mobiles en prenons en compte les ressources limité de ce dernier.

Chapitre 4

Contribution :Proposition d'un Modèle à base des courbes elliptiques

4.1 Introduction

Après avoir présenter une étude détaillée sur l'une des méthodes de cryptographie à clé publique ECC ainsi que les réseaux mobiles.Nous proposons dans ce chapitre un modèle multi niveau basé sur les courbes elliptique dédié aux Réseaux mobiles ,qui permet de choisir la méthode de chiffrement adaptée a chaque application selon les ressources disponible d'un terminale mobile.

Nous allons présenter une conception de ce modèle en fonction d'une modélisation UML basé sur le diagramme de classe et le diagramme d'activité afin de définir la structure static et dynamique de notre modèle.

4.2 Présentation du Modèle

Cette partie présente une proposition d'un chiffrement à multi niveaux qui prendre en considération les ressources utilisés par un terminal portable (espace mémoire,vitesse CPU,durée de vie de batterie...)d'une part et les exigences de l'application qui tourne sur ce dernier d'autre part.

La majorité des applications qui souhaitent chiffrer ses données ou d'une partie de celles-ci exigent deux critères : la sécurité et la durée nécessaire au traitement des données qui ont des niveaux différents,par exemple les applications de E-commerce nécessitent un chiffrement sûr et notamment pour vérifier les données de transaction, Mais elles n'ont pas besoins d'un temps d'exécution réduit,Contrairement aux applications des urgences qui besoin d'une transmission rapide .D'un autre coté les terminaux portable ayant des capacités différentes en terme des ressources (mémoire ,CPU,batterie).

Afin de remédier a cette situation nous proposons un modèle de chiffrement qui prend en considération le niveau de la sécurité d'un part et la capacité des ressources utilisé par le terminale mobile d'autre part.

Dans ce contexte nous proposons trois niveaux de sécurité,chaque niveau utilise une méthode de chiffrement ou bien une combinaison des méthodes , les trois niveaux sont basés au moins sur la méthode de chiffrement ECC :

- **Niveau 1 :** ce niveau utilise seulement la méthode ECC pour :
  - Une sécurité forte
  - Une vitesse moyenne
  - Une taille mémoire moyenne
- **Niveau 2 :**dans ce niveau nous avons combiner entre deux méthodes de chiffrement l'une est une méthode de chiffrement asymétrique ECC pour l'échange de clé et l'autre méthode de chiffrement symétrique AES pour l'échange des données.Ce niveau propose :
  - Une sécurité forte
  - Une vitesse optimale
  - Une taille mémoire importante
- **Niveau 3 :** pour élever le niveau de sécurité plus que dans le niveau 2 nous proposons de combiner les deux méthodes AES,ECC avec une autre méthode, telque une méthodes de masquage qui rend les messages invisible .Afin de prendre une sécurité très forte.

4.3 Conception du modèle

Afin de définir la structure statique du modèle nous allons le présenter sous forme d'un diagramme de classe, ainsi le comportement dynamique sera présenté ensuite par un diagramme d'activité.

4.3.1 Diagramme de classe

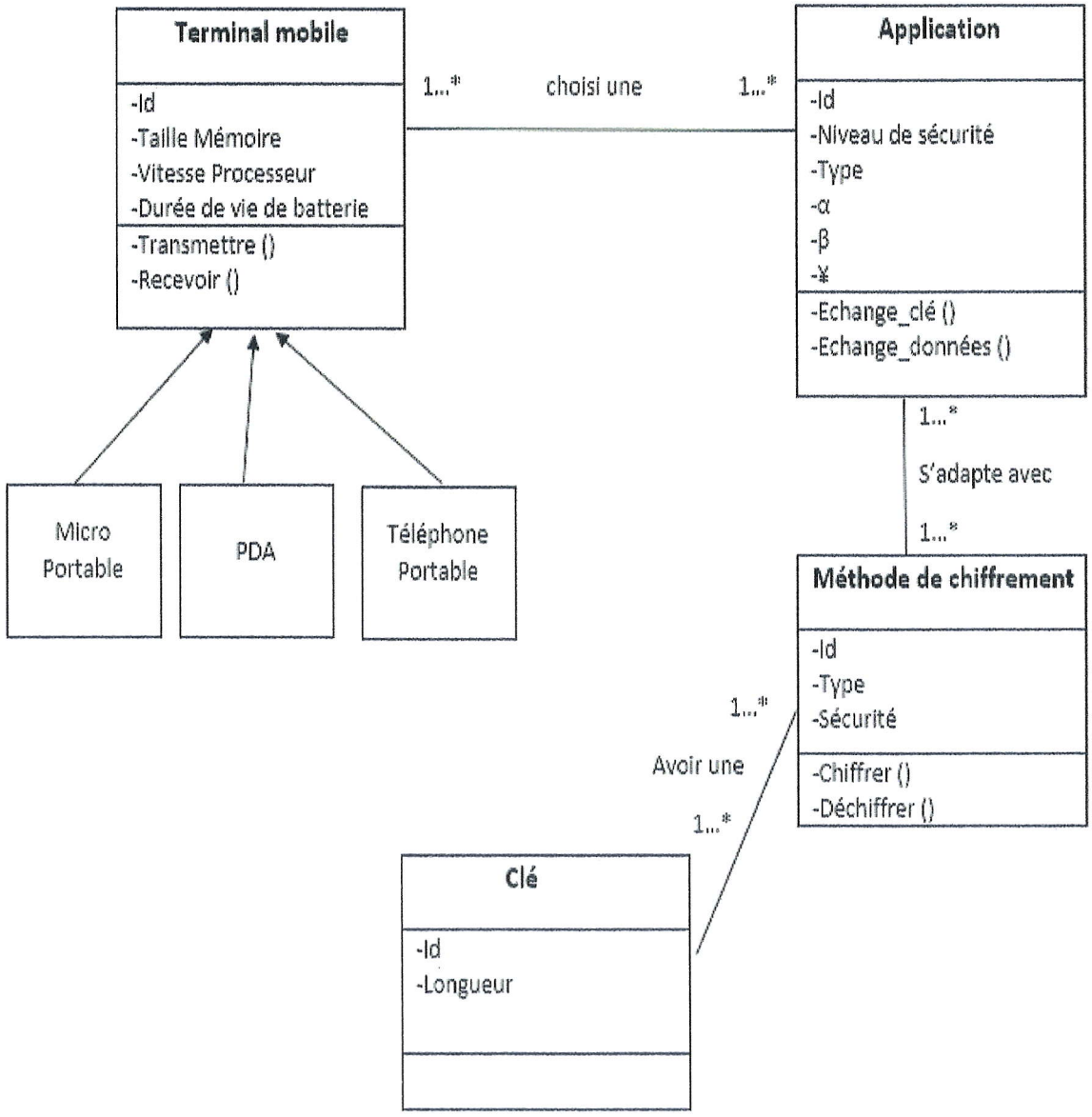


FIGURE 4.1 – La structure statique du modèle proposé.

4.3.1.1 Les classes candidates

Classe	Attributs	Méthodes
Appareil mobile	-Id d'appareil -Niveau d'énergie -Taille de mémoire -Vitesse de processeur	**-transmettre ()** : cette méthode Permet à un appareil d'envoyer un message. **-recevoir ()** : cette méthode Permet à un appareil de recevoir un message.
PDA **Téléphone mobile** **Micro portable**	- les mêmes attributs et les méthodes d'un appareil +autre attributs Selon leur type	
Application : cette classe représente les applications qui on peut les exécutés sur un appareil mobile	-Id d'application **-Type** : il ya comme type d'application (E-commerce, Discussions, réunion confidentiel....etc.). -Niveau de sécurité. **- α, β, γ** : Sont les paramètres d'équilibrage permettant de privilégier une méthode selon l'application à exécuter.	**-échange de clé** : Permet d'échanger la clé publique entre deux communicant. **-échange de donnés** : cette méthode sert d'échanger les donnés.
Méthode : elle représente l'ensemble des méthodes qui peuvent être utilisés par une ou plusieurs applications	-Id méthode. **-taille de clé** : la taille de clé utiliser pour chaque méthode de chiffrement.	**Chiffrer ( )** : permet de transformer le message en clair a un message chiffrer. **Déchiffrer ( )** : une méthode permet de transformer le message chiffrer a un message clair

FIGURE 4.2 – Les classes candidates.

Une décision multicritéres a été utilisé pour calculer la méthode a exécuter , cette décision dépend de trois paramètres : α, β, γ .

α,β,γ : Sont des paramètres d'équilibrage permettant de privilégier une méthode par rapport a l'autre selon l'application a exécuter et les ressources disponibles d'un terminale mobile.

Pour simplifier notre étude, nous supposons que ces paramètres sont indépendants et nous introduisons la relation linéaire suivante pour choisir la méthode de chiffrement à exécuter on prenant compte les paramètres N, M et P,tel que :

$$R{=}\alpha \mathrm{N} + \beta\ \mathrm{M} + \gamma\ \mathrm{P}$$

Sachant que :

N : Niveau d'énergie **M** : L'espace mémoire **P** : Vitesse de CPU

4.3.2 Diagramme d'activité

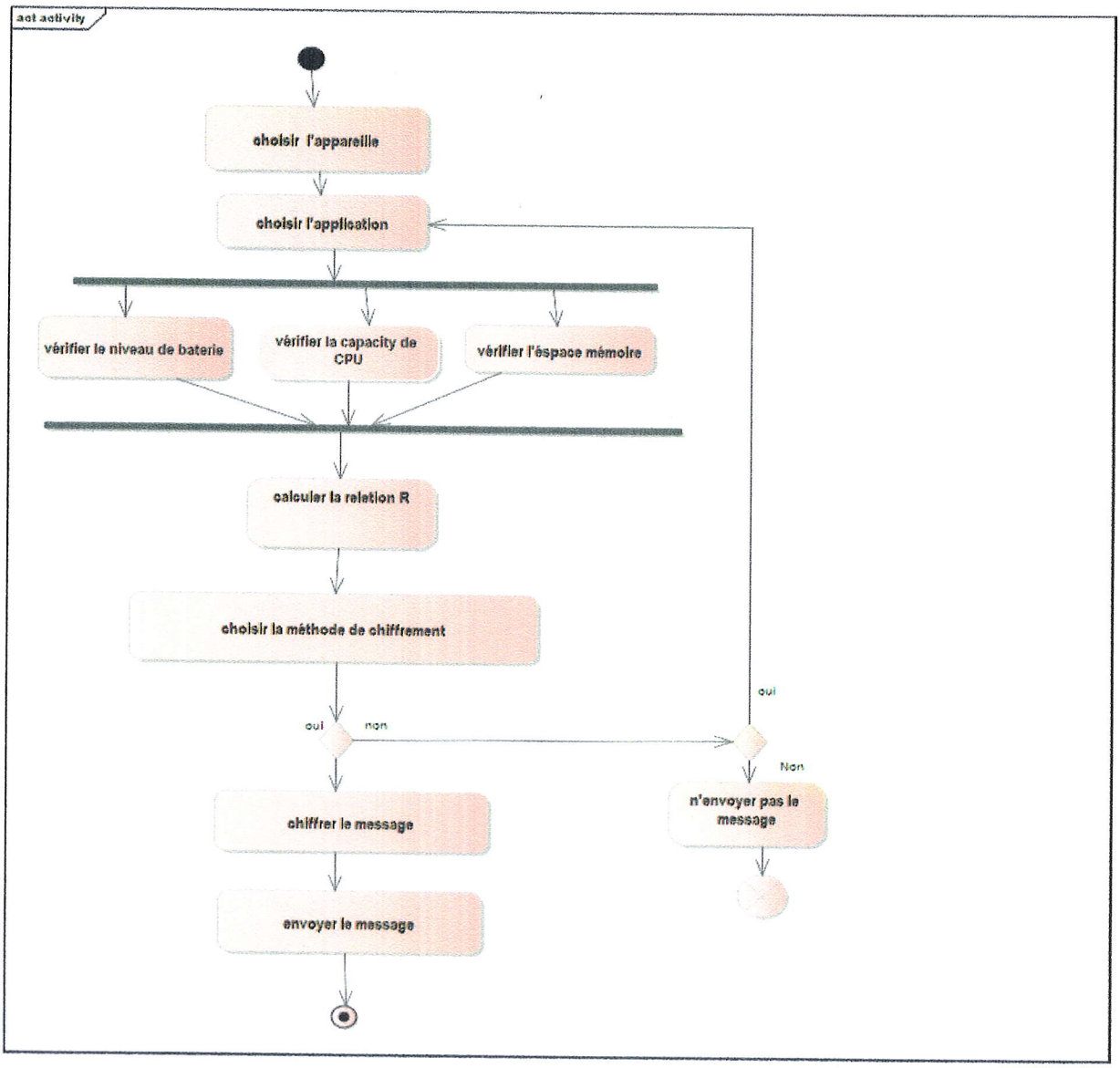


FIGURE 4.3 – La structure dynamique du modéle proposé.

4.4 Analyse comparative entre RSA et ECC

Afin de montrer l'efficacité de notre modèle ,Nous allons comparer la méthode ECC qui représente le niveau bas de sécurité par rapport a les trios niveaux de notre modèle avec RSA en terme de temps d'exécution.

En effet RSA et ECC sont connus comme les PKC les plus efficaces parmi tous les algorithmes de chiffrement asymétriques . Des travaux existant pensent que les courbes elliptiques offrent une bonne sécurité avec des clés plus petites, ce qui est très

utile dans de nombreuses applications.

c'est pour quoi nous avons fait une implémentation de RSA et ECC avec trois entrées d'échantillons de 15 bits, 63 bits, 255 bits.

nous avons choisir 5 types de courbes parmi les courbes proposées par la recommandation du NIST [49] sur $GF(p)$: $\{P-160, P-224, P-256, P-384, P-521\}$, ces courbes sont illustrés dans les tableaux suivants ,tel que :

— a et b : les coefficients de : x^3+ax+b mod p.
— r :Ordre de point de base.

— G(x,y) :Le point de base.

Selon la taille de la clé a,b,p,r seront :

Courbe P-160	
a	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC
p	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF
r	01 00000000 00000000 0001F4C8 F927AED3 CA752257
b	1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45
Gx	4A96B568 8EF57328 46646989 68C38BB9 13CBFC82
Gy	23A62855 3168947D 59DCC912 04235137 7AC5FB32

TABLE 4.1 – Courbe P-160.

Courbe P-224	
a	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFE
p	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 00000000 00000001
r	FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D
b	b4050a85 0c04b3ab f5413256 5044b0b7 d7bfd8ba 270b3943 2355ffb4
Gx	b70e0cbd 6bb4bf7f 321390b9 4a03c1d3 56c21122 343280d6 115c1d21
Gy	bd376388 b5f723fb 4c22dfe6 cd4375a0 5a074764 44d58199 85007e34

TABLE 4.2 – Courbe P-224

Courbe P-256	
a	FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC
p	FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF
r	FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
b	5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b
Gx	6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296
Gy	4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

TABLE 4.3 – Courbe P-256

Courbe P-384	
a	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFC
p	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFF
r	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973
b	b3312fa7 e23ee7e4 988e056b e3f82d19 181d9c6e fe814112 0314088f 5013875a c656398d 8a2ed19d 2a85c8ed d3ec2aef
Gx	aa87ca22 be8b0537 8eb1c71e f320ad74 6e1d3b62 8ba79b98 59f741e0 82542a38 5502f25d bf55296c 3a545e38 72760ab7
Gy	3617de4a 96262c6f 5d9e98bf 9292dc29 f8f41dbd 289a147c e9da3113 b5f0b8c0 0a60b1ce 1d7e819d 7a431d7c 90ea0e5f

TABLE 4.4 – Courbe P-384

Courbe P-521	
a	01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFC
p	01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
r	01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFA 51868783 BF2F966B 7FCC0148 F709A5D0 3BB5C9B8 899C47AE BB6FB71E 91386409
b	051 953eb961 8e1c9a1f 929a21a0 b68540ee a2da725b 99b315f3 b8b48991 8ef109e1 56193951 ec7e937b 1652c0bd 3bb1bf07 3573df88 3d2c34f1 ef451fd4 6b503f00
Gx	c6 858e06b7 0404e9cd 9e3ecb66 2395b442 9c648139 053fb521 f828af60 6b4d3dba a14b5e77 efe75928 fe1dc127 a2ffa8de 3348b3c1 856a429b f97e7e31 c2e5bd66
Gy	118 39296a78 9a3bc004 5c8a5fb4 2c7d1bd9 98f54449 579b4468 17afbd17 273e662c 97ee7299 5ef42640 c550b901 3fad0761 353c7086 a272c240 88be9476 9fd16650

TABLE 4.5 – Courbe P-521

Les expériences sont effectuées sur Netbeans 8.1 sur un processeur intel-core Intel Pentium avec 4 GB de RAM DDR3 sous la plate-forme Windows 10. L'expérimentation a été menée pour trouver le laps de temps lors du chiffrement, le déchiffrement et génération des clés par RSA et ECC ,L'efficacité de ECC sur RSA est illustrée dans les tableaux suivants.

Entrée : 15 bits						
	RSA			ECC		
taille clé(bits)	généclé (s)	chiff(s)	déchi(s)	généclé(s)	chiff(s)	déchi(s)
1024/160	0.263	0.008	0.012	0.132	0.08	0.024
2048/224	0.948	0.04	0.048	0.184	0.096	0.036
3072/256	1.644	0.12	0.136	0.184	0.128	0.044
7680/384	122.614	1.787	1.788	0.244	0.224	0.052
15360/521	847.649	13.713	13.979	0.304	0.36	0.116

TABLE 4.6 – 15bits-temps de chiffrement, déchiffrement et génération de clé

Entrée : 63 bits						
	RSA			ECC		
taille clé(bits)	généclé(s)	chiff(s)	déchiff(s)	génerclé (s)	chiff(s)	déchiff (s)
1024/160	0.62	0.012	0.016	0.184	0.212	0.016
2048/224	0.62	0.04	0.044	0.172	0.234	0.016
3072/256	2.765	0.125	0.203	0.235	0.312	0.031
7680/384	131.978	1.877	2.016	0.25	0.516	0.047
15360/521	27.771	16.603	17.733	0.281	1.078	0.094

TABLE 4.7 – 63bits-temps de chiffrement, déchiffrement et génération de clé

Entrée : 255 bits						
	RSA			ECC		
taille clé(bits)	généclé (s)	chiff(s)	déchi(s)	généclé(s)	chiff (s)	déchi(s)
1024/160	0.332	0.004	0.012	0.203	0.515	0.016
2048/224	1.438	0.031	0.047	0.203	0.615	0.031
3072/256	1.016	0.14	0.172	0.188	0.75	0.031
7680/384	120.477	1.964	1.999	0.264	1.816	0.068
15360/521	153.045	14.603	15.253	0.281	3.516	0.125

TABLE 4.8 – 255bits-temps de chiffrement, déchiffrement et génération de clé

Nous allons voir les résultats obtenus de temps de chiffrement et génération de clés dans les figures suivantes :

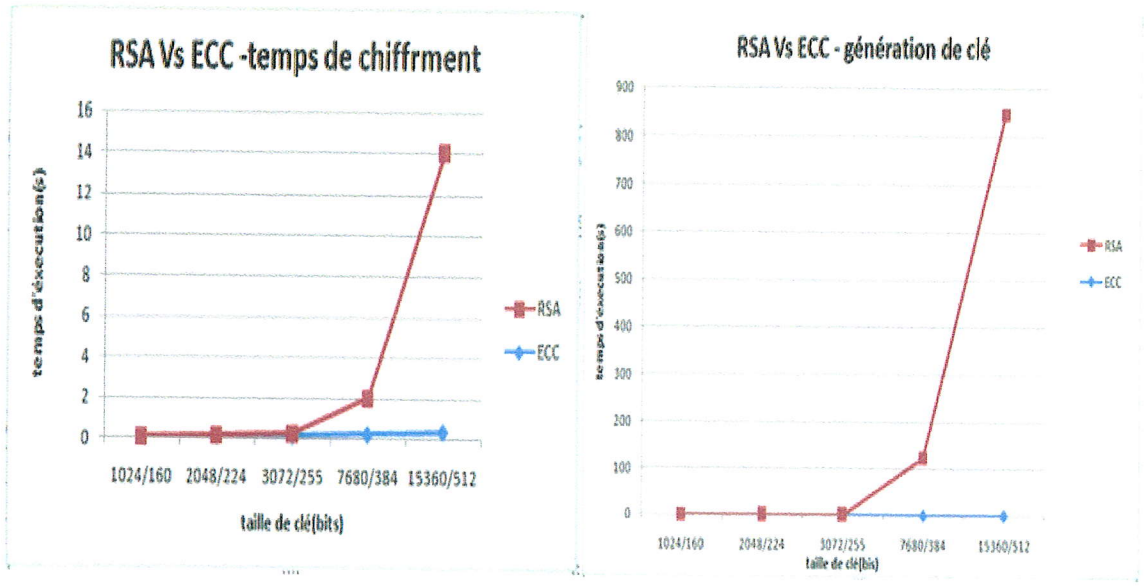


FIGURE 4.4 – Comparaison entre RSA et ECC-Entré 15bit.

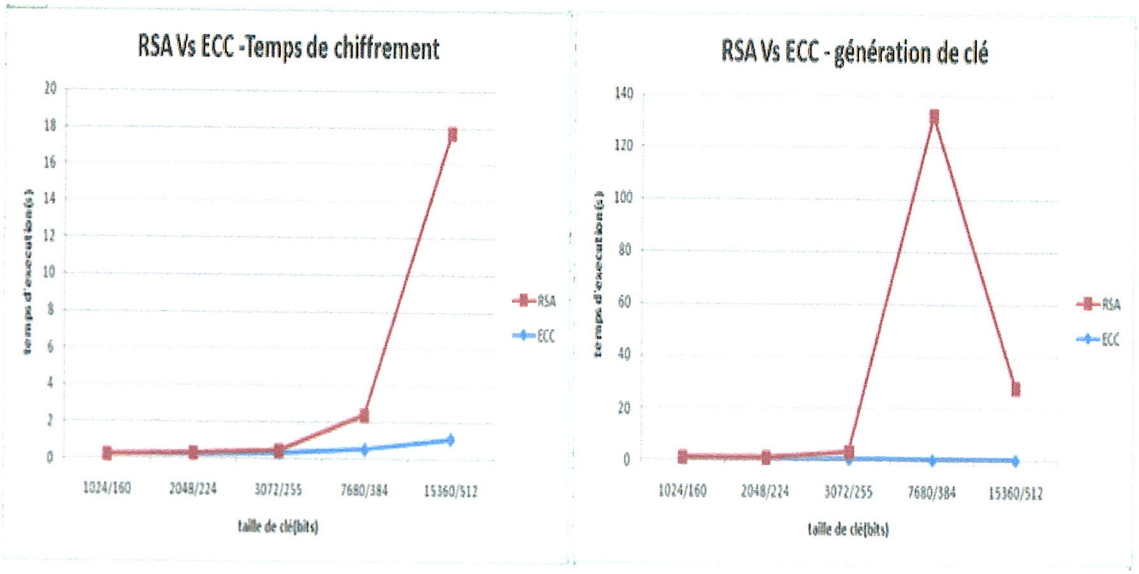


FIGURE 4.5 – Comparaison entre RSA et ECC-Entré 63bit.

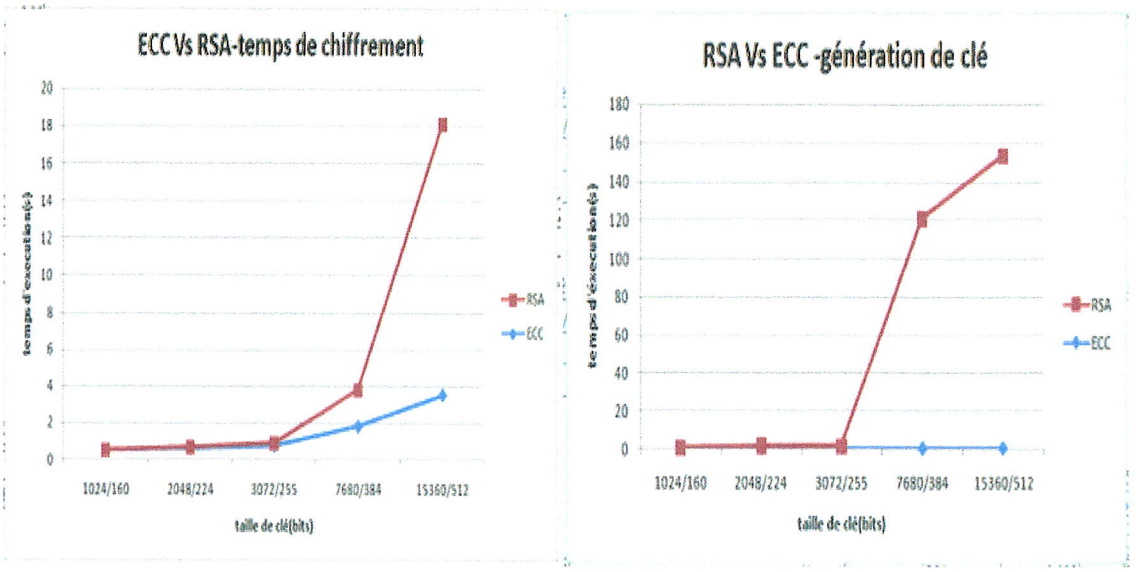


FIGURE 4.6 – Comparaison entre RSA et ECC-Entré 255bit.

Sur la base des expérimentations et les graphes obtenus dans les figures(4.4),(4.5) et (4.6) .Nous remarquons que comparé à la performance de ECC ,RSA est plus lent que l'ECC en terme de temps de chiffrement et génération de clé.

Cette différence de performance Augmente lorsque la taille des clés et des données augmentent.En conséquent ,ECC offre une vitesse (temps) de chiffrement plus rapide que RSA.

4.5 Avantages de notre modèle

- Fournir un haut niveau de sécurité pour les terminaux mobiles adéquate a leur caractéristiques.
- Offre une solution de sécurité efficace en terme de charge de calcul ,de préservation d'énergie et espace mémoire.
- Fournir une bonne flexibilité qui rendre l'utilisateur ne dépende pas par un seule méthode de chiffrement.

4.6 Conclusion

Le chiffrement par courbes elliptiques utilise des clés relativement petites et est mathématiquement très efficace, qui la rend idéal pour des petits dispositifs du communication utilisés aujourd'hui.

Dans ce chapitre, nous avons proposer un modèle de chiffrement basé sur les courbes elliptiques dédié aux réseaux mobiles.Afin de définir la structure statique et dynamique du modèle ,nous le présenté sous forme d'un diagramme de classe et un digramme d'activité.Ce chapitre contient aussi une analyse comparative en terme de temps d'exécution entre RSA et ECC. Les résultats obtenu montre l'efficacité de notre modèle.

Dans le chapitre suivant, certains détails concernant la réalisation d'un cas d'application et les outils technologiques utilisés seront présentés.

Chapitre 5

Cas d'application : Implémentation d'un chat

5.1 Introduction

Nous présentons dans ce chapitre, les étapes de conception et les outils de réalisation .Ainsi une implémentation d'un mini chat basé sur ECC comme un cas d' application d'une partie de notre modèle.

5.2 Conception

5.2.1 Présentation UML

UML est un langage formel, normalisé et un support de communication performant qui permet grâce à sa représentation graphique, de concevoir des solutions, de faciliter la comparaison et l'évolution de celles-ci. Son caractère polyvalent et sa souplesse ont en fait un langage de modélisation universel

5.2.2 Identification des acteurs

Un acteur représente un rôle joué par un utilisateur humain ou un autre système qui interagit directement avec le système étudié. Un acteur participe à au moins un cas d'utilisation.
Dans notre cas, nous avons un acteur qui est :

Client : a un accès au système via un contrôle d'accès (login et mot de passe). Les opérations qu'il peut effectuer sont :

— .Envoyer et recevoir des invitations.
— Envoyer et recevoir des messages textuel.
— Envoyer et recevoir des pièces jointes.
— Modifier le type de courbe.
— Se déconnecter.

5.2.3 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation représente la structure des grandes fonctionnalités nécessaires aux utilisateurs du système. C'est le premier diagramme du modèle UML, qui assure la relation entre l'utilisateur et les objets que le système met en oeuvre.

Nous illustrons à travers le diagramme de cas d'utilisation relatif à un client.

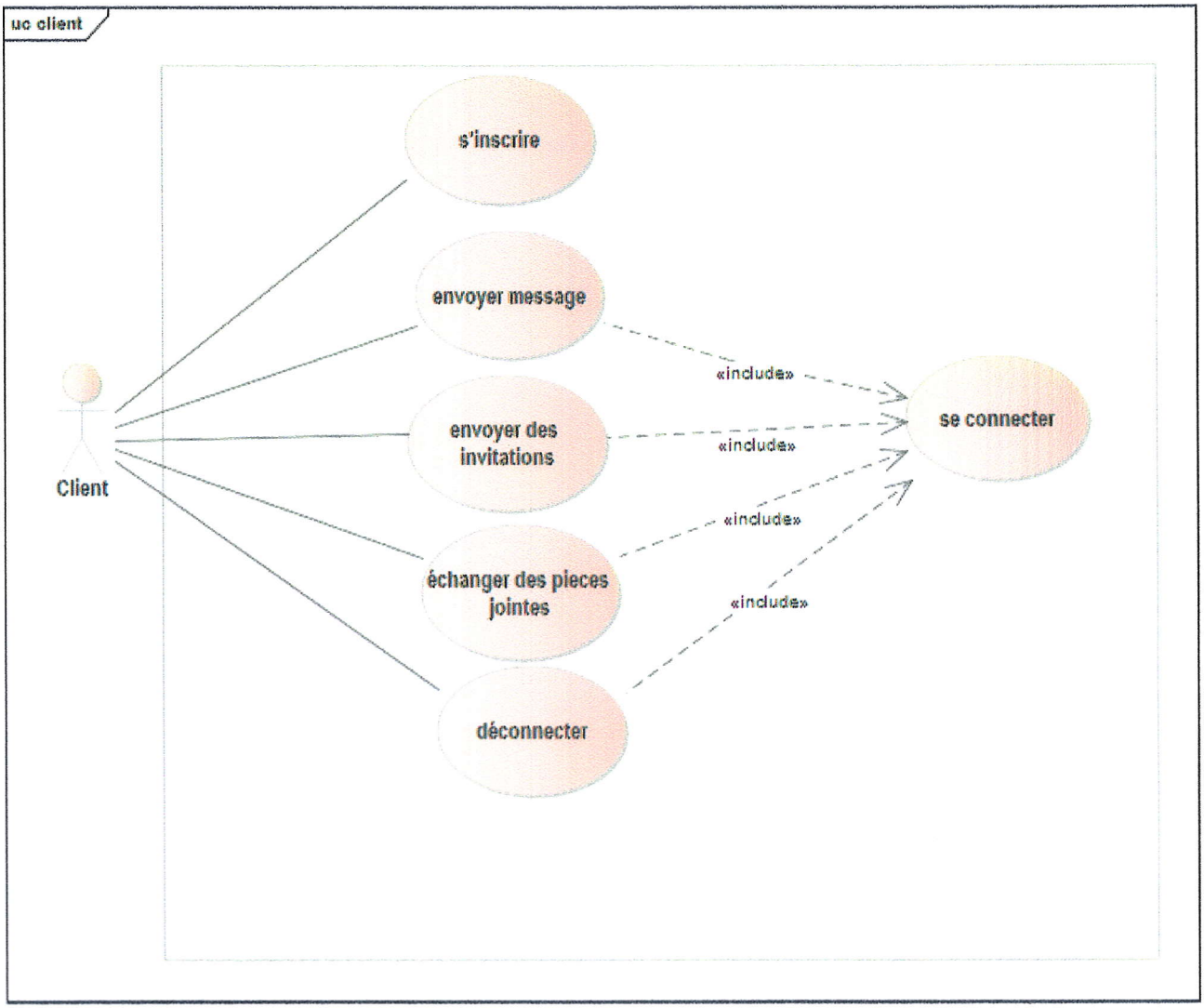


FIGURE 5.1 – Cas d'utilisation associé à un client

Diagramme du cas d'utilisation se connecté

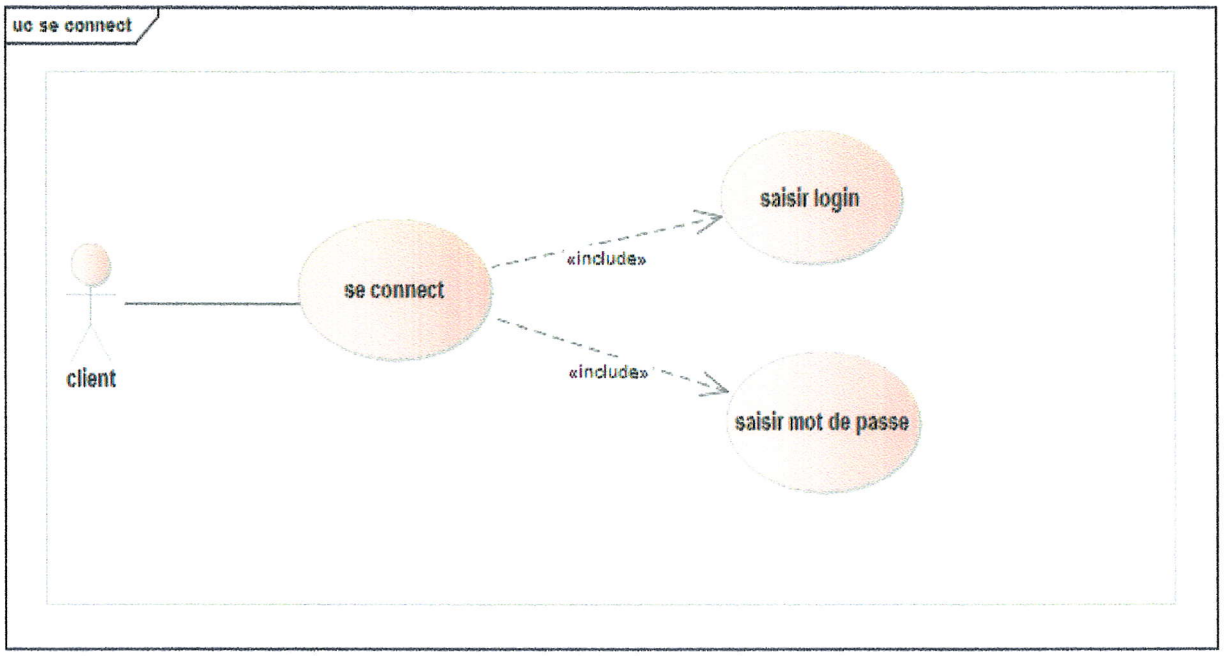


FIGURE 5.2 – Diagramme du cas d'utilisations "*seconnecté*".

Diagramme du cas d'utilisation Inscription

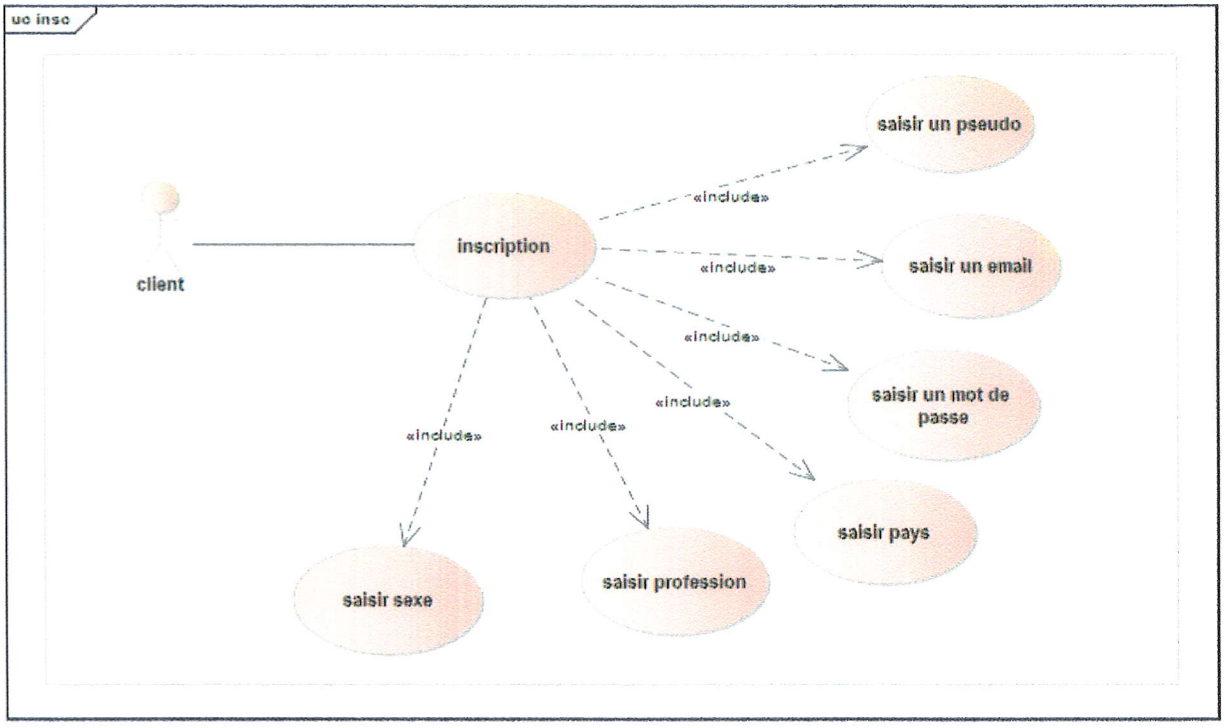


FIGURE 5.3 – Diagramme du cas d'utilisation "*Inscription*".

Description du cas d'utilisation Envoyer des messages

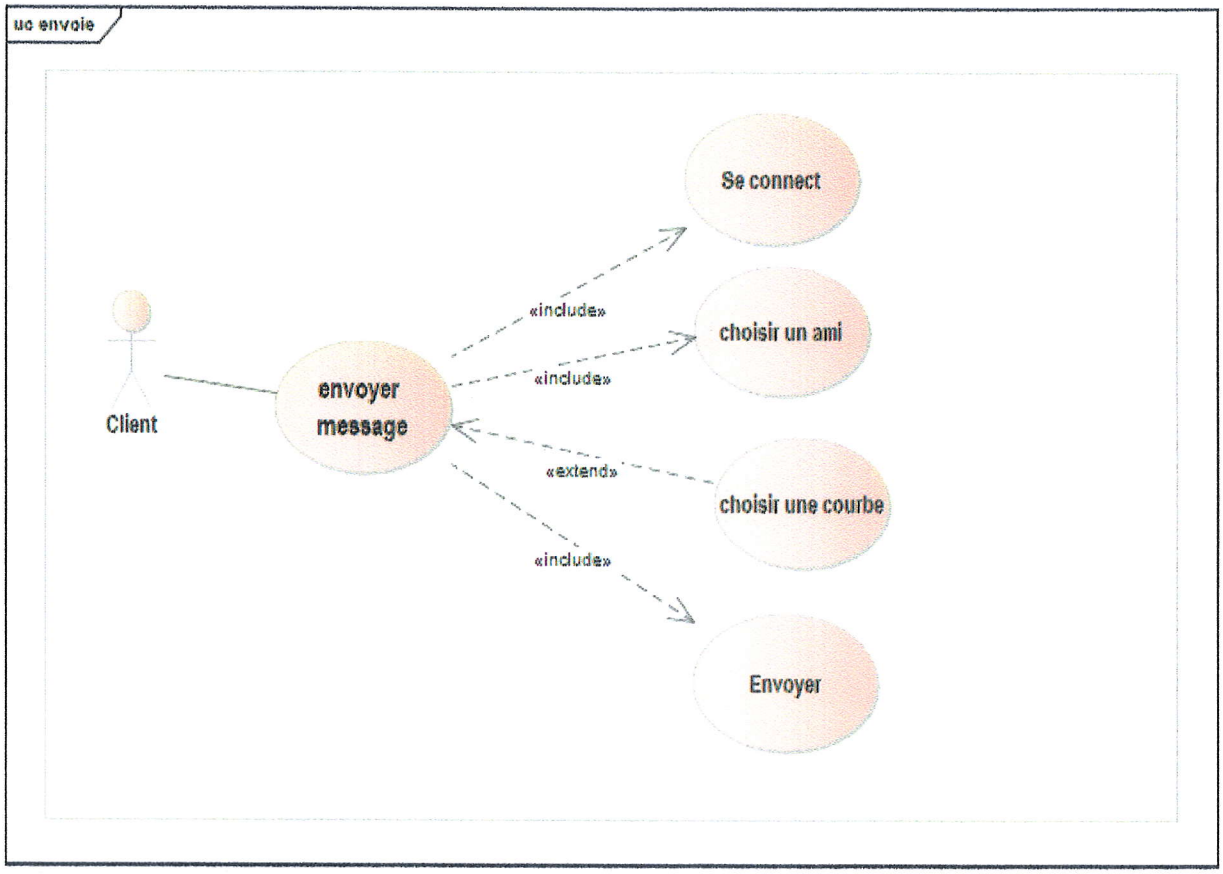


FIGURE 5.4 – Diagramme du cas d'utilisation "*Envoyer des messages*".

5.2.4 Diagramme de séquence

Un diagramme de séquences est un diagramme d'interaction qui expose en détail la façon dont les opérations sont effectuées : quels messages sont envoyés et quand ils le sont.

2.3.1 Inscription

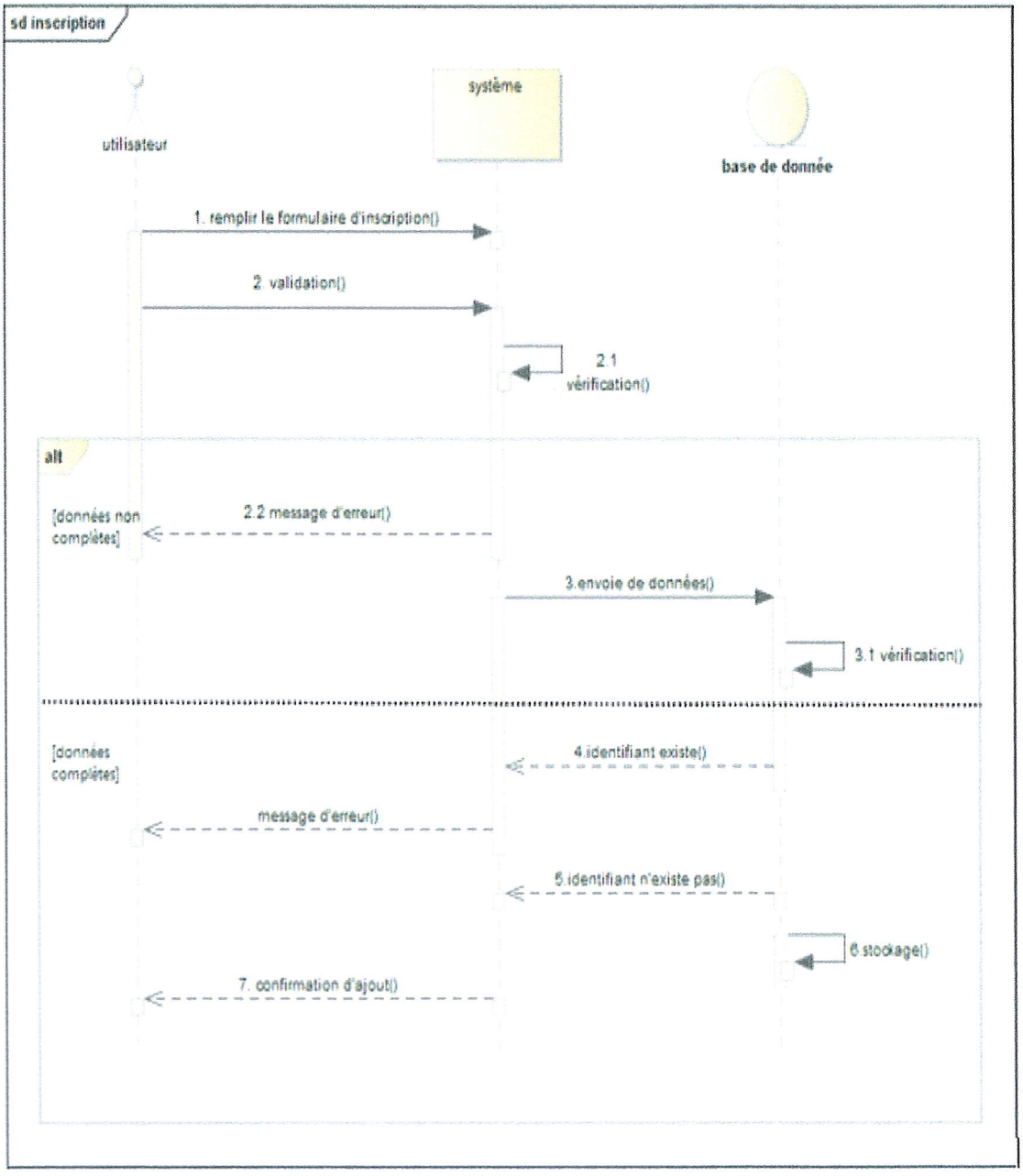


FIGURE 5.5 – Diagramme de séquence du cas d'utilisation "*Inscription*".

2.3.2 se connecté

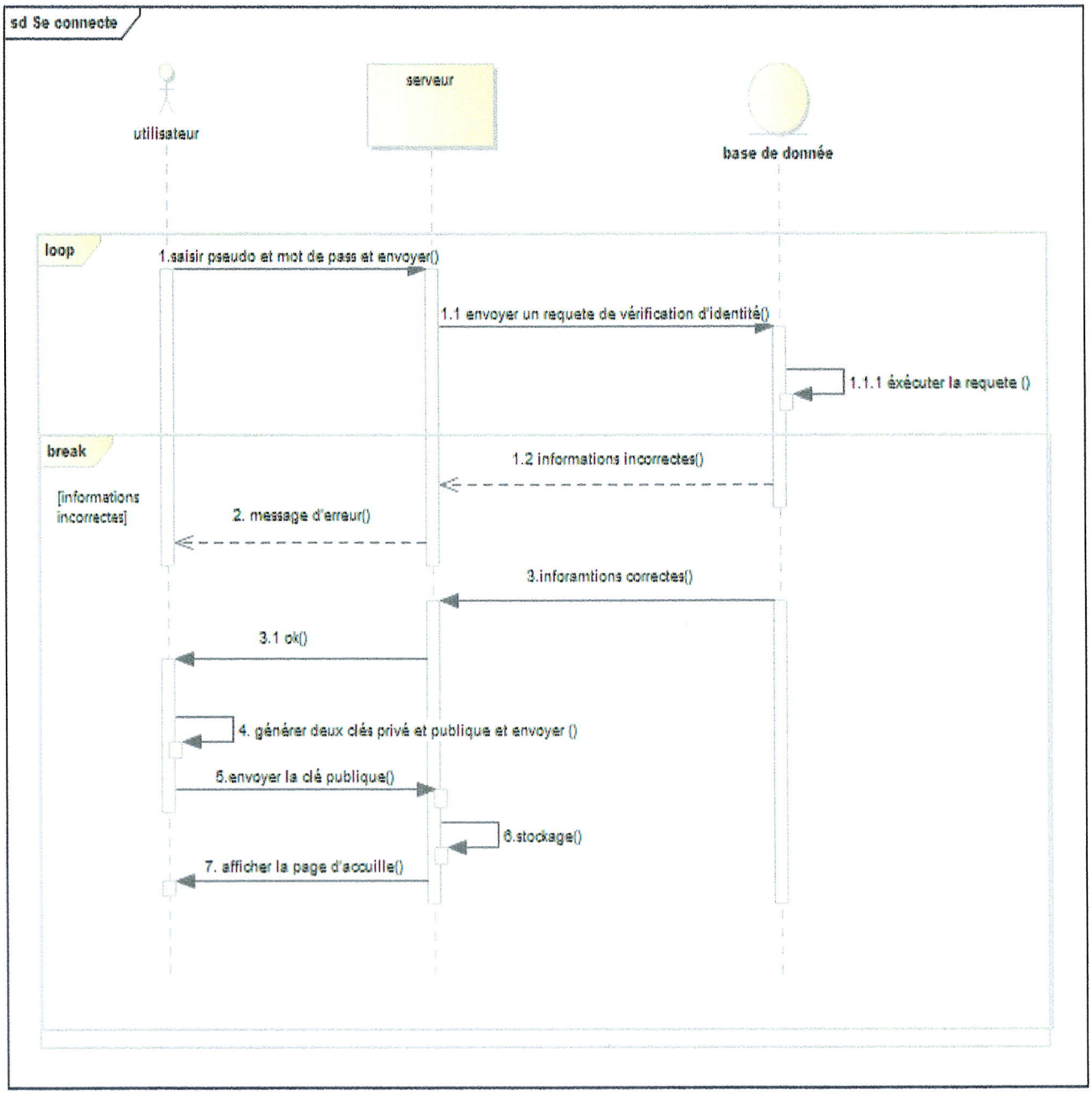


FIGURE 5.6 – Diagramme de séquence du cas d'utilisation "*seconnecté*"

2.3.3 Envoyer des messages

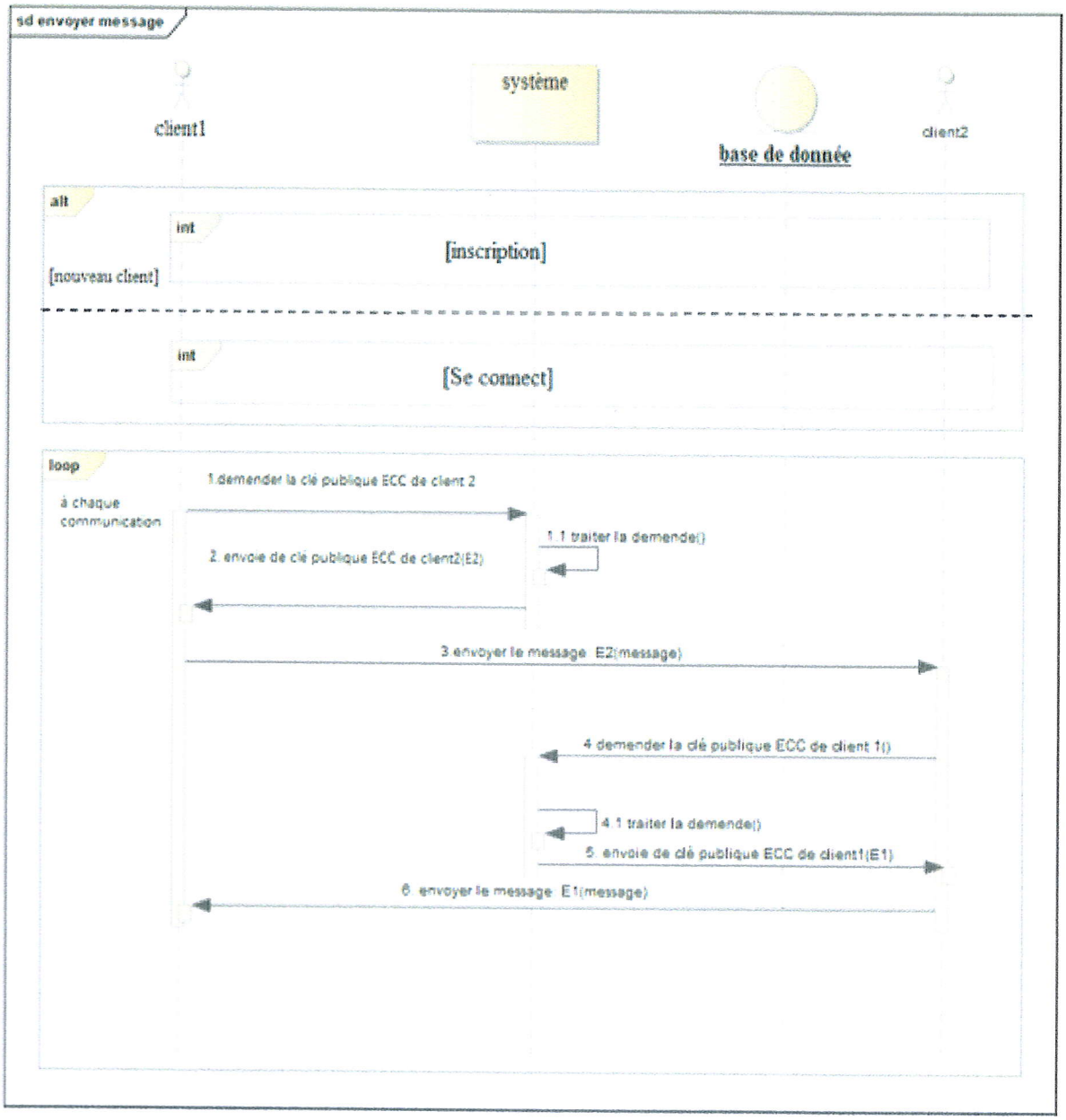


FIGURE 5.7 – Diagramme de séquence du cas d'utilisation "*envoyerdesmessages*".

5.2.5 Diagramme d'activité

Pour comprendre le processus d'envoyer un message chiffrer avec ECC ,nous allons utiliser le diagramme d'activité suivant :

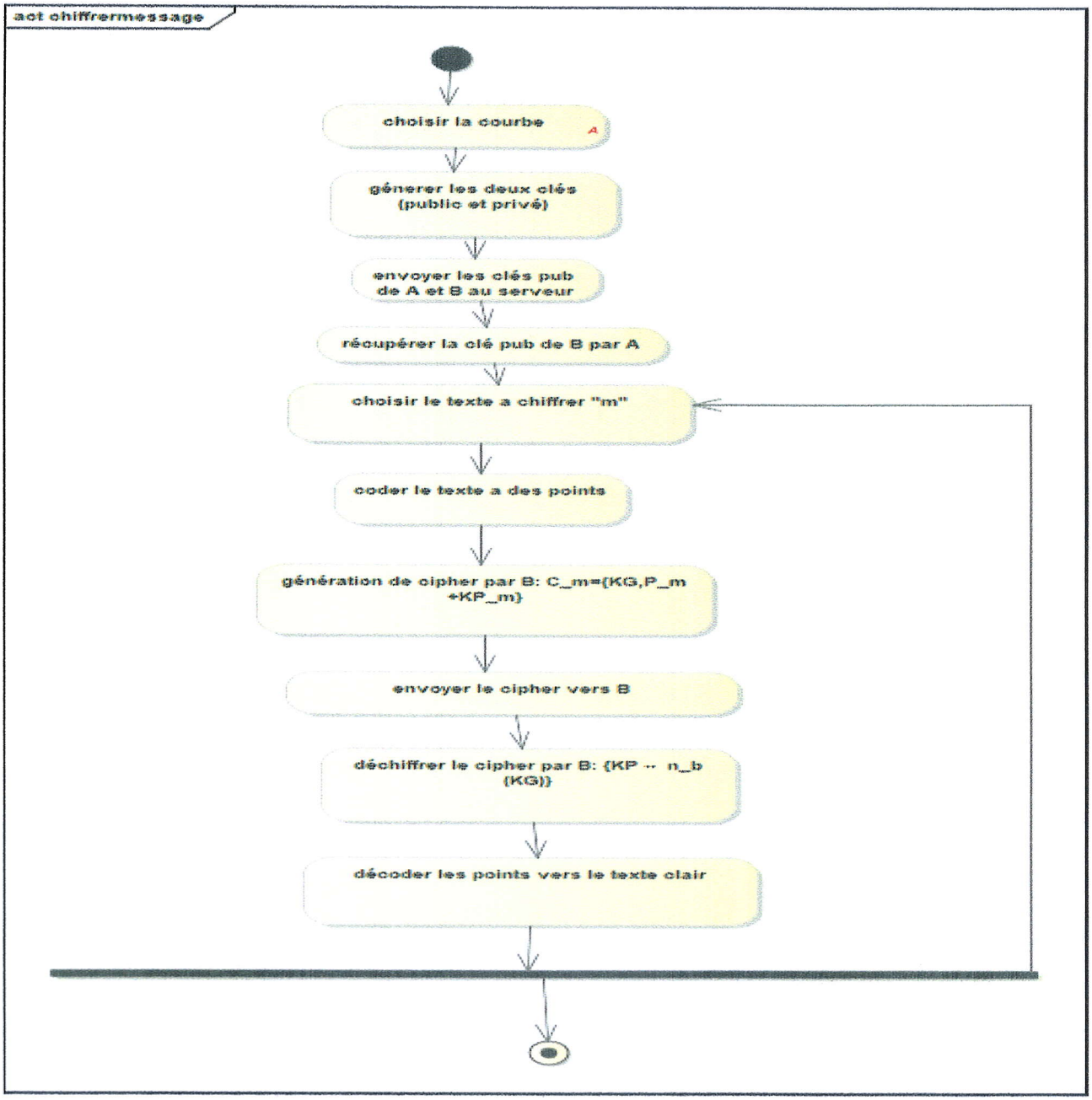


FIGURE 5.8 – Diagramme d'activité d'envoi d'un message chiffré

5.2.6 Encodage des messages

Comme indiqué dans le diagramme précédent Il faudra ici encoder le texte clair(m) comme un point (P_m) de coordonnées x et y . C'est ce point qui sera chiffré. Il faut aussi rendre publique un point G.

Dans notre application nous allons utiliser les paramètres suivants :

-comme exemple nous avons prendre la courbe de NIST sur le corps premier 160-P.

— la courbe :$y^2 = x^3 + ax + b(modp)$ telque :

a=FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC.

b= 1632357913061681105466049194032715795305483454l3.

p=1461501637330902918203684832716283019653785059327.

— le point générateur G :

G_x= 425826231723888350446541592701409065913635568770.

G_Y= 203520114162904107873991457957346892027982641970.

chaque caractère est équivalent à un point sur la courbe,comme suit :

a=G , b=2G , c= 3G , d=4G ...,0=28G ,1=29G ,2=30G , 3=31G ...etc.

les résultats obtenus est une table de correspondance utilisé pour les deux opérations : codage et décodage.

5.3 Implémentation

5.3.1 Environnement et outils de développement

Avant de commencer l'implémentation de notre application ,nous allons tout d'abord citer les outils utilisées lors le développement.

Langage java

C'est un langage de programmation orienté objet, développé par Sun Microsystems. Il possède de nombreuses caractéristiques qui font de lui un langage de choix , cette langage permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris),java est également portable, rapide, sécurisé et fiable [50].

JDK (JAVA Developement Kit)

L'environnement dans lequel le code JAVA est compilé pour être transformé en bytecode (code intermédiaire) afin que la machine virtuelle de JAVA (JAVA Virtual Machine) puisse l'interpréter[51].

Netbeans IDE

NetBeans est un environnement de développement intégré (EDI), placé en « open source » par Sun en juin 2000 sous licence CDDL et GPLv2 (Common Développent and Distribution License). En plus de Java, il permet également de supporter différents autres langages, comme Python, C, C++, JavaScript, XML, Ruby, PHP et HTML.

Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, éditeur graphique d'interfaces et de pages Web). NetBeans constitue par ailleurs une plate forme qui permet le développement d'applications spécifiques « bibliothèque Swing (Java) »[52].

SQLiteManager

pour crées nos base de données ,nous avons utilisé SQLite Manager.

SQLite Manager est un puissant système de gestion de base de données pour les bases de données sqlite. Il associe une interface conviviale à une vitesse fulgurante et des fonctionnalités avancées.

SQLiteManager vous permet de travailler avec une large gamme de bases de données SQLite3 :bases de données standard , bases de données en mémoire,bases de données cryptées AES 128/256 / RC4 ,base de données cryptée SQLCipher et également avec le serveur cubeSQL[53].

Le modèle client/serveur

Sockets TCP

Le protocole TCP offre un service en mode connecté et fiable. Les données sont délivrées dans l'ordre de leur émission.

La procédure d'établissement de connexion est dissymétrique. Un processus, appelé serveur, attend des demandes de connexion qu'un processus, appelé client, lui envoie. Une fois l'étape d'établissement de connexion effectuée le fonctionnement redevient symétrique.

Il est à noter que côté serveur on utilise deux sockets : l'un, appelé socket d'écoute, reçoit les demandes de connexion et l'autre, appelé socket de service, sert pour la communication. En effet, un serveur peut être connecté simultanément avec plusieurs clients.

5.3.2 Présentation des interfaces de l'application

1.Interface serveur

Permet de l'ouverture d'une connexion, ainsi que répondre aux requêtes envoyées par les clients.

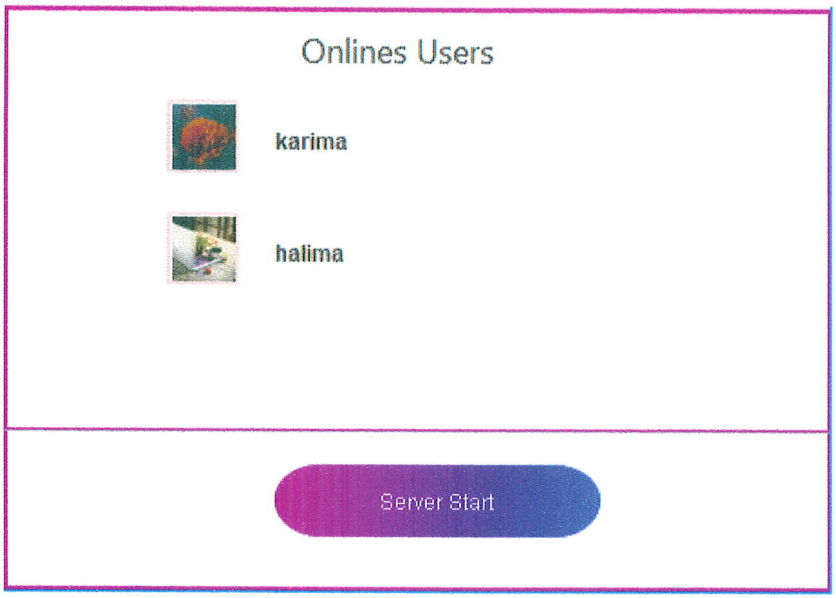
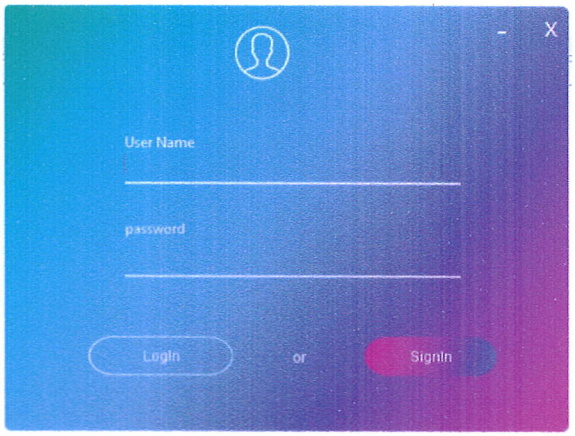


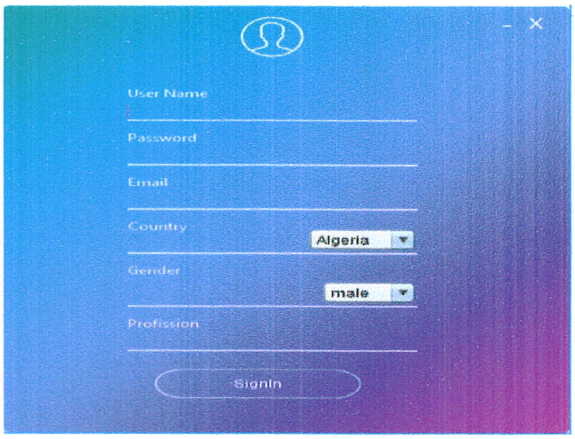
FIGURE 5.9 – Interface serveur.

2.Inscription et authentification

Permet au client de s'inscrire ou se connecter avant de commencer la discussion avec un autre client(ami).



(a) Authentification



(b) Inscription

3.Page d'accueille :

-Représente les information d'un utilisateur (username,la location ect..)

-Elle permet aux utilisateur d'accéder aux discussion,envoyer une invitation ,voir des notification ,configurer l'application(choisi la courbe préféré) et peut aussi de se déconnecter.

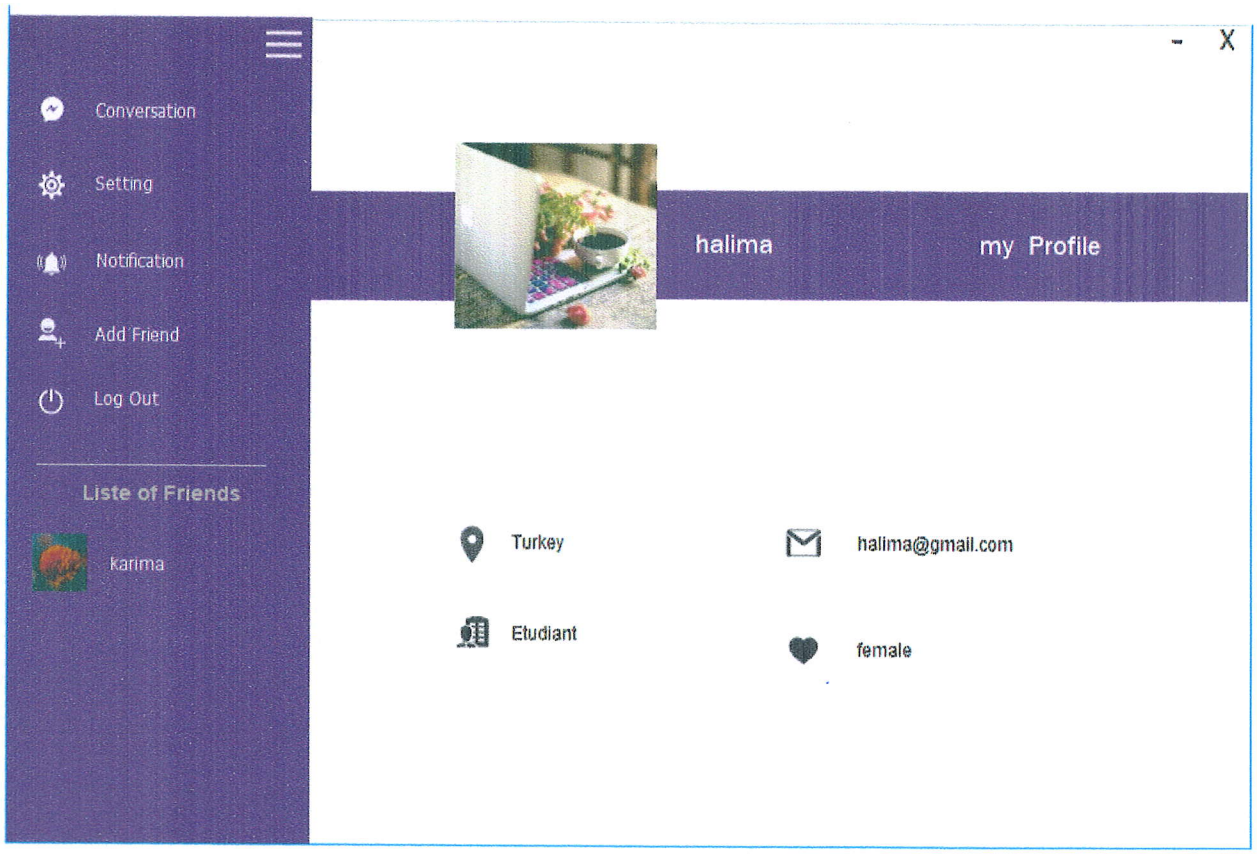


FIGURE 5.10 – Page d'accueille.

4.Discussion

après l'authentification :

- Le client peut échanger des messages ou des pièces joints avec un autre client .

Avant d'envoyer le message , le client doit :

1. Générer deux clés :une clé privé garder chez lui et une clé publique envoyer aux serveur(publication).

2.Choisir un ami et demander leur clé publique.

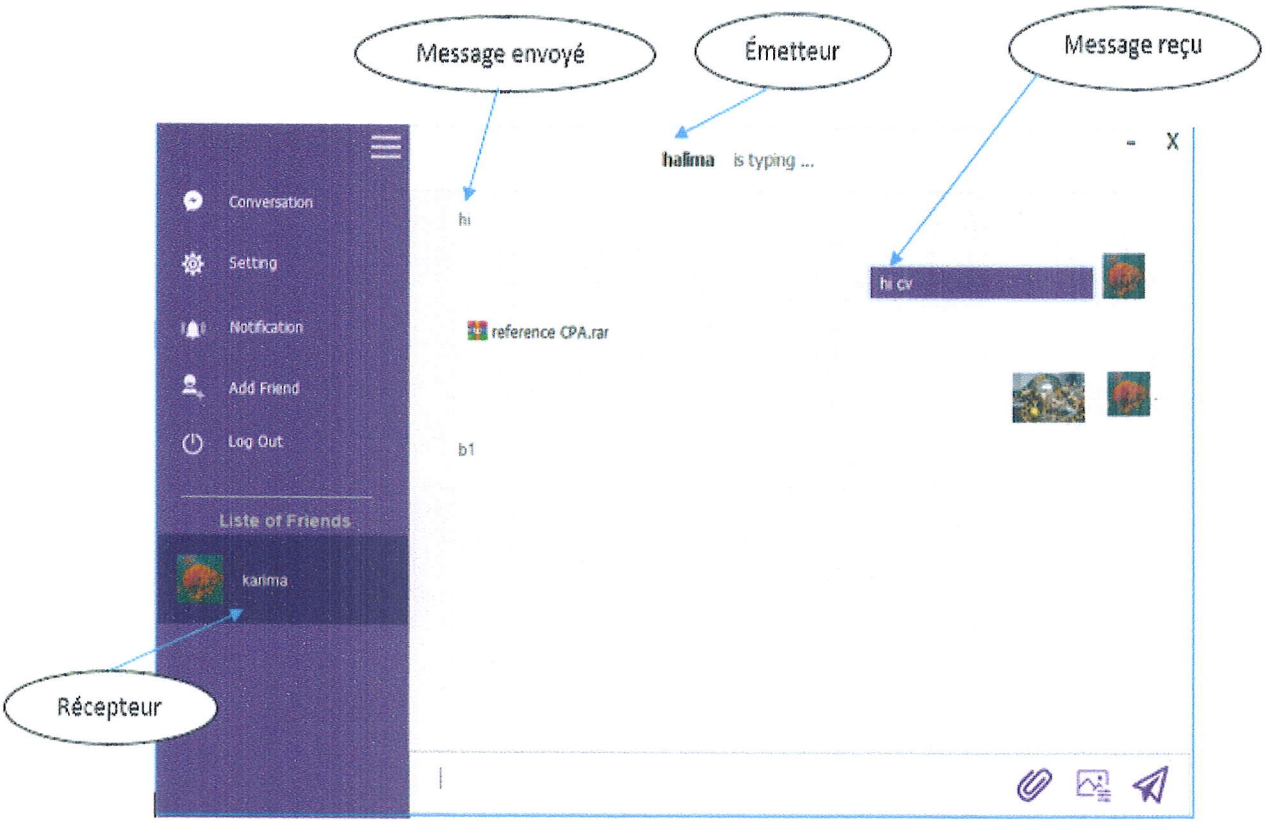


FIGURE 5.11 – Fenêtre de discussion.

-La discussion est fait par la courbe de NIST p-160 par défaut, mais l'application offre la possibilité de choisir un autre type parmi les 5 types de NIST Suivant :

— Courbe P-160
— Courbe P-224
— Courbe P-256
— Courbe P-384
— Courbe P-521

-si le client choisi un autre type de courbe ,l'application envoyer une notification a tout leur amis pour les informer

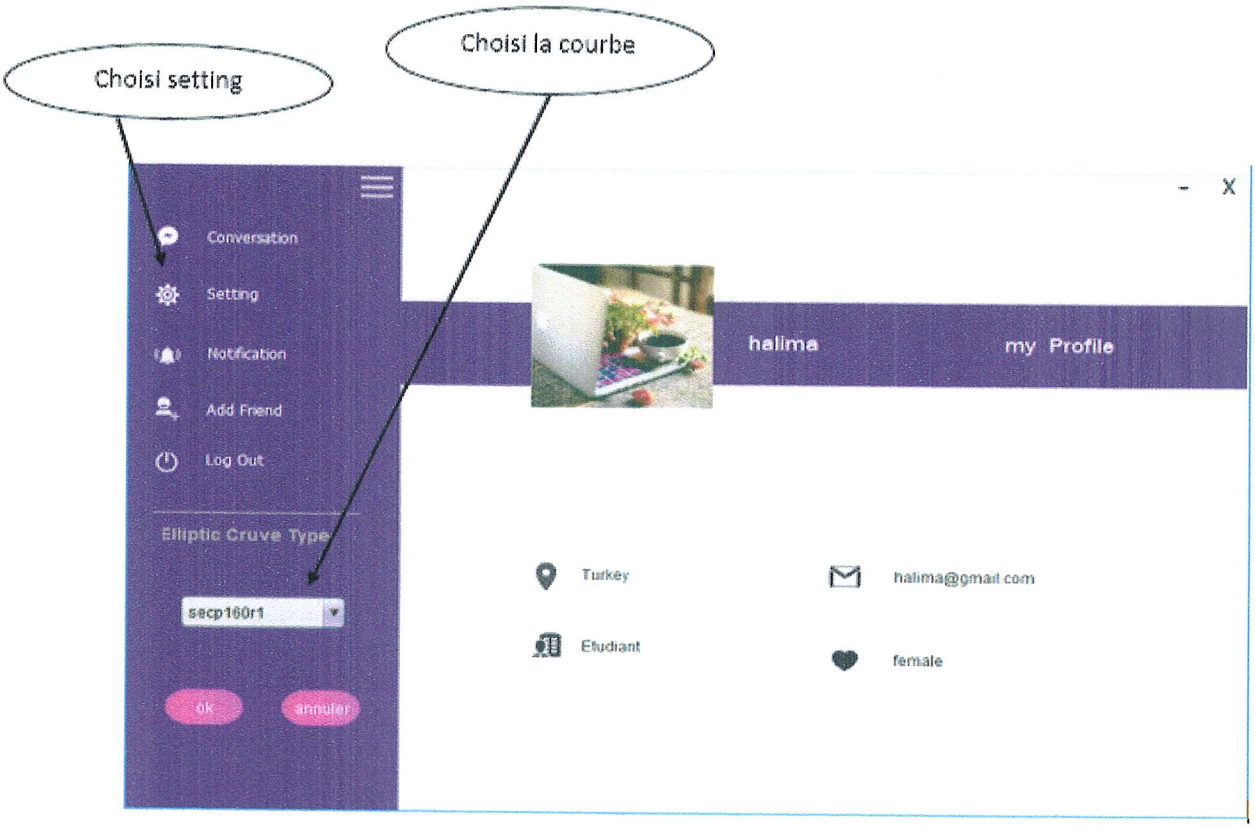


FIGURE 5.12 – Fenêtre de configuration.

4.Interface des informations

Cette interface permet aux récepteur de connaitre les détailles du message reçu lorsque il cliquer sur le message comme :

-Le nom de l'émetteur.

-La courbe et le point générateur utilisé.

-La clé publique de chiffrement qui représente un point .

-La clé privé de déchiffrement .

-Message codé.

-message chiffré.

FIGURE 5.13 – Informations du message reçu.

5.4 Conclusion

Au cours de ce chapitre, nous avons présenter une implémentation d'un mini chat et les différentes phases de la réalisation de ce dernier. Nous commençons par une conception générale a travers une modélisation UML.Ensuite nous avons recenser les différents technologies logiciels utilisées pour le développement.

Et enfin, nous avons exposer certains imprimes écrans qui illustré les différents facettes de notre application.

Conclusion générale

Le travail réalisé dans le cadre de notre mémoire s'intéresse aux problématiques liées à la sécurité des données sensibles sur les dispositifs mobiles qui ont fait l'objet de recherches ces dernières années utilisant la cryptographie basé sur les courbes elliptiques.

Pour cela nous avons proposé un modèle de chiffrement basé sur les courbes elliptiques qui fournit une amélioration de niveau de sécurité au sein d'un terminale mobile et prend en compte les caractéristiques de ce dernier . Ce modèle permette les applications de choisir le niveau de sécurité le plus approprié en termes de capacité de ce périphérique et d'autre part l'importance de la sécurité pour chaque application.

Les méthodes de chiffrement proposées dans notre modèle sont basés sur la technique de cryptographie à base des courbes elliptiques, ce qui présente l'un des points forts de ce modèle. Le cryptosystème ECC a l'avantage d'offrir des tailles des clés les plus petites comparé aux autres cryptosystèmes asymétrique traditionnels comme RSA, mais avec le même niveau de sécurité. Cette caractéristique rend le crypto système ECC plus attractif sur les dispositifs mobiles sans fil contraints en ressources.Ainsi nous avons implémenter comme un cas d'application un minichat afin d' implémenter une des méthodes de chiffrement proposé par notre modèle, c'est la méthode ECC, pour un niveau bas de sécurité .

Comme perspectives de notre travail, nous prévoyons de vous orientez vers une combinaison de ECC avec une méthode de chiffrement symétrique **AES** pour élever le niveau de sécurité ,et pour une sécurité plus fort nous proposons de combiner une méthode de masquage avec les deux méthodes (AES et ECC) .

Bibliographie

[1] C.Linda. *Localisation des mobiles pour une stratégie de prédiction.* PhD thesis, Université de M'hmed Bougara-Boumerdes ;thése de doctorat, 2010-2011.

[2] B.Lydia et T.Ibtissam. Développement des méthodes de sécurité des réseaux mobiles. Master's thesis, Université A/Mira de Béjaïa, 2014-2015.

[3] B.Amina. *Plateforme Basée Agents Pour l'Aide à la Conception et la Simulation des Réseaux de Capteurs Sans Fil.* PhD thesis, Université 20 AOUT 55 de SKIKDA ;thése de doctorat, 2009-2010.

[4] B.Samira et D.Zahira. Conception des réseaux sans fils ieee 802.11 en modes infrastructure et adhoc. Master's thesis, UNIVERSITÉ ABOU BEKR BELKAID TLEMCEN, 2015-2016.

[5] Ch.Omar. *Sécurité des réseaux ad hoc.* PhD thesis, l'Ecole Nationale d'Ingénieurs de Sfax ;thése de doctorat, 2005.

[6] F.Mohamed Amine. *La sécurisation des réseaux sociaux mobiles.* PhD thesis, Université BADJI MOKHTAR-ANNABA ;thése de doctorat, 2013-2014.

[7] B.Wafa. *Sécurisation des données sensibles sur téléphone mobile / dispositif d'assistant numérique personnel (PDA).* PhD thesis, Université Abderrahmane Mira de Béjaïa ;thése de doctorat, 2007-2008.

[8] Mr B.Abdesselem. *De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc.* PhD thesis, Université de L'Hadj Lakhdar-Batna ;thése de doctorat, 2008-2009.

[9] L.Bloch et Ch.Wolfhugel. *Sécurité informatique.* 2e édition edition, 2009.

[10] B.Mouchira. *Sécurité des échanges dans un réseau de noeuds mobiles.* PhD thesis, Université de L'Hadj Lakhdar-Batna ;thése de doctorat, 2008-2009.

[11] S.Nicolas. Sécurité dans les smartphones. Technical report, 2006-2007.

[12] Melle RABEHI Fatima. *mémoire de magister en informatique.* PhD thesis.

[13] CH.Noureddine. *La sécurité des communications dans les réseaux VANET.* PhD thesis, Université ELhadj Lakhder -BATNA ;thése de doctorat, 2008.

[14] Dr.N.Meskaoui Pr.N.WAKIM Ing.Franjieh EL KHOURY, Pr.M.EGEA. une approche ,technique biométrique/agent, pour la sécurité des réseaux informatiques.

[15] M.Jadliwala I.Bilogrevic and J.Hubaux. Security issues in next generation mobile networks : Lte and femtocells.

[16] Y.Venkataramani S.A.Arunmozhi. Ddos attack and defense scheme in wireless ad hoc networks.

[17] S.Nawal. *Conception et réalisation d'un systéme collaboratif pour les experts métier à base d'agents et des algorithmes de cryptage.* PhD thesis, Université d'Oran ;thése de doctorat, 2017.

[18] R.Dumont. *Cryptographie et Sécurité informatique.* (2009 - 2010).

[19] Antoine Wurcker. *Etude de la sécurité d'algorithmes de cryptographie embarquée vis-à-vis des attaques par analyse de la consommation de courant.* PhD thesis, Université de Limoges ;thése de doctorat, 2015.

[20] Daniel Barsky and Ghislain Dartois. *Cryptographie Paris 13.* 2010.

[21] B.MOHAMED KAMAL. *Approche Cryptographique basé sur les algorithmes génétique pour la sécurité des réseaux adHoc.* PhD thesis, Université d'Oran ;thése de doctorat.

[22] H.NOURA. *Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants.* PhD thesis, Université Nantes Angers Le Mans ;thése de doctora, 2012.

[23] Pierre-Louis Cayrel. *Chiffrement par blocs.*

[24] K.Zakaria. *mise en ouvre de nouvelles techniques pour la sécurité informatique bases sur les algorithmes evolutionnistes et les fonctions de hachage.* PhD thesis, Université de MOHAMMED V ;thése de doctorat, 2014.

[25] S.JULIA. *Techniques De Cryptographie.* (2003-2004).

[26] R.Tripathi and S.Agrawal. Comparative study of symmetric and asymmetric cryptography techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, 2014, `https://pdfs.semanticscholar.org/e0e4/810c5276f9c05cc82425fcf911f206c52bef.pdf`.

[27] Mehdi Tibouchi. *Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA.* PhD thesis, l'Université Paris Diderot et de l'Université du Luxembourg ;thése de doctorat, 2011.

[28] C. SCHRYVE and L.GAJNY. *Cryptographie à clef publique.* 2010.

[29] S.KHALI. *Développement D'une Technique de Distribution de Clés de cryptage pour les applications multicast sur les réseaux sans fil ad hoc.* PhD thesis, Université Du Québec ;thése de doctorat, 2008.

[30] S.Jacob. *Protection cryptographique des bases de données : conception et cryptanalyse.* PhD thesis, l'université Pierre et Marie Curie ;thése de doctorat, 2012.

[31] Philip R. Zimmermann. Pretty good privacy (pgp). 1991,`http://philzimmermann.com/FR/background/index.html`.

[32] G.Assche. *Quantum cryptography and secret key distillation.* Cambridge University Press, 2006.

[33] Y.SHOU. *Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs.* PhD thesis, Université de Franche-Comté ;thése de doctorat, 2014.

[34] B.Hichem. *Sur la sécurité de l'information par le biais des courbes elliptiques.* PhD thesis, Université Djillali Liabes Faculté Des Sciences exactes ,Sidi Bel Abbés ;thése de doctorat, 2018.

[35] S.Pontié. *Sécurisation matérielle pour la cryptographie à base de courbes elliptiques.* PhD thesis, Université Grenoble Alpes ;thése de doctorat, 2016.

[36] G.Seroussi I.Blake, G.Seroussi and N Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.

[37] V. Gayoso Martinez et C. Sanchez Avila J. Espinosa Garcia, L. Hernandez Encinas. Elliptic curve cryptography :java implementation issues. 2005.

[38] Vincent Verneuil. Courbes elliptiques et attaques par cannaux auxiliaires. *Science et Technologie*, 2009.

[39] A.Singh et R.Singh. Various attacks over the elliptic curve-based cryptosystems. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2015.

[40] Randimbindrainibe F.et Razakarivony J.3 Rakotondraina T.E. Performances des cryptosystèmes basés sur les courbes elliptiques. *MADA-ETI, ISSN 2220-0673, Vol.2*, 2010.

[41] I.Lotfi. *Cryptographie à base de courbes elliptiques.* PhD thesis, Ecole Nationale Supérieure d'Informatique ;thése de doctorat, 2017.

[42] C.GONÇALVES. *Cryptographie Avancée Courbes elliptiques.* 2015.

[43] P.G.Rajeswari et K.Thilagavathi. An efficient authentication protocol based on an elliptic curve cryptography for mobile networks. 2009.

[44] Dan Zhou et Shusheng Peng Feng Xu, Xuan Zhou. Application of elliptic curve cryptography in zigbee wireless sensor network. 2013.

[45] Wenbo Shi et Peng Gong. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. 2013.

[46] Josyula R. Raoet Berk Sunar. *Cryptographic Hardware and Embedded Systems-CHES 2005.* 2005.

[47] M.BOUDIA et O.Rafik. *agrégation des donnees et sécurité des reseaux de capteurs sans fil.* PhD thesis, Université De Tlemcen ;thése de doctorat, 2014.

[48] J.Francq. *Conception et sécurisation d'unités arithmétiques hautes performances pour courbes elliptiques.* PhD thesis, université Montpellier ;thése de doctorat, 2009.

[49] https ://www.secg.org/SEC2-Ver-1.0.pdf.

[50] P.Crescenzo. *OFL :un modèle pour paramétrerla sémantique opérationnelle des langages à objets application aux relations inter-classes.* PhD thesis, l'Université de Nice-Sophia Antipolis ;thése de doctorat, 2001.

[51] Http ://www.oracle.com/technetwork/java/javase/tech/index.html.

[52] https ://www.techno-science.net/definition/5346.html.

[53] https ://sqlabs.com/sqlitemanager.