Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études
Pour l'obtention du diplôme de Master en Informatique

Option: *Modèle Intelligent et Décision(M.I.D)*

Thème

Cryptographie symétrique des messages dans un réseau P2P

Réalisé par :

DJEZZAR Fatima Zahra **BRIKCI SID Fatima Zahra**

Présenté le 19/12/ 2017 devant les jury composé de:

- **Mr Bekara Chakib** **Président**
- **Mme Amraoui Asma** **Examinateur**
- **Mr Belhocine Amine** **Encadrant**

Année Universitaire: 2016-2017

« Louange à Allah qui nous a guidés à ceci. Nous n'aurions pas été guidés, si Allah ne nous avait pas guidés »

[Sourate 7. Al Araf verset 43]

Remerciements

Nous remercions ALLAH de nous avoir données la santé et lecourage afin de pouvoir réussir ce travail.
Ce travail est l'aboutissement d'un long cheminement au coursduquel nous avons bénéficié l'encadrement, des encouragementset du soutien de plusieurs personnes, à qui nous tenons à dire profondément et sincèrement merci.

Dédicaces

Je dédie ce travail à mes estimables parents dont aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours eu pour vous.

Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être.

Ce travail est le fruit de vos sacrifices que vous avez consentis pour mon éducation et ma formation. Mais aussi à mon frère "AbdeNnasser" et mes soeurs "Narimane" et "Djihan" ma grand-mère et mes oncles"Mohamed" et "Khalifa" à et spécialement "Dine Houari" en témoignage de l'attachement, de l'amour et l'affection que je porte pour toi, vous êtes toujours dans mon coeur. Ainsi que toute ma famille.

À tous ceux qui de près ou de loin m'ont soutenu de façon directe ou indirecte.

À la promotion MID 2016/2017, à toutes les communautés bissau-guinéennes, et aussi toutes les communautés étrangères du Tlemcen, à mes professeurs, et tous mes amis et connaissance proche.

Djezzar Fatima zahra

Dédicaces

Je dédie ce Modeste Travail a :

A Mes Parents « sid Ahmed &CherietOuahiba », Aucun hommage ne pourrait êtrea la hauteur de l'amour Dont ils ne Cessent de me combler .Que dieu leur procure bonne santé et longue vie Je Vous Aimes Beaucoup .

A l'âme de mon grand-père Cheriet Mohamed.

A ma grande mère Cherifa, Mon FrèreAzou ,MesChéresHayet ,Chahra, Tonton Zohir , Mais Petits Rihame,yasser, Hani .& Tout Mes Tantes & Oncles Brikçi

Un Grand Merci A Ma Binôme Djezzar Fatima Zahra ,Je Remercie aussi Mr Belhocine Amine & Mais Cher Sœurs

De cœur « Tema, Theldja ,Djazia,

Meriem,Radia,Safaa,Aicha ,Yasmina , Amel , Sara» & Ibrahim Qui Ma trop Aide &touts Le Membre Du groupe Mid&Mais Amies &Aux Membre de Jury & Toute L'équipes De Société zaatcha .

À tous ceux qui de près ou de loin m'ont soutenu de façon directe ou indirecte.

Merci Beaucoup A tous

Brikçi Sid Fatima Zahra

Table des matières

Table des Figures

Liste des tableaux

Introduction générale

Le besoin de dissimuler les informations préoccupe l'homme depuis le début de la civilisation La confidentialité apparait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle se développe énormément à des fins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre deux interlocuteurs ou plusieurs, via un vecteur d'information comme les réseaux de télécommunications actuels et futurs. Ainsi, les banques utilisent ces réseaux pour assurer la confidentialité des opérations avec leurs clients ; les laboratoires de recherche s'en servent pour échanger des informations dans le cadre d'un projet d'étude commun ; les chefs militaires pour donner leurs ordres de bataille, etc. De nos jours, la nécessité de cacher ou de casser une information rentre dans un vaste ensemble appelé cryptographie.

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une actionspécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffré.

La cryptographie est l'art du secret à celle de la piraterie, sert non seulement à préserver laConfidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

L'objectif principal de notre projet de fin d'étude, est de développer une application qui va chiffrer des messages et qui assuré la confidentialité.

Ce rapport est organisé en trois chapitres. Chaque chapitre aborde des points spécifiques. Il est structuré comme suit :

Le premier chapitre présente une introduction aux réseaux peer-to-peer, et les différents concepts liés à ces réseaux ainsi que les différents algorithmes mis en oeuvre dans différents types architectures. Le deuxième chapitre expose les concepts fondamentaux de la cryptographie moderne comme ils sont définis par les standards internationaux de la sécurité. Dans le dernier chapitre, on présente notre application avec ses différents étapes de fonctionnement et les outils utilisés pour la réalisation. Enfin, nous terminons le mémoire par une conclusion générale dans laquelle nous résumons l’essentiel de notre travail.

Chapitre 1 : Le réseau Peer to Peer

Introduction

En 1969, l'ARPA met au point les premiers réseaux mondial : ARPANET. Suite à diverses modifications dans les années 70 et 80, ce réseau devient le réseau INTERNET au début des années 90.

Aujourd'hui, ce réseau mondial fonctionne intégralement sur le concept de client-serveur mais fin 1998, Shawn fanning un étudiant américain passionné informatique alors âgé 19 ans vient bouleverser le monde bien établi du client-serveur. Il décide de quitter L'université et se lance dans l'écriture d'un logiciel permettant l'échange de fichiers musicaux. En septembre 2000, Napster atteint un nombre de téléchargement record, c'est à partir de ce moment que l'architecture Peer to Peers'estdémocratisée et que des logiciels utilisant cette architecture commencent à émerger.

L'architecture Peer to Peer (P2P), que l'on traduit généralement par réseau de "poste à poste", "pair à pair" ou encore "d'égal à égal" désigne une architecture de réseau où les postes connectés communiquent directement entre eux et partagent leurs ressources. Tous les postes ont un rôle équivalent, à la fois client et serveur par rapport à ces ressources (espace de stockage, puissance de calcul...), d'où leur appellation de "servent" (contraction de serveur et client). C'est la mise en commun de ces ressources qui fait la force et le succès de ces réseaux.

1. Définition d'un système distribué

Un système distribué est un système disposant d'un ensemble d'entités communicantes, installées sur une architecture d'ordinateurs indépendants reliés par un réseau de communication, dans le but de résoudre en coopération une fonctionnalité applicative commune. [1]

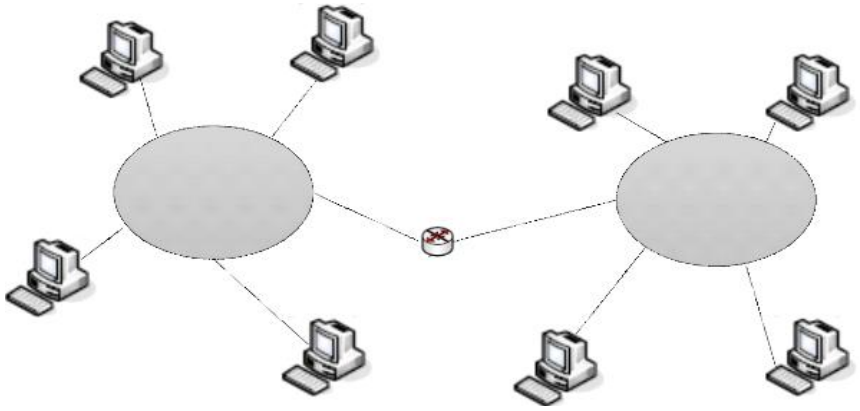

Figure 1.1: Représentation d'un système distribué

1.1 Intérêt des systèmes distribués

Les systèmes distribués ont plusieurs raisons de leur existence.

- Partage des ressources (données, programme, services) qui permet un travail collaboratif.
- Accès distant, c'est-à-dire qu'un même service peut être utilisé par plusieurs acteurs situés à des endroits différents.
- Amélioration des performances : la mise en commun de plusieurs unités de calcul permet d'effectuer des calculs parallélisa blés en des temps plus courts.
- Confidentialité : les données brutes ne sont pas disponibles partout au même moment, seules certaines vues sont exportées.
- Disponibilité des données en raison de l'existence de plusieurs copies.
- Maintien d'une vision unique de la base de données malgré la distribution.
- Réalisation des systèmes à grande capacité d'évolution.
- Augmentation de la fiabilité grâce à la duplication de machines ou de données, ce qui induit à une réalisation des systèmes à haute disponibilité.

2. Définition P2P

Peer-to-Peer (P2P) est un modèle de communication décentralisé dans lequel chaque partie a les mêmes capacités et l'une ou l'autre partie peut lancer une session de communication. Contrairement au modèle client / serveur, dans lequel le client effectue une demande de service et le serveur satisfait la demande, le modèle de réseau P2P permet à chaque nœud de fonctionner à la fois comme client et serveur.

Les systèmes P2P peuvent être utilisés pour fournir un routage anonyme du trafic réseau, des environnements informatiques parallèles, du stockage distribué et d'autres fonctions. La plupart des programmes P2P sont axés sur le partage de médias et P2P est donc souvent associé au piratage de logiciels et aux violations des droits d'auteur.

En règle générale, les applications Peer-to-Peer permettent aux utilisateurs de contrôler de nombreux paramètres de fonctionnement: combien de connexions membres de rechercher ou de permettre en même temps; À quels systèmes se connecter ou éviter; Quels services proposer; Et le nombre de ressources système à consacrer au réseau. Certains se connectent simplement à un sous-ensemble de nœuds actifs dans le réseau avec peu de contrôle de l'utilisateur, cependant. Bien que les utilisations des topologies de réseau P2P aient été explorées depuis les jours d'ARPANET, les avantages du modèle de communication P2P ne sont pas devenus évidents pour le public jusqu'à la fin des années 1990, lorsque les applications P2P de partage de musique comme Napster sont apparues.

Napster et ses successeurs - comme Gnutella, et plus récemment, Bit Torrent - ont réduit les profits de l'industrie de la musique et du cinéma et ont changé la façon dont les gens pensaient à l'acquisition et à la consommation de médias. [2]

3. Les caractéristiques P2P

Dans cette section, nous présentons les principales caractéristiques que présente le modèle Peer-to-Peer:

Décentralisation: le fait que chaque nœud gère ses propres ressources permet d'éviter la centralisation de contrôle. Un système P2P peut fonctionner sans avoir aucun besoin d'une administration centralisée ce qui permet d'éviter les goulets d'étranglements et d'augmenter la résistance du système face aux pannes et aux défaillances.

Passage à l'échelle: il s'agit de faire coopérer un grand nombre de nœuds (jusqu'à des milliers ou des millions) pour partager leurs ressources tout en maintenant une bonne performance du système. Cela signifie qu'un système P2P doit offrir des méthodes bien adaptées avec un environnement dans lequel il y a un grand volume de données à partager, un nombre important de messages à échanger entre un grand nombre de nœuds partageant leurs ressources via un réseau largement distribué.

L'auto-organisation: puisque les systèmes P2P sont souvent déployés sur l'Internet, la participation d'un nouveau nœud à un système P2P ne nécessite pas une infrastructure couteuse. Il suffit d'avoir un point d'accès à l'Internet et de connaitre un autre nœud déjà connecté pour se connecter au système. Un système P2P doit être un environnement ouvert ; c'est-à-dire, un

utilisateur sur un nœud doit être capable de connecter son nœud au système sans avoir besoin de contacter une personne et sans avoir besoin de passer par une autorité centrale.

Autonomie des nœuds: chaque nœud gère ses ressources d'une façon autonome. Il décide quelle partie de ses données à partager. Il peut se connecter ou/et se déconnecter à n'importe quel moment. Il possède également l'autonomie de gérer sa puissance de calcul et sa capacité de stockage.

Hétérogénéité: à cause de l'autonomie de nœuds possédant des architectures matérielles et/ou logicielles hétérogènes, les systèmes P2P doivent posséder des techniques convenables pour résoudre les problèmes liés à l'hétérogénéité de ressources.

Dynamique: à cause de l'autonomie de nœuds, chaque nœud peut quitter le système à n'importe quel moment ce qui fait disparaitre ses ressources du système. De nouvelles ressources peuvent être ajoutées au système lors de la connexion de nouveaux nœuds. Alors, à cause de l'instabilité de nœuds, les systèmes P2P doivent être capables de gérer un grand nombre de ressources fortement variables. La sortie d'un nœud du système (Les réseaux pair à pairpannent d'un nœud) ne doit pas mettre le système en échec. Elle doit être tolérée et avoir un "petit" impact sur la performance de tout le système.[3]

4. Les applications Peer to Peer

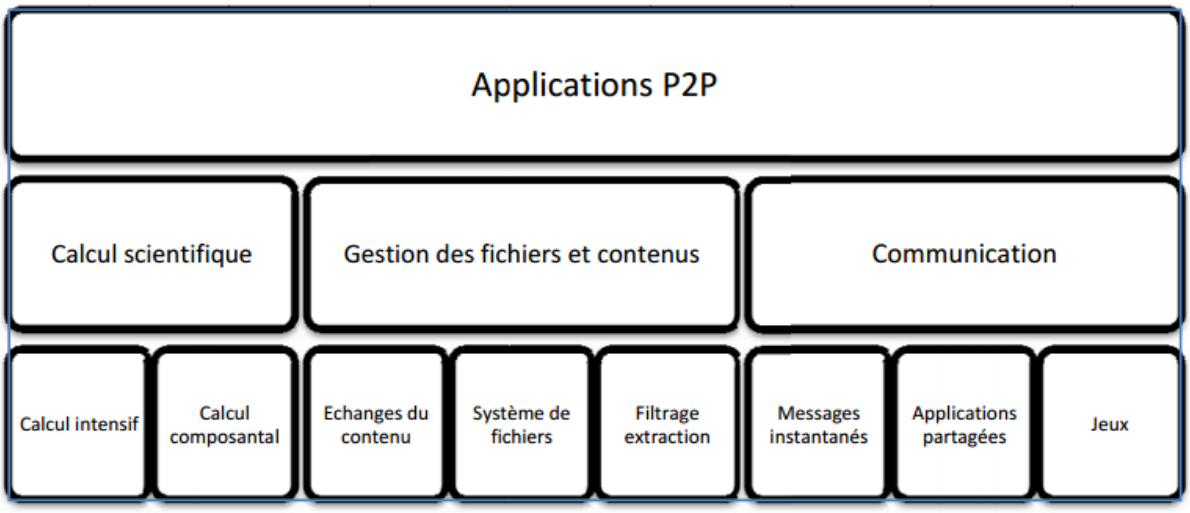

Figure1.2: Taxonomie des Applications P2P

Il existe défirent types d'application utilisant le concept du P2P : [3]

A. Communication

(P2P Chat) largement répandue grâce à la caractéristique qu'ont les pairs d'interagir directement entre eux. Les implémentations varient beaucoup.

Exemples des systèmes pairs à pair dans la messagerie instantanée

- ✓ AOL Instant Messenger,
- ✓ Yahoo! Messenger,
- ✓ MSN Messenger,
- ✓ ICQ,
- ✓ Skype, etc.

B. Applications partagées

Ce type d'applications permet à des usagers de collaborer en temps réel sans utiliser de serveur central. Ces applications permettent de travailler de manière commune sur un projet distribué en permettant le partage des idées, ressources,documents et l'emploi du temps via une communication interactive
Exemple:

- ✓ Groove,
- ✓ Magi,
- ✓ PowerPoint distribué,
- ✓ NextPage,
- ✓ Knari.

C. Les jeux en réseau

En réseau. C'est un domaine vaste pour le P2P, dont l'architecture est exempte de toute autorité centrale, ceux-ci font également partie des applications de collaboration P2P

Exemple: Doom.

D. Gestion des fichiers et contenus

Généralement utilisée pour échanger les fichiers multimédia (musique, vidéo, etc.)

Exemples:

- ✓ Napster,
- ✓ Gnutella,
- ✓ Emule,
- ✓ Kazaa,
- ✓ BitTorent, etc.

E. Les bases de données distribuées

L'idée est de sauvegarder des fichiers et des informations de manière distribuée sur le réseau (sans se limiter aux disques durs locaux).

Exemples : Mari posa, Chord, etc.

F. Le calcul scientifique

Grilles de calcul Le P2P permet de mettre en commun de nombreux ordinateurs, disposant chacun de ressources limitées. Mais en « additionnant » ces ressources, on obtient des performances théoriques considérables. Par exemple le calcul matriciel dont le but est de diviser ce gros calcul en petits calculs que l'on pourra répartir ente les pairs.

D'autres exemples:

- ✓ Chord
- ✓ Cx : Transformer votre PC en ressources globales de calcul
- ✓ Farsite : Stockage de données dans un environnement non sécurisé
- ✓ Globe : Gestion d'objets distribués
- ✓ OceanStore : Stockage massif de données
- ✓ Pastry : Une sous-couche pour les applications P2P
- ✓ XtremWeb : Calcul scientifique à travers le Web

5. Les avantages du p2p

- Les communications sont directes
- Décentralisation
- Passage à l'échelle
- La réplication, redondance des données
- Un nœud peut accéder directement à un ou plusieurs nœuds.
- Si une machine tombe en panne, cela ne remet pas en cause l'ensemble du système.
- Le réseau est faiblement couplé
- Possibilité de créer des groupes

6. Les inconvénients du p2p

- Pas de Qualité du Service (QoS)
- Les temps de localisation sont plus longs
- Recherche peut être Non Déterministe
- problèmes de sécurité
    - ✓ Virus, backdoors (spyware)
    - ✓ Distributed Denial of Service (DDoS)
    - ✓ Confidentialité, Authentification

7. L'objectifs du P2P

Différentes applications peuvent utiliser le P2P, les objectifs varient:

- Partage et réduction des coûts entre les différents peers.
- Fiabilité et passage à l'échelle, l'absence d'élément centralisé pour l'échange des données permet d'accroître la fiabilité en supprimant tout point central de panne et d'améliorer le passage à l'échelle en évitant les goulots d'étranglement.
- Agrégation des ressources et interopérabilité, en mettant en commun des ressources individuelles comme la puissance de calcul ou l'espace de stockage.
- Accroissement de l'autonomie en l'absence d'une autorité centrale, il est de la responsabilité de chacun de partager ou non des fichiers.
- Anonymat pouvant être assuré par certaines applications, en utilisant par exemple des algorithmes de routage qui rendent quasiment impossible le pistage d'une requête.[4]

8. Classification de l'architecture P2P

Centralisés et systèmes distribués, à leur tour les distribués, sont divisés en deux: le modèle client/serveur et le modèle pair à pair.

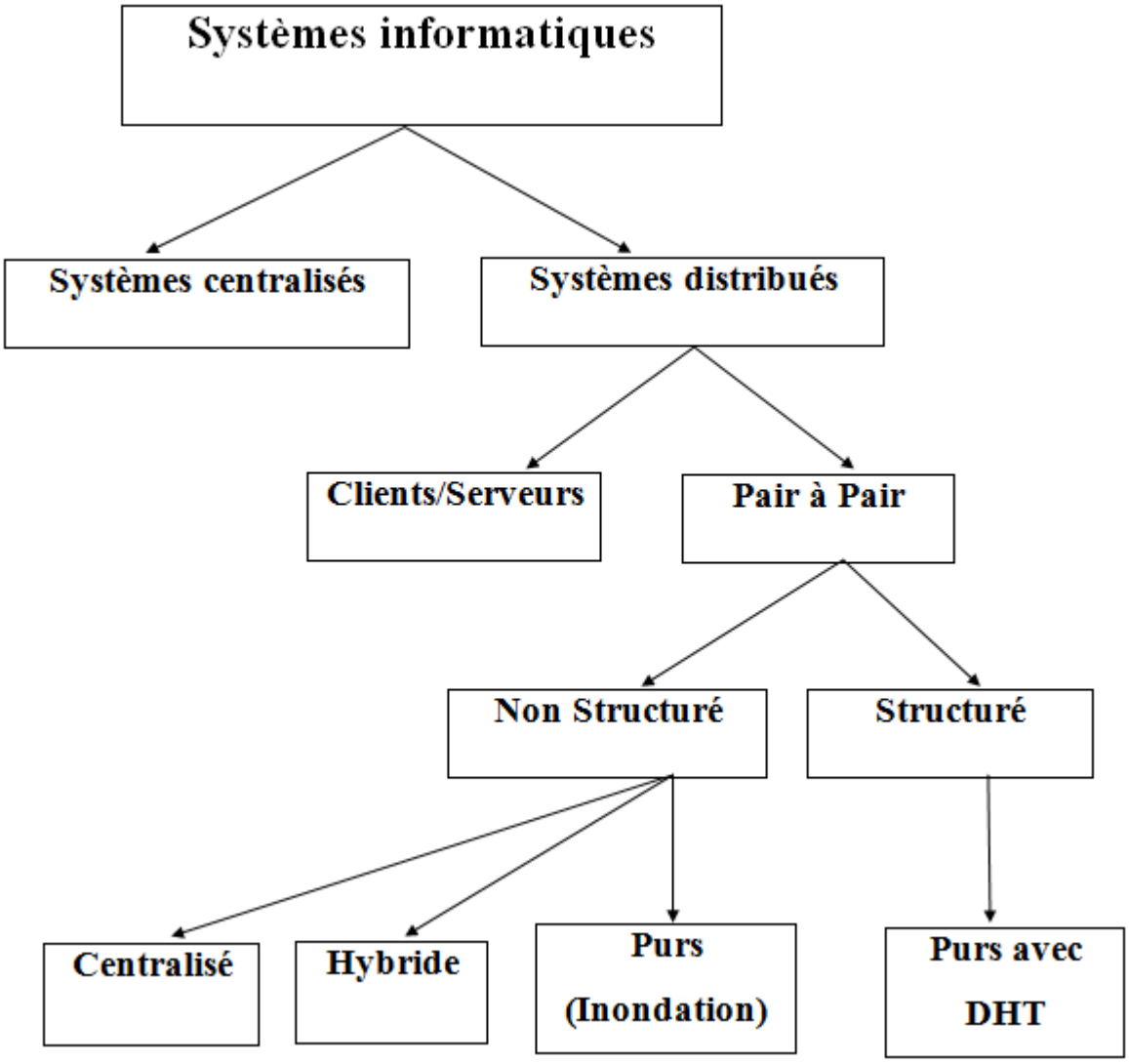

Figure 1.3: Classification des systèmes distribués

Il existe deux catégories principales de réseaux virtuels: les structurés, les non-structurés peut être soit centralisé, soit hybride ou bien pur, selon le fonctionnement de recherche du contenu.[7]

8.1 Réseaux non Structurés

Un réseau pair à pair non structuré est exclusivement basé sur les liens physiques qui relient ces nœuds ceux-ci reposent sur une construction aléatoire du graphe de connexion. Ces réseaux n'ont aucune structure logique, Un nœud joint le réseau par l'intermédiaire d'un autre nœud déjà connecté.

Les mécanismes sont simples et faciles à implémenter cependant les performances lors de la recherche d'un pair sur le réseau sont souvent limitées. Un nœud désirant localiser une ressource, demande à ses voisins s'ils connaissent cette ressource, à leurs tours, ses voisins

demandent à leurs voisins s'ils ont des connaissances de cette ressourcer et ce, jusqu'à une profondeur fixée par le système. Le nœud possédant la ressourcer renvoie une réponse qui parcourt le chemin initial dans le sens inverse.

Le réseau Gnutella est l'un des premiers réseaux non-structurés qui a mis en évidence l'abondance de communication entre pairs.

8.1.1 P2P décentralisé « purs »

Dans l'architecture p2p décentralisé, on dispense des services des serveurs en autres termes on n'a pas besoin des serveurs, tous les nœuds sont égaux et jouent le même rôle, lorsque un pair est supprimé du réseau, les services offerts ne seront pas affectés (voir figure 1.4) par contre, l'absence d'un serveur central ayant une vue globale sur la localisation des ressources hébergées par les pairs dans le réseau P2P pose le problème suivant: Comment un pair peut découvrir et accéder à une ressource dans ce contexte ? Pour cela deux solutions ont été proposées : la première basée sur la technique de l'inondation et la deuxième est basé sur les tables de hachages distribuées "DHT". Ces deux solutions sont connue sous les noms des réseaux P2P décentralisés non structurés et réseaux P2P décentralisés structurés.[6]

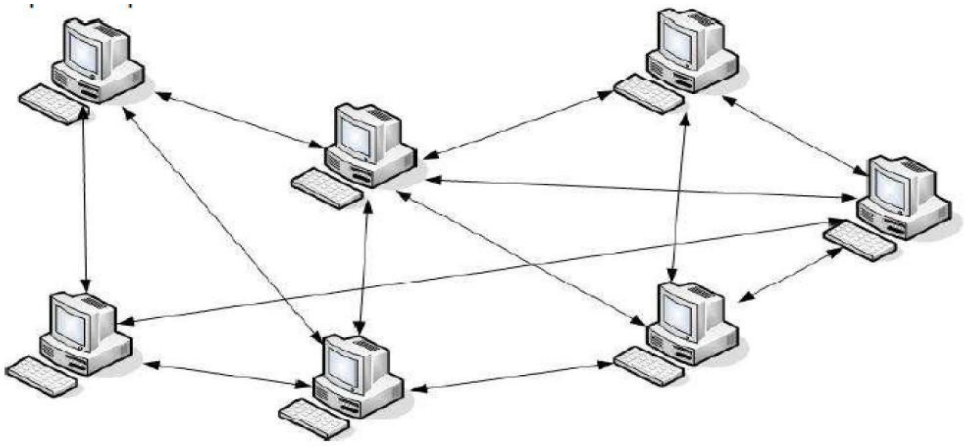

Figure 1.4: Architecture p2p décentralisé

8.1.2 Recherche par inondation

Pour découvrir une ressource, une requête sera transmise d'un pair à un autre jusqu'à atteindre le client qui partage l'objet désiré, comme ici la technique est l'inondation des messages alors on peut vite tombé dans le cas des saturation des réseaux(bande passante) car on aura trop des messages échangé entre les pairs mais aussi les messages zombies et pour remédier à ces problèmes de l'inondation du réseau et messages zombie durant un temps trop long, le système associe à chaque requête un temporisateur TTL "Time To Live".

La valeur attribuée au TTL est généralement 7. Lorsqu'il arrive à zéro, la requête n'est plus renvoyée.

Oui le temporisateur TTL a pu régler le problème de l'inondation et de le message zombie mais par contre il a créé un inconvénient majeur de ce mécanisme, que est l'expiration du TTL car si le TTL arrive à zéro certes qu'on n'aura pas des problèmes des saturations mais on ne sera pas sûr de parcourir l'intégralité du réseau, ce qui peut aboutir à l'échec d'une recherche bien que l'objet désiré soit disponible sur le réseau P2P. Ce réseau passe mal à l'échelle et génère

une surcharge du réseau par les trames de broadcasté diffusées. Cette méthode est utilisée dans le protocole Gnutella.

8.1.2.1 Gnutella

L'exemple de l'utilisation du réseau P2P décentralisé non structuré est gnutella, il est constitué d'un ensemble de pairs joignant le réseau d'après certaines règles (voir le tableau), la technique utilisé en gnutella est l'inondation alors nous avons quelques requêtes à prendre en compte exemple lors qu'un pair souhaite utilisé le réseau Gnutella. Premièrement un message Ping sera envoyé avec le but d'identifier les nœuds présents sur le réseau, on appelle ce message le message d'identification. Ce message Ping sera envoyé à ses voisins, qui l'envoient à leur tour à leurs voisins et ainsi de suite, mais au bout d'un temps ce message ne sera plus renvoyer et sera stoppée alors dans ce cas c'est tout simplement à cause du TTL qui sera à 0. Alors l'autre requête à prendre en compte est le pong qui est une réponse à un Ping alors ici c'est très simple un client que reçoit un Ping sa réponse c'est automatique il répond avec le message Pong contenant l'adresse IP, le numéro de port, le nombre et la taille des fichiers partagés. Pour chercher une ressource dans le réseau, le client envoie une requête Query en spécifiant le nom de ressource et les critères de recherche, un servent qui reçoit ce message de type Query et s'il dispose de la ressource, renvoie une réponse QueryHit au voisin qui lui a retransmis la requête, spécifiant son adresse IP et son numéro de port TCP où l'objet peut être téléchargé. La réponse remonte de proche en proche jusqu'au client initiateur. Ce dernier télécharge ensuite en envoyant directement une requête de téléchargement au pair possédant le fichier. Un message Push est utilisé si les données sont derrière un firewall. [4][5]

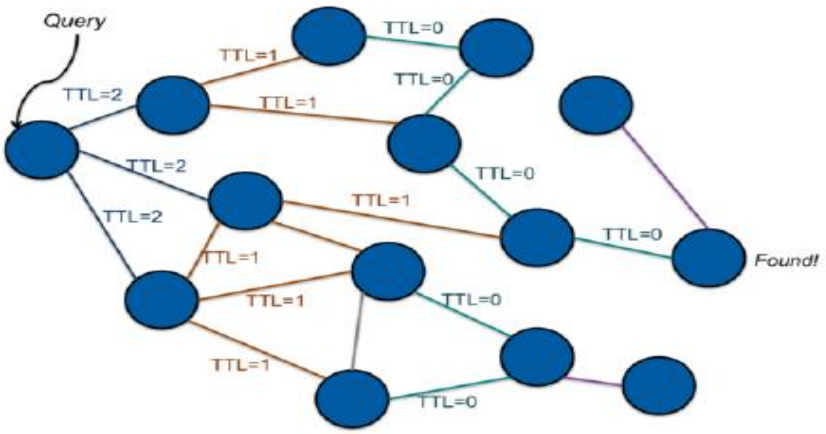

Figure1.5: Fonctionnement du Gnutella

Parmi les applications qui implémentent le protocole Gnutella, on trouve Limewire, BearShare, Gnucleos ou Phex, de plus les échanges peuvent être effectués quel que soit l'aplateforme (Windows, Linux/Unix, Macintosh, etc.) du client.

Type	Description	Information
Ping	Une requête à la recherche du pair	Vide
Pong	Réponse à un Ping	IP numéro du port nombre du fichier partagé
Query	Requête	IP numéro du port bande passante, nom du fichier
QueryHit|	Une réponse à un query si on possède le ressource	IP, numéro du port, bande passante, taille de fichier
Push	Demande de téléchargement en cas de présence d'un firewall	IP, Index du fichier demandé numéro du port etc.

Tableau 1.1: Les requêtes gnutella

8.1.3 P2P centralisé

Ici on a encore les serveurs avec une fonction un peu particulier et différent des serveurs du modèle client/serveur, ce modèle du p2p centralisé est la première génération P2P car le modèle p2p a fait son apparition par le concept de centralisation.il existe un serveur central, avec un objectif claire qui est d'avoir le rôle d'un annuaire qui va stocker que des informations concernant la description des ressources partagées (nom, taille,……) et l'emplacement d'où ils peuvent être pris, en d'autres terme les informations sur les utilisateurs qui les hébergent (nom utilisé, IP, nombre de fichiers partagés,……), comme illustré dans la figure ci-dessous.

Tous les nœuds souhaitant partager des ressource, alors il contacte le serveur central et lui déclare, celui-ci stocke son adresse IP ainsi un numéro de port donné par le nœud où il pourra être contacté pour un téléchargement. Quand un utilisateur a envie de faire une recherche d'un fichier, alors lui aussi prend contact avec le serveur central en lui envoyant une requête et celui-ci lui répond en transmettant la liste des nœuds possédant le fichier demandé leur IP leur numéro de port, alors l'utilisateur a le choix de choisir parmi les réponses indiquées par l'index central celle qui lui convient le mieux, il contacte directement le ou les postes choisis, Le contenu reste toujours du côté client, ne passant jamais par le serveur.

Le modèle centralisé est déterministe et il permet une recherche simple, il est facile à administrer et à contrôler, c'est le cas souvent où on a le serveur, il est peu coûteux, nécessite qu'un seul serveur central pour la découverte et une machine hôte pour l'accès à la ressource, cependant il présente plusieurs inconvénients, il n'est pas robuste car la surcharge ou la panne du serveur central rend tout le réseau indisponible, mais il passe très mal à l'échelle. L'exemple le plus connu reposant sur cette architecture est "Napster". [6]

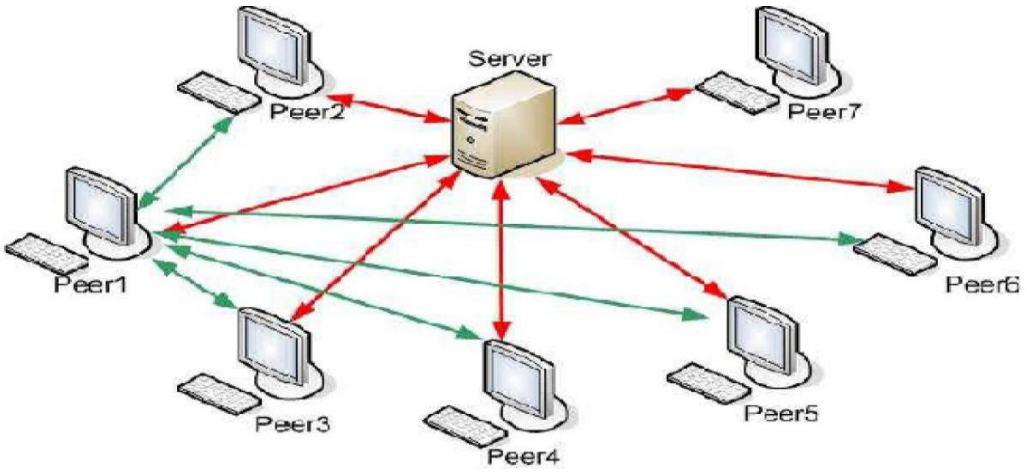

Figure 1.6: P2P centralisé

8.1.3.1 Napster

Lors d'apparition du réseau P2P on a comme tout premier logiciel Napster, il est l'exemple de l'architecture P2P centralisé, alors sa façon de fonctionner c'est la façon standard de l'architecture P2P centralisé dont on a parlé précédemment ça veut dire que tous les membres du réseau doivent passer par le serveur qui est notre annuaire dans le but de l'informer des fichiers dont ils disposent mais aussi de le contacter pour l'obtention des coordonnées d'un élément lorsqu'on souhaite lancer une recherche des fichiers dans ce réseaux. Un client désirant partager des fichiers doit exécuter sur son ordinateur le logiciel Napster. Etant connecté à Internet, le client établit une connexion TCP avec le serveur central Napster et lui déclare les fichiers partagés, le serveur central Napster qui est notre annuaire contient l'index avec toute<s les adresses IP des clients participants, ainsi qu'une liste de ressources partagées, comme nous avons dit précédemment, le fichier ne transite pas par le serveur central. Le logiciel permet à l'utilisateur de se connecter au pair désiré directement, c'est cette communication directe entre les pairs qui différencie le modèle P2P centralisé du modèle client-serveur classique. [6]

Principe :

a) Tout le monde doit avoir le logiciel Napster. On doit avoir la connexion internet lors de l'exécution du logiciel.

b) Après la stabilisation de la connexion entre le serveur et le client. Alors on déclare notre ressource, adresse IP, Port où on pourra être contacté.

c) Le serveur central maintient un répertoire des ordinateurs clients connectés et stocke les informations sur ces utilisateurs (notamment les fichiers en partage).

d) Le nœud voulant une ressource dans Napster doit contacter notre fameux serveur.

e) Le serveur renvoie à l'utilisateur une liste des réponses éventuelles : adresse IP, nom d'utilisateur, taille du fichier, l'utilisateur choisit le fichier qu'il veut et établit une connexion directe avec l'hôte du fichier, en lui envoyant sa propre adresse IP et le nom du fichier demandé.
f) Transfert du fichier entre les deux ordinateurs, puis connexion interrompue à la fin du transfert.

8.1.3.2 Les avantages d'un système centralisé

- Présence d'un serveur central : facile à administrer, et donc facile à contrôler.
- Evite les recherches coûteuses sur le réseau : pas de routage et planification de la gestion des utilisateurs.

8.1.3.3 Les limites d'un système centralisé

- Pas d'anonymat partout car chaque pair est connu du serveur et des pairs sur lesquels
- il télécharge.
- Limites habituelles d'un serveur central : problème de disponibilité, de passage à l'échelle (saturation de la bande passante et du nombre de processus).
- Cas de Napster : facile à fermer.

8.1.4 P2P hybrides

Dans les hybrides on a un véritable mélange et une combinaison des caractéristiques entre les modèles Pair à Pair totalement décentralisé et les modèles Pair à Pair centralisé.

Cette solution a permis de surpasser quelques problèmes rencontrés dans le modèle centralisé, car son côté décentralisation assure l'extensibilité, la tolérance aux pannes et le passage à l'échelle.

Ici on a les Super Pairs ces derniers ont des rôle particulier, généralement ces sont des pairs qui ont une forte capacité de calcul et une large bande passante, alors ces super-pairs ont des groupes des autres pairs moins puissants où il sert comme le serveur local pour ce groupe de pairs, comme la montre la figure. De nombreuses applications sont construites selon ce modèle, par exemple : Kazaa, BitTorrent. [11][12]

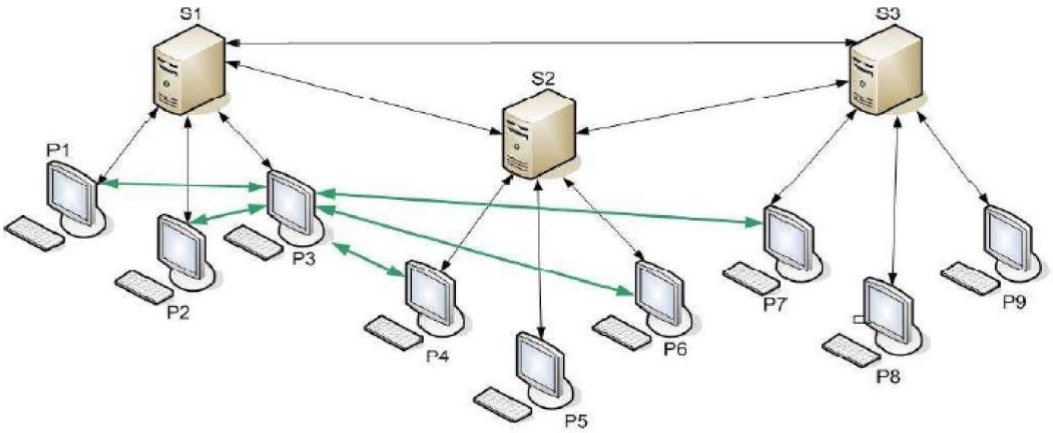

Figure 1.7: Modèle p2p Hybride

Remarque:

Certaines classifications des architectures P2P considèrent les modèles hybrides et centralisés comme identiques : le modèle centralisé est un modèle hybride avec un seul super pair.

8.1.4.1 KaZaA

Premièrement on doit classifier les pairs qui ont des capacités supérieurs aux autres pairs dans certains cas par exemple : une grande vitesse de connexion, une grande capacité de disque, et une grande capacité de traitement. Ceux-ci sont immédiatement désignés comme des super-pairs, ces derniers en plus de leur rôle spécifique à savoir l'hébergement de la liste des fichiers partagés par les clients peuvent aussi partager et télécharger des fichiers comme les autres pairs ordinaires. Tous les nœuds entre en contact avec des super pairs dont ils font partie pour pouvoir se connecter au réseau, et lui envoie la liste des fichiers qu'il désire partager afin qu'ils y soient indexés. Il lui envoie également des requêtes sur des fichiers qu'ils veulent obtenir. Une fois les contacts est établis entre les supers pairs et les pairs ordinaires alors les pairs obtiennent des adresses IP du pair qui dispose la donnée recherche, le super pair qui fournit ce adresse IP peut soit la cherche dans sa propre indexation local(les liste des ressource hébergés) donc ici on est dans le cas centralisé ou bien, il passe des requêtes aux autres super-pairs donc la technique utilisée entre les super pair pour communiquer est l'inondation de messages, les données restent toujours distribuées sur les pairs et les échanges se font directement d'un pair à un autre via le protocole HTTP. [6]

8.2 Réseaux structuré(DHT)

La deuxième grande classe est celle des réseaux P2P structurés, ils sont dits structurés, car au-dessus du réseau physique sous-jacent, les nœuds sont reliés par un réseau recouvrant construit sous certaines contraintes, répondant à plusieurs propriétés et connectant les peers selon une structure particulière donnée exemple en anneau : Chord ou cartésiennes : CAN.

On déploie une organisation de la topologie virtuelle dans l'architecture P2P structuré pour les méthodes de routage et localisation en vue de la faire correspondre à une topologie connue (anneau, Can,...). Chaque topologie présente des méthodes de nommage, routage et localisation qui lui sont propre. Les principales études sont basées sur les tables de hachage distribuées (Distribué Hash Table). L'avantage principal de ces topologies est qu'elles garantissent de trouver la donnée une fois elle est présente dans le système.

8.2.1 Chord

Chord est un protocole de recherche distribué, qui repose sur une structure en anneau, Chord utilise les hachages pour assigner aux nœuds et aux données leur identifiants à m bit et les id sont compris entre 0 à 2^m-1 (m est la taille d'un identifiant). L'identifiant d'un pair 37

Est un hachage réalisé à partir de son adresse IP et l'identifiant d'une ressource est le hachage de la donnée stockée. [6]

La figure suivante montre que les nœuds dans le protocole Chord sont ordonnés dans un cercle :

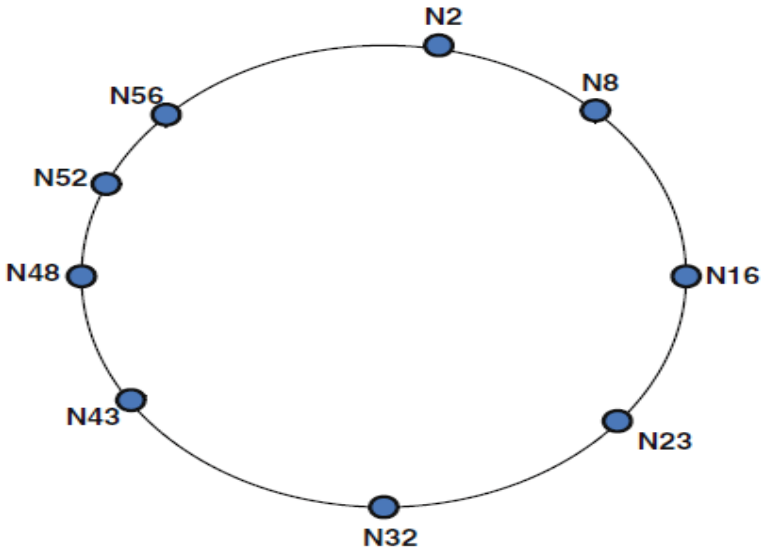

Figure 1.8: Architecture Chord

Table de Routage

Ici on a deux parties dans les mécanismes pour les routages en Chord la premier tables de routage : les tables de routages (Finger Table) sont très importantes pour les mécanismes de recherche des ressources qui sont réparties sur les différents nœuds de l'anneau. Ces tables de routages ont m entré où m est la longueur de l'identifiants exemple étant donné que l'id dans nœud est 8, l'i^{eme}entré dans le table de routage pointe vers le nœud qui est le plus proche numériquement a $8+2^{i-1}$ dans la direction des aiguilles d'une montre. Exemple on suppose que 8 est l'id d'un nœud alors la 3eme entrée dans le table pointe vers le nœud plus proche à

$8+2^{3-1}=12$ dans ce cas 16, et la deuxième est la liste de successeur d'un nœud qui contient non seulement le successeur immédiat mais une liste des n-1 nœuds successeurs, alors ça permet de gérer la robustesse et l'arrivée et départ des nœuds comme présenté dans les figure suivantes.

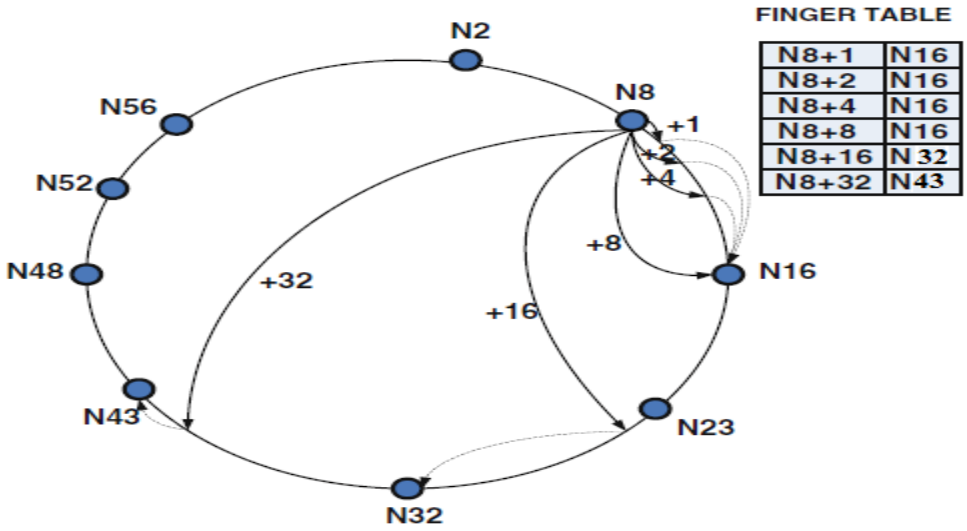

Figure 1.9: Illustration table du routage

Arrivé et départ des nœuds

Pour un nouvel arrivant la première chose à faire est le boostraping qui est tout simplement une opération qui doit être faite pour tous les nouveaux arrivants. Le boostraping commence depuis l'arrivée du nœud jusqu'au fonctionnement normal de ce nœud : quelques étapes pour réaliser le boostraping. [7][8]

1) Le nœud arrivant doit utiliser le hachage pour générer son id.

2) Il doit contacter un nœud déjà existant dans les réseaux pour chercher son successeur.

3) Le nouveau nœud utilise le protocole de la stabilisation pour corriger les tables des routages ce protocole est utilisé périodiquement en arrière-plan ce protocole a deux fonction suivant :

a) stabilise : que permet aux nœuds de savoir qu'il y a un nouvel arrivé ou un départ de nœud.

b) Fixfingers : assure que les tables soit maintenue correctement.

4) Construction de sa table de routage.

9. Conclusion

La technologie pair- à- pair offre des systèmes pair-à-pair qui ont été les derniers invités à arriver sur Internet, ils représentent un nouveau moyen d'offrir des services au bout de l'internet pour et par les usagers. Les systèmes pair-à-pair ne sont rien d'autres que des applications distribuées et massivement déployées, supportées par les ressources fournies par des usagers interconnectés par Internet, ces systèmes sont donc composés par un grand nombre d'hôtes, leurs propriétés ont permis le passage à l'échelle.

Chapitre 2:Lacryptographie

Introduction

La sécurité de l'information est un domaine très vaste qui regroupe tous les aspects de la sauvegarde ou la protection de l'information ou des données, sous quelque forme que ce soit. Les recherches actuelles en sécurité de l'information menées à se concentrent sur l'aspect plus technique du sujet, et plus particulièrement sur la sécurité dans les communications numériques et les systèmes d'information, la cryptologie, les principes mathématiques sous-jacents et les applications.

1. Les enjeux de sécurité dans un réseau sans fil P2P

Quelle que soit la nature du réseau, sa politique de sécurité vise à satisfaire lespropriétéssuivantes: [9]

- **Confidentialité des données:**

La confidentialité des données est une exigence importante dans la sécurité du réseau. Elle permet d'assurer qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour sécuriser le transfert des données.

- **Intégrité des données:**

L'intégrité peut être vue comme un ensemble de mesures garantissant la protection des données contre les modifications et altérations non autorisées. On peut distinguer les altérations accidentelles dues à l'environnement dur de communication, par exemple une mauvaise couverture des ondes, et les altérations volontaires d'un attaquant. Cela concerne aussi la protection contre l'injection ou la modification des paquets.

- **Disponibilité:**

La disponibilité est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate.

- **Authentification des pairs:**

L'authentification peut être définie comme le processus de prouver une identité revendiquée. La confidentialité, l'intégrité des données, et la non-répudiation dépendent tous de l'authentification appropriée. Un système sans cette fonctionnalité ne pouvait pas fournir les objectifs de sécurité mentionnés de manière satisfaisante. Elle est la pierre angulaire d'un réseau sans fil P2P sécurisé.

- **Non-répudiation:**

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.

2. Les modèles d'attaques

Les réseaux sans fil P2P sont susceptibles aux différentes attaques qui tentent d'exploiter ses différentes vulnérabilités pour mener des manipulations malicieuses. Les attaques peuvent se produire de différentes manières. La classification de ces attaques dépend de plusieurs paramètres :

2.1 Actif vs Passif: Une attaque passive obtient les données échangées dans le réseau sans perturber le fonctionnement de la communication, tandis qu'une attaque active implique l'interruption d'information, la modification, ou la fabrication, ce qui Perturbe le fonctionnement normal du réseau sans fil P2P. [10]

2.2 Interne vs Externe: Les attaques peuvent aussi être classées en deux catégories, À savoir les attaques externes et les attaques internes, selon le domaine de l'attaque. Les attaques externes sont effectuées par des nœuds qui n'appartiennent pas au domaine du réseau. Les attaques internes sont entreprises par des nœuds compromis, qui font partie du réseau. Les attaques internes sont plus graves par rapport aux attaques externes car l'attaquant connaît des informations précieuses et secrètes, et Possède un accès privilégié au réseau. [10]

2.3Individuelle vs Distribuée: Les attaques peuvent enfin être classées en attaques Individuelles ou attaques distribuées. Les attaques individuelles sont simples et ils Sont issus d'une seule source et par un chemin simple sans utiliser des stations Intermédiaires. Par contre, une attaque distribuée est une attaque évoluée invoquant Plusieurs stations ou provenant de plusieurs sources. Les attaques distribuées sont Plus dangereuses et difficiles à détecter puisqu'ils utilisent plusieurs stations Intermédiaires, ce qui a pour effet la difficulté de déterminer la source d'une telle Attaque.

3. Définition de la cryptographie

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses. [21]

3.1 Vocabulaire de base

3.1.1 Cryptologie: Il s'agit d'une science mathématique comportant deux branches : la cryptographie et lacryptanalyse.

3.1.1.1 Cryptographie: La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des donnéesde manière confidentielle sur un support donné.

Chiffrement: Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendreincompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.

Texte chiffré: Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'unchiffrement à un texte clair.

Clef: Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.
Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

3.1.1.2 Cryptanalyse: Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir detextes chiffrés en déterminant les failles des algorithmes utilisés. [17]

Crypto système: Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairset chiffrés possibles associés à un algorithme donné. [22]

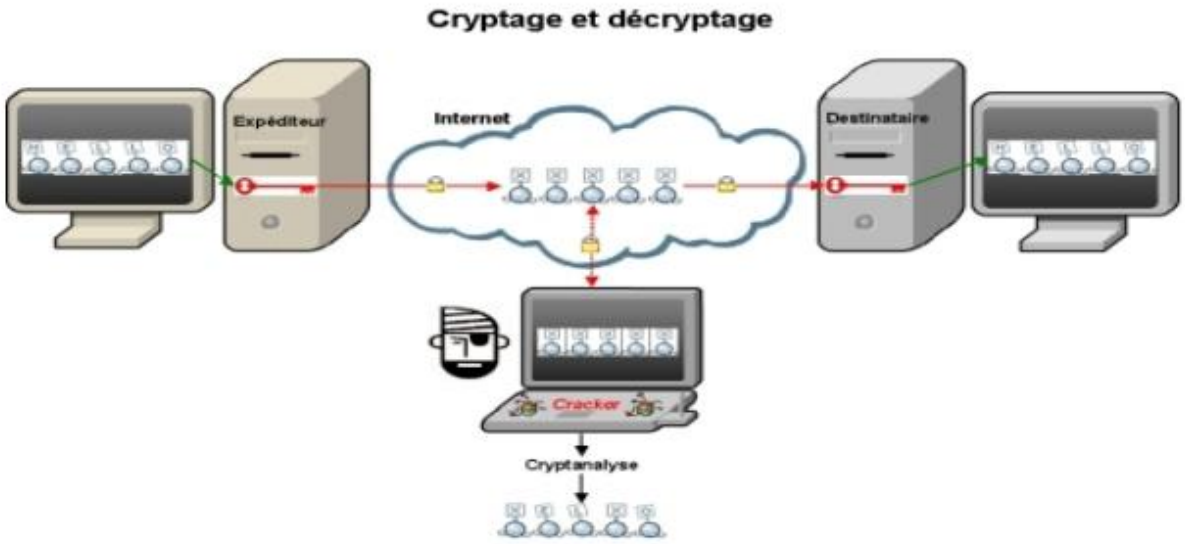

Figure 2.1: schéma de cryptage/décryptage.

4. Le cryptage symétrique

Le cryptage symétrique est la technique la plus ancienne et la plus connue. Une clé secrète, qui peut être un numéro, un mot ou simplement une chaîne de lettres dans le désordre, est appliquée au texte d'un message pour modifier le contenu d'une certaine manière. Cela pourrait être aussi simple que de décaler chaque lettre d'un certain nombre d'emplacements dans l'alphabet. Tant que l'expéditeur et le destinataire connaissent la clé secrète, ils peuvent crypter et décrypter tous les messages qui utilisent cette clé. [14] [24]

Le cryptage symétrique fonctionne selon deux procédés différents :

- le cryptage par flot: le cryptage s'effectue en continu, bit par bit

- le cryptage par bloc: Dans un système par blocs, chaque texte clair est découpé en blocs de même longueur et chiffré bloc par bloc.

4.1 Caractéristiques

– Les clés sont identiques : KE = KD = K

– La clé doit rester secrète.

– Les algorithmes les plus répandus sont le DES, AES, 3DES, ...

– Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés, – Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé.

– La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256.

Figure 2.2: chiffrement symétrique

5. L'algorithme L'AES

L'AdvancedEncryptions Standard a fait l'objet d'un appel d'offre datant de 1997.
Il s'agissait de remplacer le DES dont la taille des clés (56 bits) était devenuetrop petite pour les performances des ordinateurs modernes.
Parmi les 15 candidats, le candidat retenu (en 2000) se nomme RIJNDAEL (mais
On l'appelle simplement l'AES). Il est dû à deux chercheurs Belges, Rijmen etDaemen.[17][18]

C'est un chiffrement par bloc qui fonctionne itérativement
• Taille du bloc: 128 bits (mais aussi 192 ou 256 bits)
• Longueur de la clé: 128, 192 ou 256 bits
• Nombre de tours: 10, 12 ou 14
• Programmation de clés: 44, 52 ou 60 sous-clés ayant une longueur = 32 bits

Chaque tour (sauf le dernier) est une composition uniforme et parallèle

• AddRound key (bit-by- bit XOR with an expanded key)
SubBytes (byte-by-byte substitution using an S-box)
• ShiftRows (a permutation, which cyclically shifts the last three rows in the State)
• MixColumns (substitution that uses Galois Fields, *corps de Galois*, GF (28) arithmetic)

5.1 AES Keys

Avec 128 bit: 2^{128} = 3.4x 1038 clés possibles [19]
– A PC qui essaie 2^{55} clés par seconde besoins 149.000 milliards d'années à rompre AES

- con192 bit: 2^{192} = 6.2x 1057 clés possibles
- con 256 bit: 2^{256} = 1.1x 1077 clés possibles

Matrice:

En interne, les opérations de l'algorithme AES sont effectuées sur un Tableau bidimensionnel d'octets appelé l'état
- 4 lignes contenant chacune Nb octets
- Nb colonnes, chiffrées par des mots de 32 bits
- Sr, c désigne l'octet de rligne et de la colonne c

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Figure 2.3: Matrice

Le tableau d'octets en entrée est copié dans la matrice d'état

Sr, c ⟵ in

À la fin, la matrice d'état est copiée dans la matrice de sortie

Out ⟵ Sr, c

5.2 AddRoundKey (Matrices, Clé)

Convertir le contenu de chaque matrice en binaire ensuite ranger(XOR) avec la clé en binaire aussi.

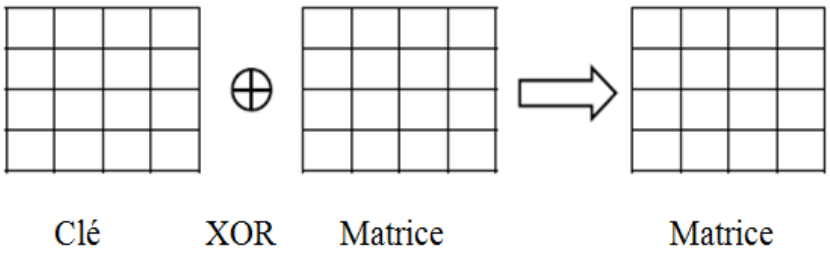

Figure 2.4: Rangement de matrices

5.3 SubBytes Transformation

Remplacement d'octets en utilisant un non-linéaire (mais inversible)
S-Box (indépendamment sur chaque octet).
• S-box est représenté comme un tableau 16x16, lignes et
Colonnes indexées par des bits hexadécimaux
• 8 octets remplacés comme suit: 8 octets définissent un
nombre hexadécimal rc, alors Sr, c = binaire (S-box (r, c))

Sr, c ⟵ S-BOX (Sr, c)

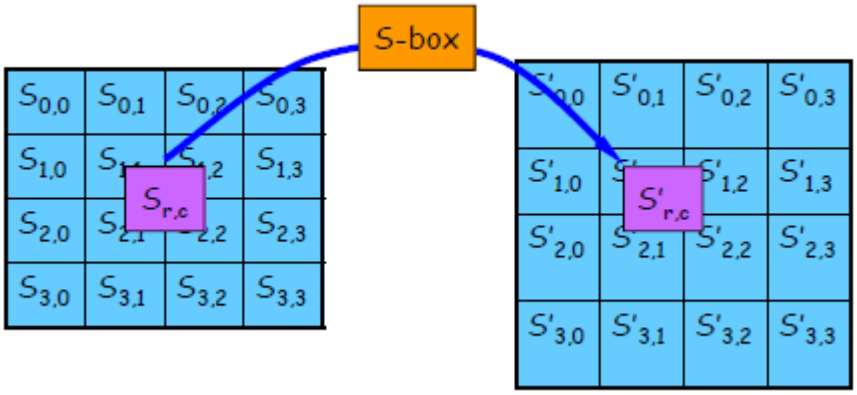

Figure 2.5: Les octets sont transformés à l'aide d'une boîte S non linéaire

Rijandael S-box Table:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	3	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tableau 2.1: Rijandael S-box

Exemple: hexa 53 est remplacé par hexa ED 17
(Les 4 premiers bits de l'octet (la première valeur hexadécimale, par conséquent) individualisent la ligne,
Les 4 derniers bits indiquent la colonne)

5.4 ShiftRows

Décalage circulaire à gauche d'un nombre d'octets égal
au numéro de ligne.

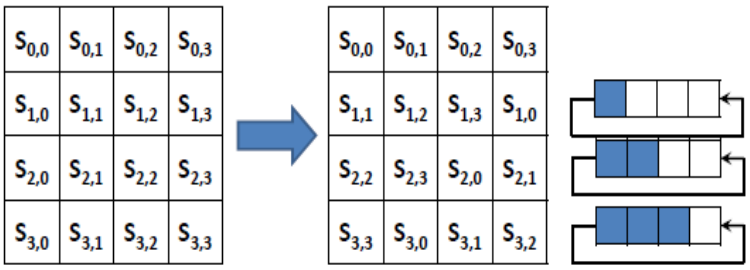

Figure 2.6: ShiftRows

5.5 MixColumns Transformation

- Interpréter chaque colonne comme un vecteur de longueur 4
- Chaque colonne d'État est remplacée par une autre

Colonne obtenue en multipliant cette colonne
avec une matrice dans un champ particulier (Galois Field)

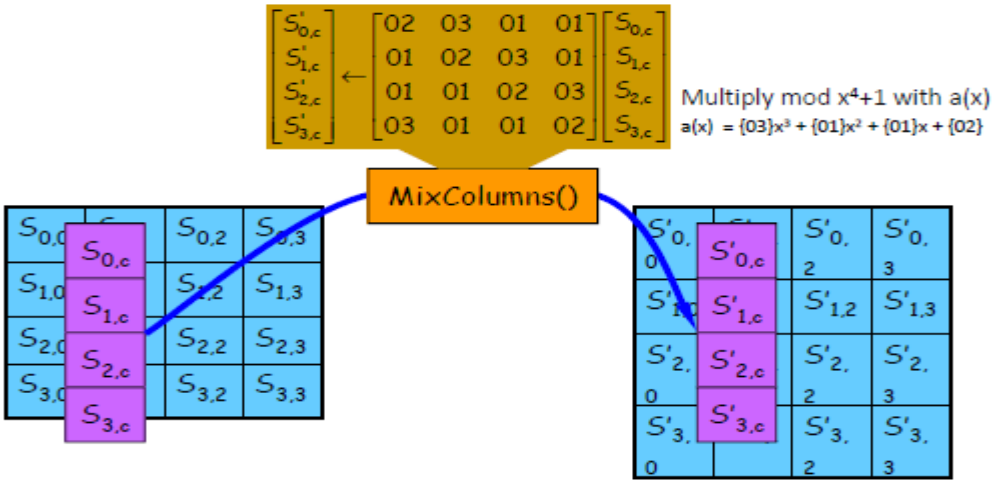

Figure 2.7: Les octets dans les colonnes sont combinés linéairement

5.6 Déchiffrement:

• L'algorithme de déchiffrement n'est pas identique à l'algorithme de chiffrement, mais utilise le même calendrier clé.
• Il existe également un moyen de mettre en œuvre décryptage avec un algorithme qui est équivalent à l'algorithme de cryptage (chaque opération remplacée par son inverse), cependant, dans ce cas, l'horaire clé doit être modifiée. [18]

6. Les avantages du cryptage symétrique

- la rapidité d'exécution (une seule clé utilisée).
- la simplicité d'implémentation (gestion d'une seule clé).
- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc...)
- Clés relativement courtes.

7. Les inconvénients du cryptage symétrique

- la complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.
- la sécurisation de la chaîne de transmission de la clé.
- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature.

8. Le cryptage asymétrique

Le problème avec les clés secrètes est de les échanger sur Internet ou sur un réseau de grande taille tout en évitant qu'elles ne tombent pas dans de mauvaises mains. Quiconque connaissant la clé secrète peut décrypter le message. Une réponse est un cryptage asymétrique, dans lequel il y a deux clés liées - une paire de clés. Une clé publique est librement disponible pour quiconque voudrait vous envoyer un message. Une seconde, une clé privée est gardée secrète que vous êtes le seul à connaître.

Tous les messages (texte, fichiers binaires ou documents) cryptés à l'aide de la clé publique peuvent uniquement être décryptés en appliquant le même algorithme, mais à l'aide de la clé privée correspondante. Tous les messages cryptés à l'aide de la clé publique peuvent uniquement être décryptés à l'aide de la clé publique correspondante.

Ce qui signifie que vous ne devez pas vous inquiéter sur la circulation des clés publiques sur Internet (les clés sont supposées être publiques). Toutefois, le problème peut résider dans le fait que le cryptage asymétrique est plus lent que le cryptage symétrique. Il nécessite une capacité de traitement supérieure pour crypter et décrypter le contenu des messages. [24] [14]

On peut classer l'utilisation des algorithmes à clé publique en 3 catégories :

– **Chiffrement/déchiffrement:** cela fournit le secret.

– **Signatures numériques:** cela fournit l'authentification.

– **Échange de clés** (ou des clefs de session).

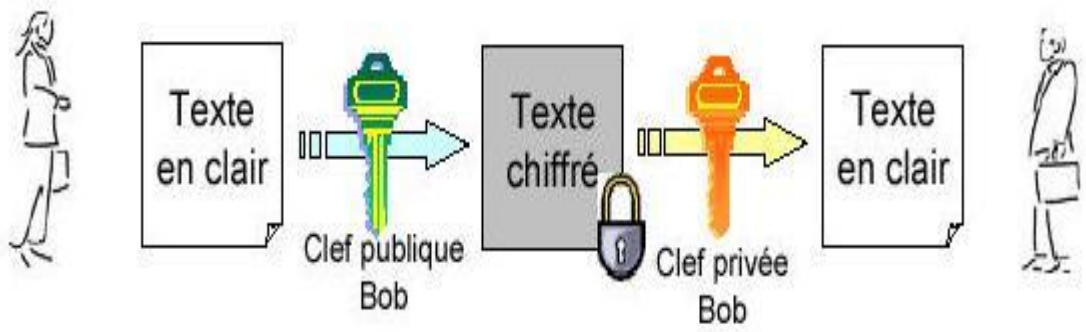

Figure 2.8: chiffrement asymétrique

9. L'algorithme RSA

RSA est un algorithme pour la cryptographie à clé publique qui repose sur la Difficulté présumée d'affacturage de grands nombres entiers, problème d'affacturage.

RSA signifie Ron Rivest, Adi Shamir et Leonard Adleman, qui d'abord Décrit publiquement l'algorithme en 1977. Clifford Cocks, un anglais Mathématicien, avait développé un système équivalent en 1973, mais il N'a été déclassifié qu'en 1997. RSA utilise partout - https, ssl, Transferts d'argent.

Un utilisateur de RSA crée et publie ensuite le produit de deux grands premiers Les nombres, avec une valeur auxiliaire, comme leur clé publique. Premier Les facteurs doivent être gardés secrets. Toute personne peut utiliser la clé publique pour chiffrer un Mais avec les méthodes actuellement publiées, si la clé publique est Assez large, seule une personne connaissant les facteurs primaires peut Décrypter le message de façon réaliste. La rupture du cryptage RSA est-elle aussi Dès lors que l'affacturage est une question ouverte appelée problème RSA. [26]

9.1 Description détaillée de l'algorithme

L'algorithme de chiffrement Départ :

• Il est facile de fabriquer de grands nombres premiers p et q (+- 100 chiffres)

• Etant donné un nombre entier n = p*q, il est très difficile de retrouver les facteurs p et q

• Déterminer e tel que $3 < e < \Phi(n)$ et $(e, \Phi(n)) = 1$

1) Création des clés

• La clé secrète : 2 grands nombres premiers p et q

• La clé publique : n = p*q ; un entier e premier avec$\Phi = (p-1)\ (q-1)$

2) Chiffrement : le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante : $C = M^e \bmod n$

3) Déchiffrement : il s'agit de calculer la fonction réciproque $M=C^d \bmod n$

Tel que $D = e^{-1} \bmod [(p-1)\ (q-1)]$

- La clé publique se compose du module n et du public (ou du cryptage)Exposant e.

- La clé privée se compose du module n et du privé(Ou décryptage) exposant d, qui doit être gardé secret.

P, q et φ (n)Doivent également être gardés secrètes car ils peuvent être utilisés pour calculer d.

Exemple

Soient p = 31, q = 53 c'est-à-dire n=1643. Φ(n) = 1560 (nombre d'éléments relativement premiers à n et < n).

Soit e = 11 (par exemple, et on a bien (e, Φ(n))=1).

On détermine que d = 851 (inverse modulaire de e sur ZΦ(n)).

La clé publique est donc (11,1643) et la clé privée est (851,1643).

Soit le codage par la position dans l'alphabet du mot «ANEMONE». Il vient

01 14 05 13 15 14 05

On procède selon deux conditions :

1. Découpage en morceaux de même longueur, ce qui empêche la simple substitution :

011 405 131 514 05

On ajoute un pudding initial si nécessaire.

001 140 513 151 405

Cela provoque la perte des patterns (« NE »).

2. Découpage en morceaux de valeur inférieure à n, car opération modulo n.

Lors du chiffrement, on a

$001^{11} \bmod 1643$	0001
$140^{11} \bmod 1643$	0109

$513^{11} \bmod 1643$	0890
$151^{11} \bmod 1643$	1453
$405^{11} \bmod 1643$	0374

Tableau 2.2: Exemple de chiffrement

Et pour le déchiffrement,

$0001^{851} \bmod 1643$	001
$0109^{851} \bmod 1643$	140
$0890^{851} \bmod 1643$	513
$1453^{851} \bmod 1643$	151
$0374^{851} \bmod 1643$	405

Tableau 2.3: Exemple de déchiffrement

Lors du déchiffrement, sachant qu'il faut obtenir des blocs de 2 éléments (grâce au codage particulier de l'exemple), on a bien

01	14	05	13	15	14	05
A	N	E	M	O	N	E

Tableau 2.4: résultat de déchiffrement

- **Remarques**

Il n'est pas très astucieux de choisir d'aussi petites valeurs car on peut retrouver d très facilement.

En pratique, il faut prendre de très grandes valeurs de p et q. Pour retrouver ces grandes valeurs, il faudra alors utiliser le Jacobien et le test de Solovay-Strassen par exemple.

10. La sécurité

10.1 Attaques:

Il existe trois approches pour attaquer le RSA : [24][25]

- recherche par force brute de la clé (impossible étant donné la taille des données),
- attaques mathématiques (basées sur la difficulté de calculer Φ(n), la factorisation du module n) :
- factoriser n=p*q et par conséquent trouver Φ(n) et puis d,
- déterminer Φ(n) directement et trouver d,
- trouver d directement.
- attaques de synchronisation (sur le fonctionnement du déchiffrement).

A l'heure actuelle, la factorisation connait de lentes améliorations au cours des années. La meilleure amélioration possible reste l'optimisation des algorithmes. Excepté un changement dramatique, le RSA- 1024 restera sûr pour les prochaines années. D'après les projections, une clé de 2048 bits est sensée tenir jusque 2079 si on tient compte de la loi de Moore. Mais ces valeurs sont correctes uniquement si on respecte les propriétés de e, d, p et q. [7]

- **Attaque de synchronisation (timing attack)**

Développé dans le milieu des années 90, il s'agit d'exploiter les variations de temps pris pour effectuer certaines opérations (par exemple la multiplication par un petit ou un grand nombre). Plusieurs contre-mesures existent telles que l'emploi de temps constants d'élévation à une puissance, l'ajout de délais aléatoires, ou le fait de rendre non visibles les valeurs utilisées dans les calculs. Dans ce dernier cas, cela reviendrait à calculer :

$$(r^e * m^e)\ d \bmod n$$

10.2 La menace quantique

Les valeurs précitées sont valables si on pratique la factorisation. A côté de cela, la physique pourrait faire pencher la balance, par l'utilisation d'un ordinateur quantique[4]. Celui-ci existe d'un point de vue théorique depuis 1994 (algorithme de Shor), et son prototype depuis 1996. Si son évolution se poursuit, il permettrait de réaliser la factorisation d'un nombre en un temps polynomial. Le principe est que les 0 et 1 représentés par les portes logiques des transistors sont

remplacés par l'orientation du champ magnétique émit par les atomes (que l'on nomme des q-bits).

11. Conseils d'utilisation du RSA

Pour garantir une bonne sécurité, il faut respecter certains règles telles que :

– Ne jamais utiliser de valeur n trop petite,

– N'utiliser que des clés fortes (p-1 et q-1 ont un grand facteur premier),

– Ne pas chiffrer de blocs trop courts

– Ne pas utiliser de n communs à plusieurs clés

– Si (d, n) est compromise ne plus utiliser n.

12. La vitesse de l'algorithme RSA

L'Algorithme RSA est lent, en raison de nombreuses multiplications. Vous pouvez Crypter / décrypter à vitesse de plusieurs kb / sec. Il est trop lent à utiliser pour Session de cryptage. Donc, habituellement, il y a une session AES. AES est Algorithme symétrique. C'est la sécurité et rapide. Clé d'échange de serveurs pour Session, en utilisant RSA. Nous avons donc une session rapide et sécurisée

13. Les avantage du cryptage asymétrique

- Résolvent le problème de la transmission des clés (clé de chiffrement publique => on peut envoyer un message chiffré à quelqu'un que ''on n'a jamais rencontré)
- Sont beaucoup plus lents que les algorithmes symétriques
- Sont vulnérables à une attaque « à texte clair connu » (la clé de chiffrement étant publique un pirate peut essayer de nombreux textes clairs et voir si le texte chiffré correspond)
- Sont vulnérables à une attaque « de
- l'intermédiaire » (un pirate peut substituer une clé publique par la sienne, intercepter et déchiffrer les messages, puis les rechiffrer avec la correcte clé publique et les

renvoyer). Attaque indécelable simplement => nécessité de la certification des clés publiques

14. Les inconvénients du cryptage asymétrique

- Il n'est pas prouvé que les problèmes mathématiques sous-jacents ne puissent être résolus par de meilleurs algorithmes
- Il n'est pas prouvé que la cryptanalyse est de même difficulté que les problèmes mathématiques sous-jacents (pour RSA il est juste prouvé que trouver d ou (p-1)(q-1) est de même difficulté que la factorisation)
- Les progrès des algorithmes et de la technologie informatique imposent des clés de taille élevée (au moins 1024 bits)
- Dans la pratique, les algorithmes à clé publique sont surtout utilisés pour chiffrer et transmettre une clé de session (le message est ensuite chiffré en utilisant un algorithme symétrique et cette clé de session) : crypto systèmes hybrides.

15.Conclusion

Dans ce chapitre, nous avons présenté les deux différents types de chiffrement symétrique et asymétrique et on a fait une comparaison (avantages et inconvénients) entre ces deux types, et on a décrit l'algorithme de chiffrement AES et l'algorithme à clé publique RSA la plus utilisé,

Mais bien sûr il en existe beaucoup d'autres. Ce algorithme joue un rôle important aussi bien au niveau de la sécurité que des performances.

Chapitre 3: Conception et Réalisation De L'application

Introduction

Dans ce chapitre, nous allons présenter notre application qui est fondée sur le cryptage d'un contenu (text, fichier, photo) partagé dans un réseau P2P, nous parlerons de l'objectif de cette application, nous présenterons par la suite les outils que nous avons utilisés pour commencer la réalisation de notre projet. Enfin nous nous intéresserons au fonctionnement de l'application par des diagrammes, des captures d'écran et des interfaces graphiques.

1. L'objectif

Notre application a pour objectif de maintenir des communications privées dans un réseau P2P, c'est-à-dire de pouvoir cacher les informations lors de la transaction des messages, des fichierset des photos. La raison pour laquelle nous avons utilisé les algorithmes cryptographiques que nous mentionnons:

L'algorithme AES:

Lors du cryptage de messages longs et volumineux, nous avons rencontré plusieurs problèmes dans RSA, car cela prend trop de temps et parfois n'obtient pas lerésultat. Nous avons utilisé AES pour crypter des messages volumineux et des fichiers. Dans chaque message d'envoi, générer une nouvelle clé et crypter le message avec ces clés.

L'algorithme RSA:

En utilisé la cryptographie asymétrique par l'algorithme RSA pour crypter les clés AES qui en a générer dans chaque envoi d'un message. L'algorithme RSA crypté les clés AES avec la clé public (public. Key) et décrypté les même clés avec la clé privé (private.key) au moment de la réception des messages.

Les clés RSA sont les même dans toutes les peers de ce réseau par contre les clés AES distribué avec chaque message parce que chaque message avoir son clé AES, les clés RSA

(Public et privé sont enregistrés dans une ficher (public. Key et private.key).

2. Les outils de travail

Java est à la fois un langage de programmation informatique orienté objet et un environnement d'exécution informatique portable créé par James Gosling et Patrick Naughton employés de Sun Microsystems, présenté officiellement le 23 mai 1995 au SunWorld. Les applications (ex: Peer to Peer) développées en Java peuvent fonctionner sur différents systèmes d'exploitations, comme Windows ou Mac OS.

Java présente un ensemble de classes standards (bibliothèque standard) pour tous les domaines d'application informatique existants. [27]

Figure 3.1: Java-prog-Logo

NetBeans est un environnement de développement intégré (IDE) open-source pour le développement avec Java, PHP, C ++ et d'autres langages de programmation. NetBeans est également appelé une plate-forme de composants modulaires utilisés pour développer des applications de bureau Java.

Techopedia explique NetBeans.

NetBeans est codé en Java et fonctionne sur la plupart des systèmes d'exploitation avec une machine virtuelle Java (JVM), including Solaris, Mac OS, and Linux. [28]

Figure 3.2: Netbeans Logo

WampServer est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l'aide du serveur Apache2, du langage de scripts PHP et d'une base de données MySQL. Il possède également PHPMyAdmin pour gérer plus facilement vos bases de données. [29]

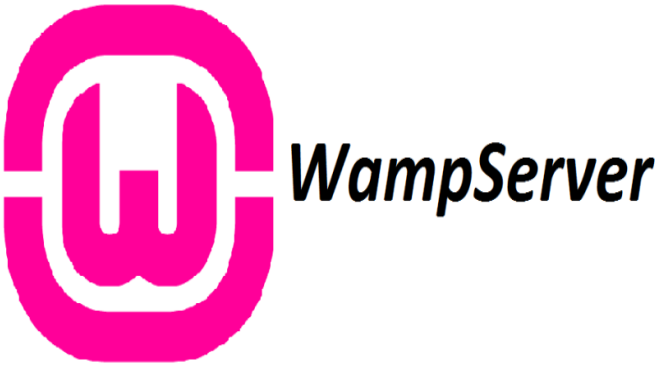

Figure 3.3: Wampsever Logo

3. Fonctionnement de notre application

Type de message :

Dans une conversation entre deux Peer. Chaque message contient sa propre informations et compose de :

- type de message (texte ou fichier)

- le message crypté par l'algorithme AES

- la clé AES crypté par RSA

- les informations de l'expéditeur

- nom de fichier

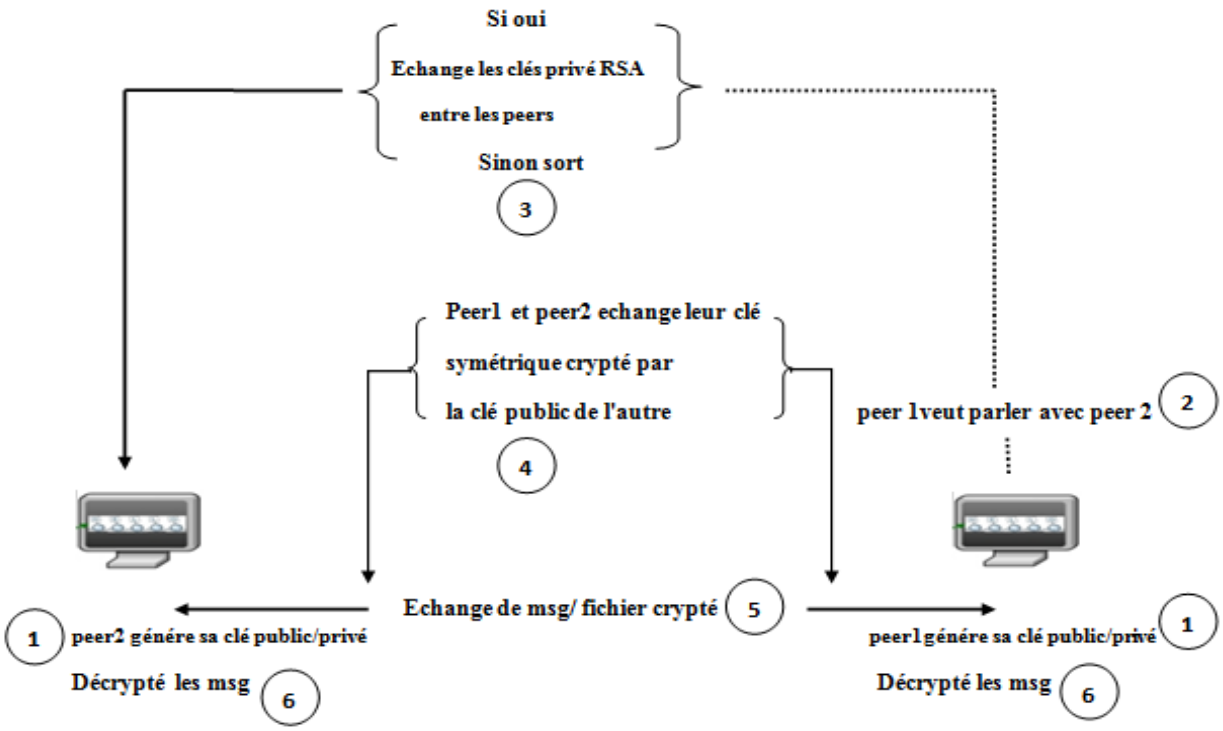

Figure 3.4: Fonctionnement de l'application entre deux Peer

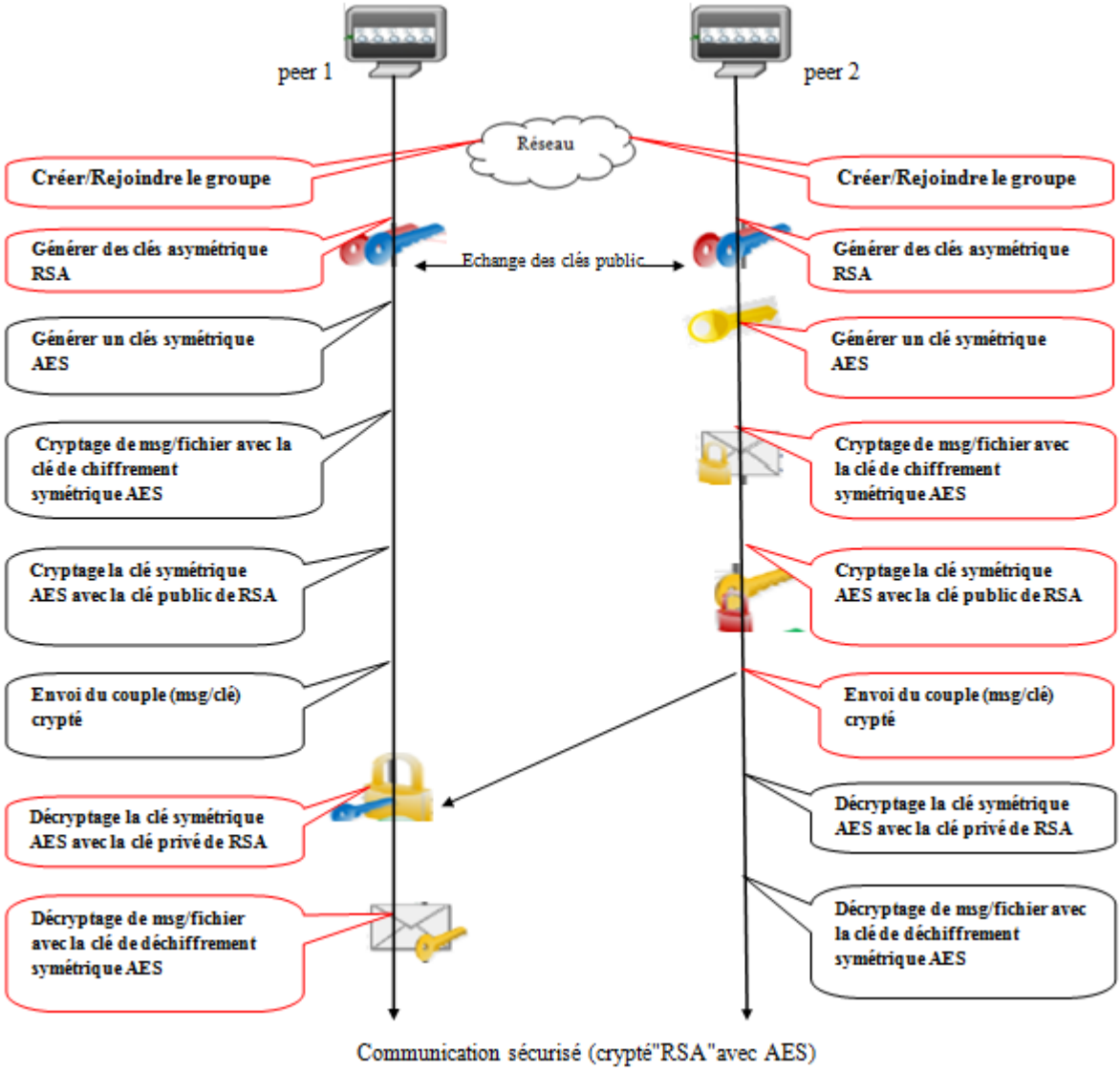

Figure 3.5: Fonctionnement détaillé de l'application

Le cas de l'envoi de message

Etape 01: Cryptographie symétrique

Commencer par générer une clé AES, ensuite convertir le message (text, fichier) ce que nous voulons envoyer comme une liste des bits crypté par l'algorithme AES.

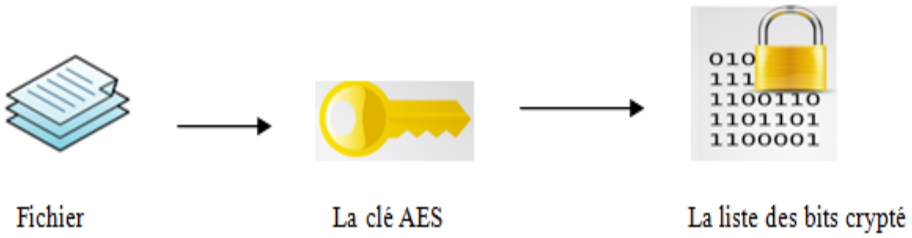

Figure 3.6: Fichier crypté par l'algorithme AES

Etape 02:Cryptographie asymétrique

Crypter la clé AES par la clé publique de RSA (public. Key) et l'envoyer avec la liste des bits auparavant crypté.

Figure 3.7: La clé AES crypté par la clé public de RSA

Le casde recevoir de message

Etape 01: Cryptographie asymétrique

Recevoir la clé AES et le contenu de ce message (comme une liste des bits crypté),

et décrypter la clé AES par la clé privé de l'algorithme RSA (private.key).

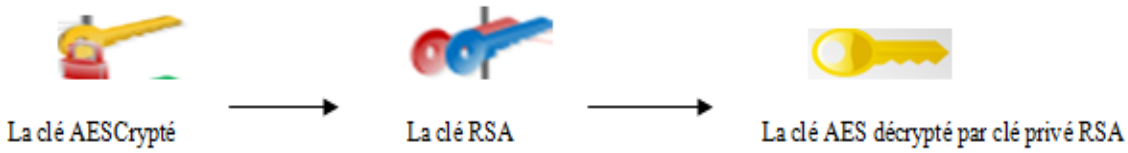

Figure 3.8: La clé AES décrypté par la clé privée de RSA

Etape 02: Cryptographie symétrique

Décrypter le contenu de message par la clé AES (qui on a déjà décrypté) ensuite convertir la liste des bits a un message (text, fichier), En conséquence, le message est affiché.

Figure 3.9: Décrypté le fichier par l'algorithme AES

4. Interface graphique

Cette première capture présente la fenêtre initiale qui s'ouvre lors du lancement de l'application.

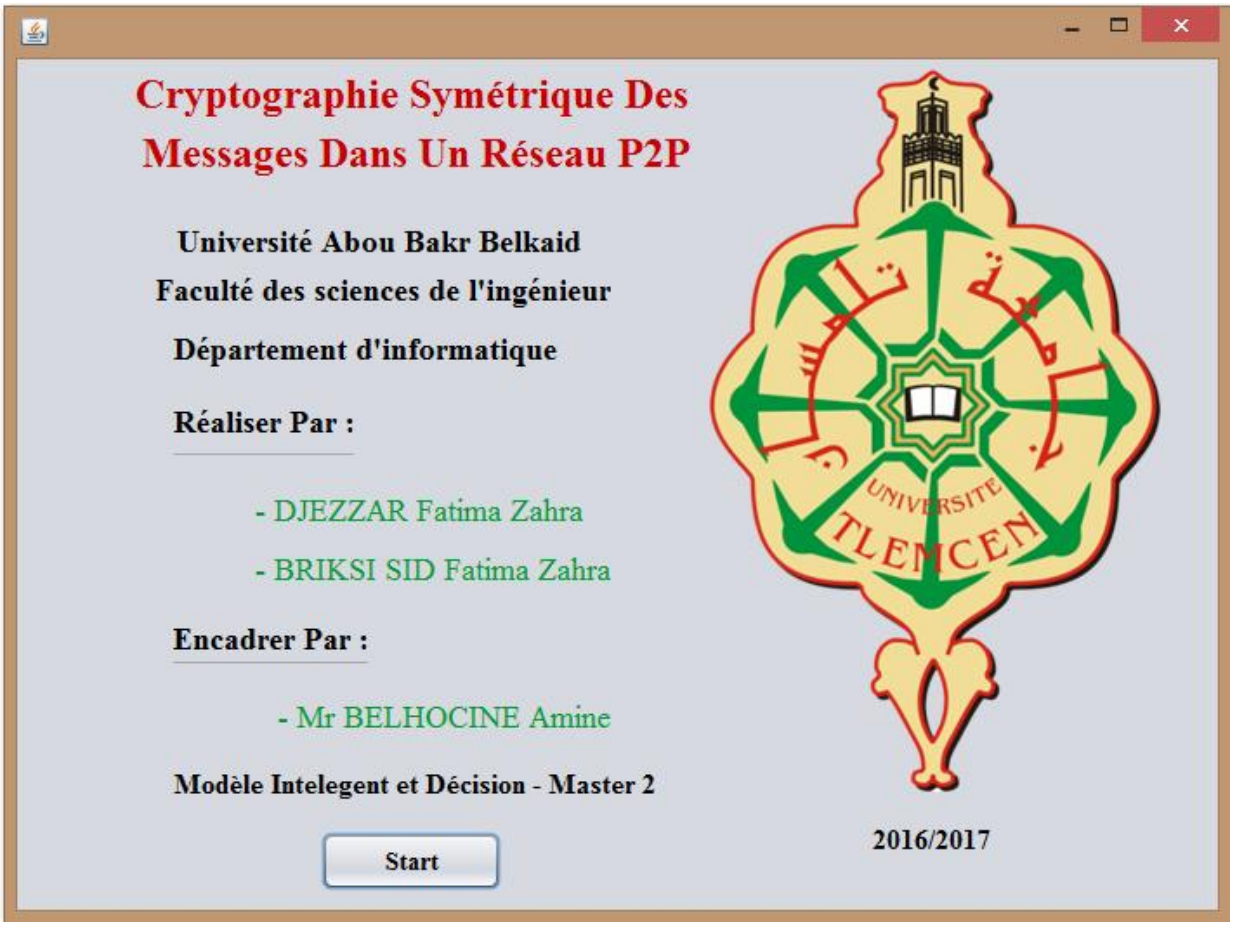

Figure 3.10: Interface initiale

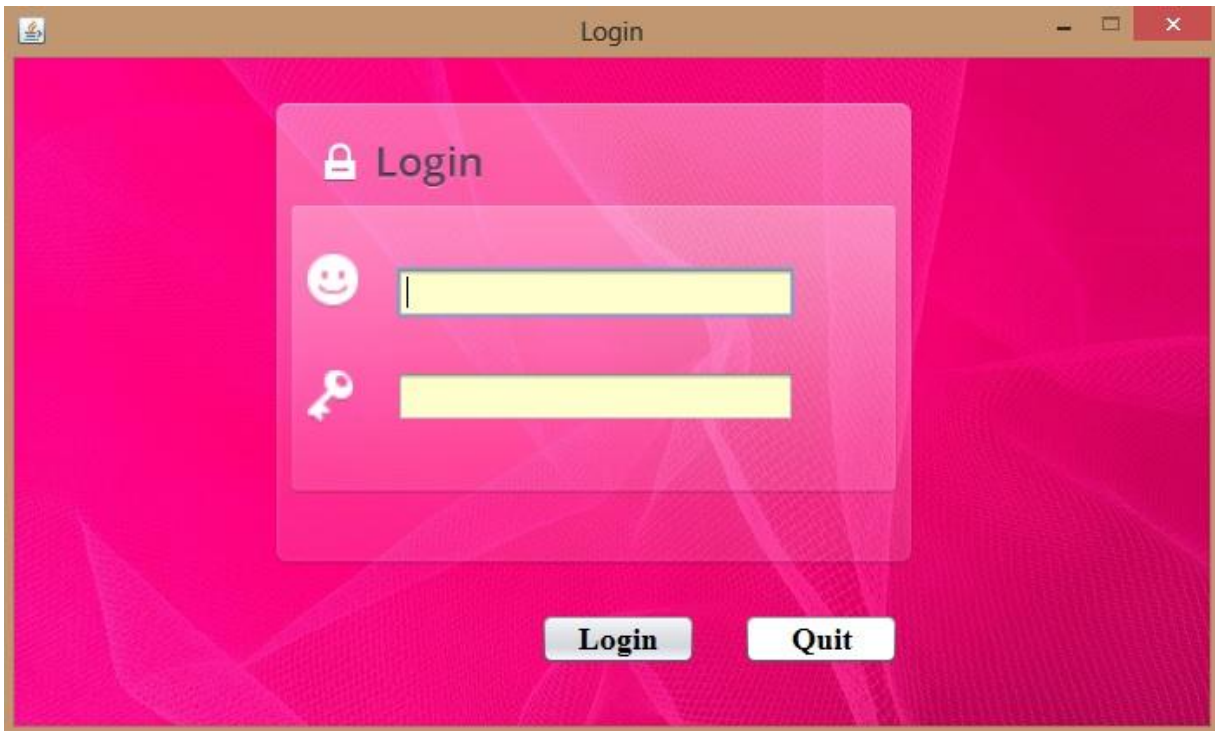

Figure 3.11: logind'une application

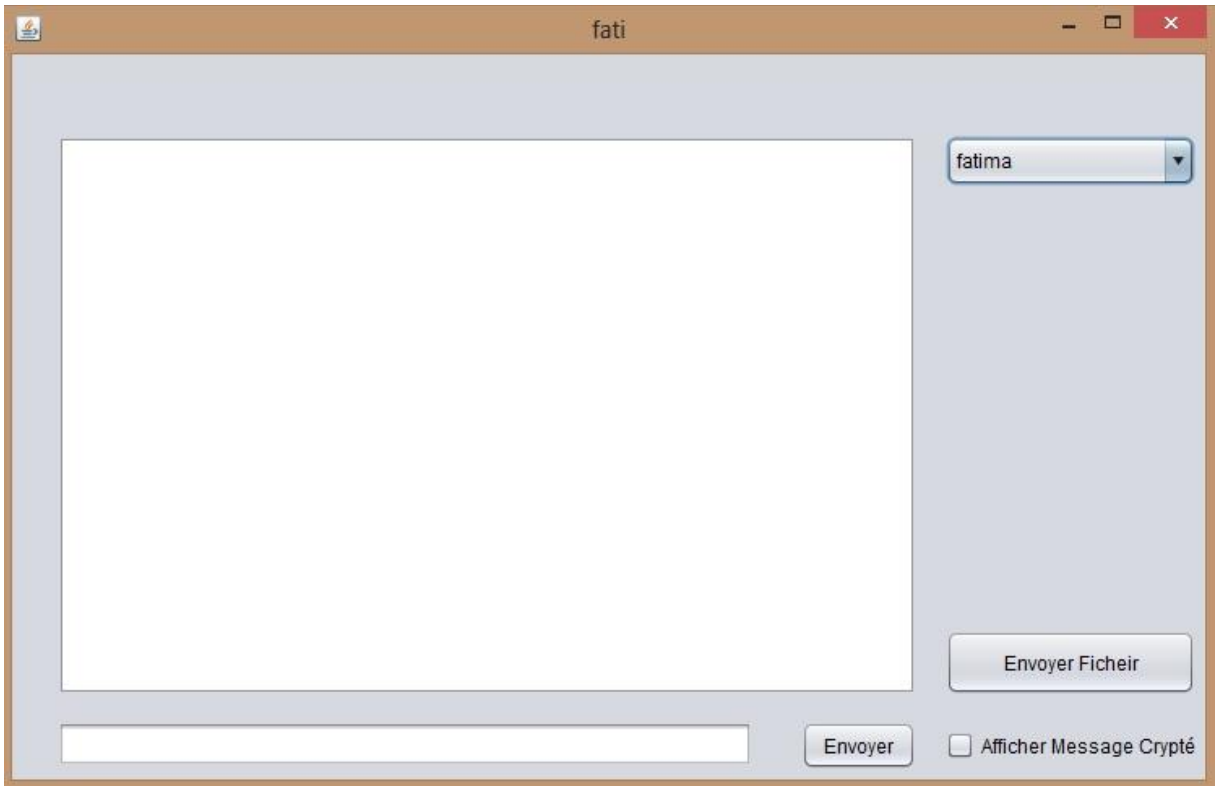

Figure 3.12: L'interface de chat

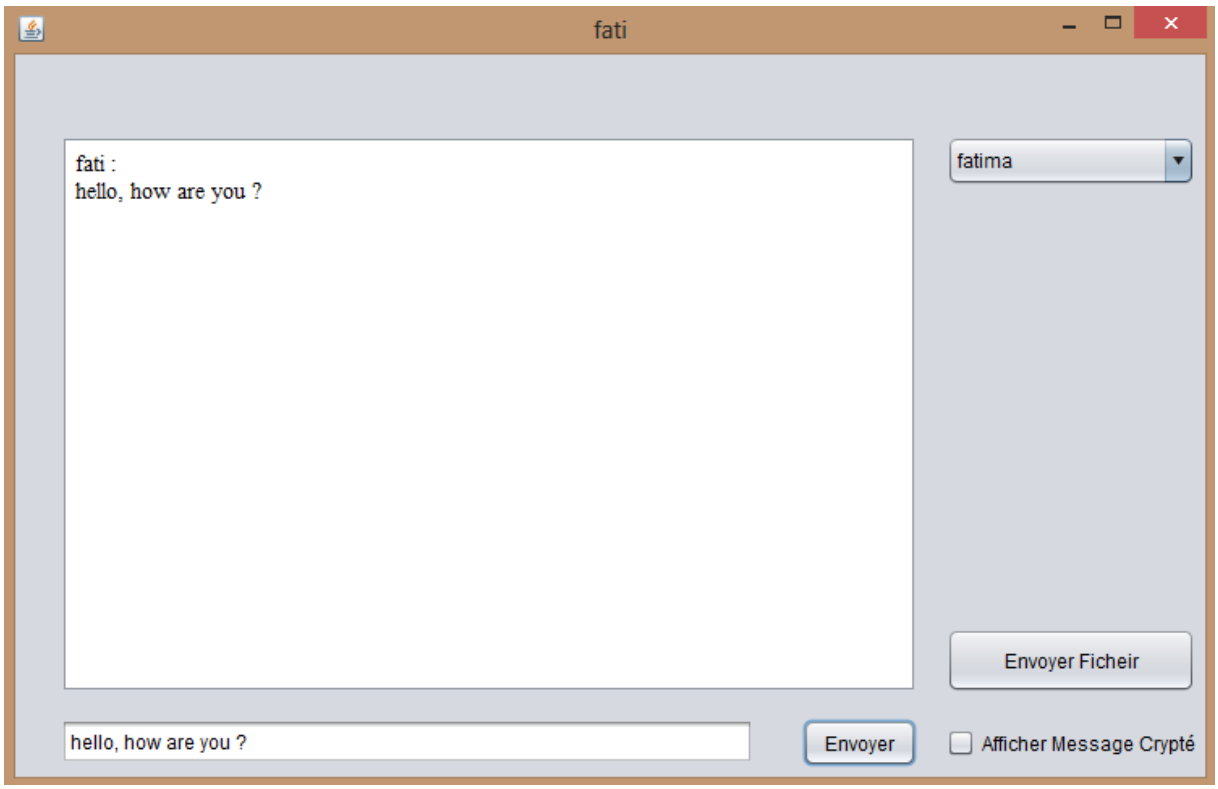

Figure 3.13: L'envoi d'un message clair

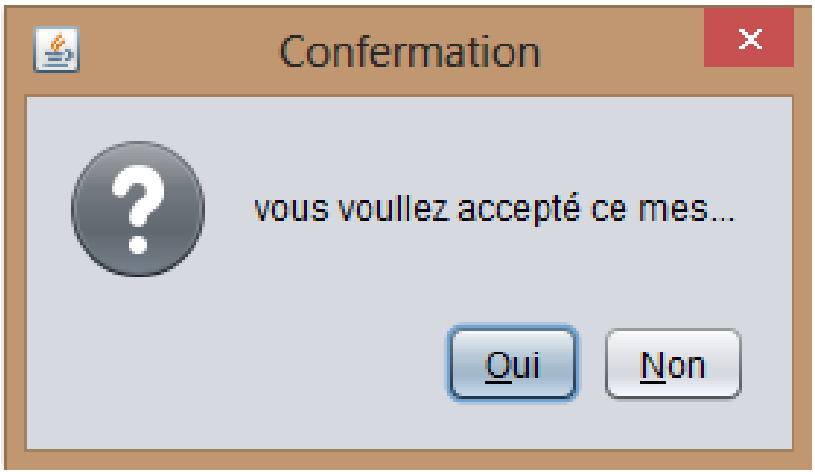

Figure 3.14: Alerte de confirmation

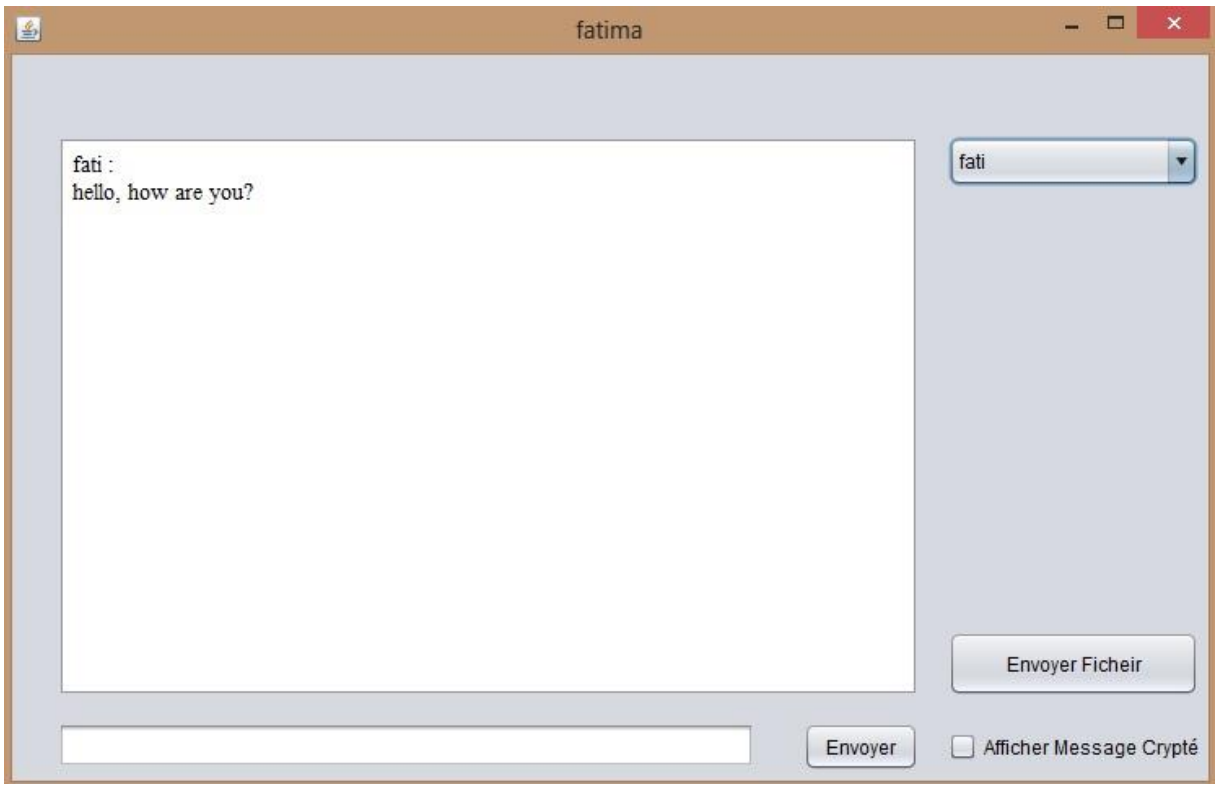

Figure 3.15: Recevoir un message clair

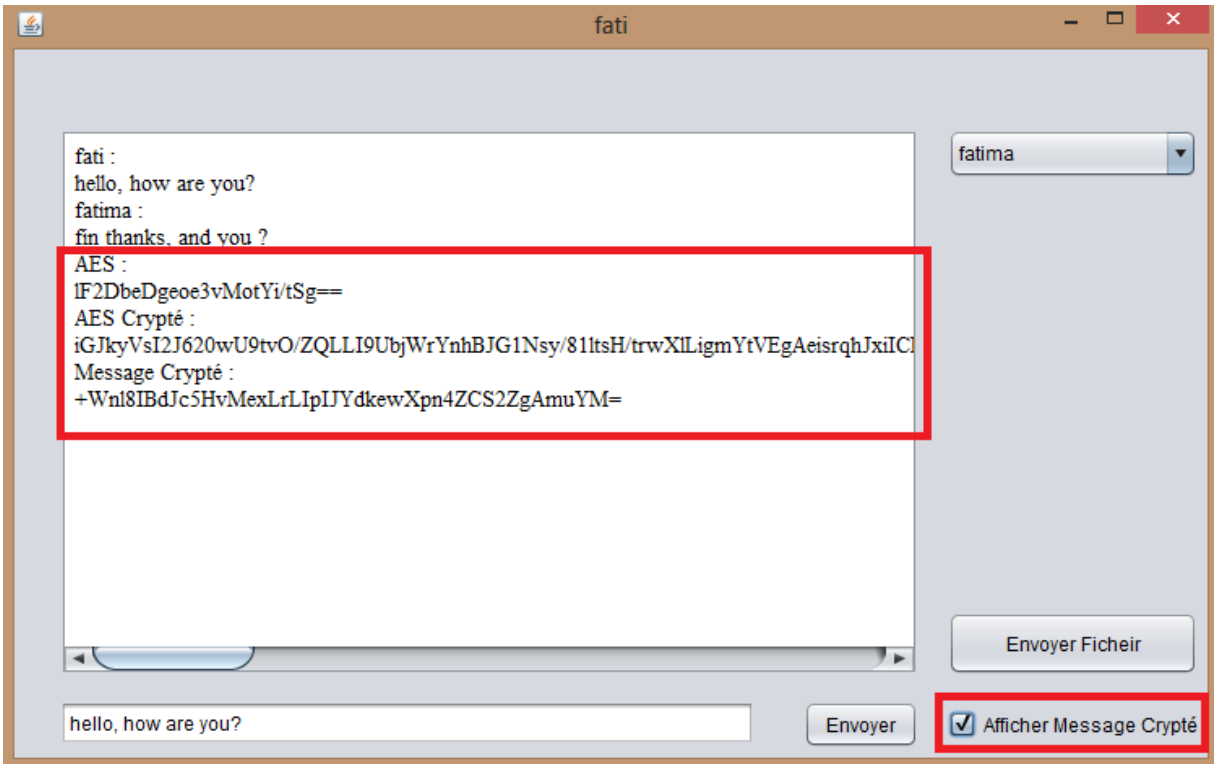

Figure 3.16: Recevoirun message crypté

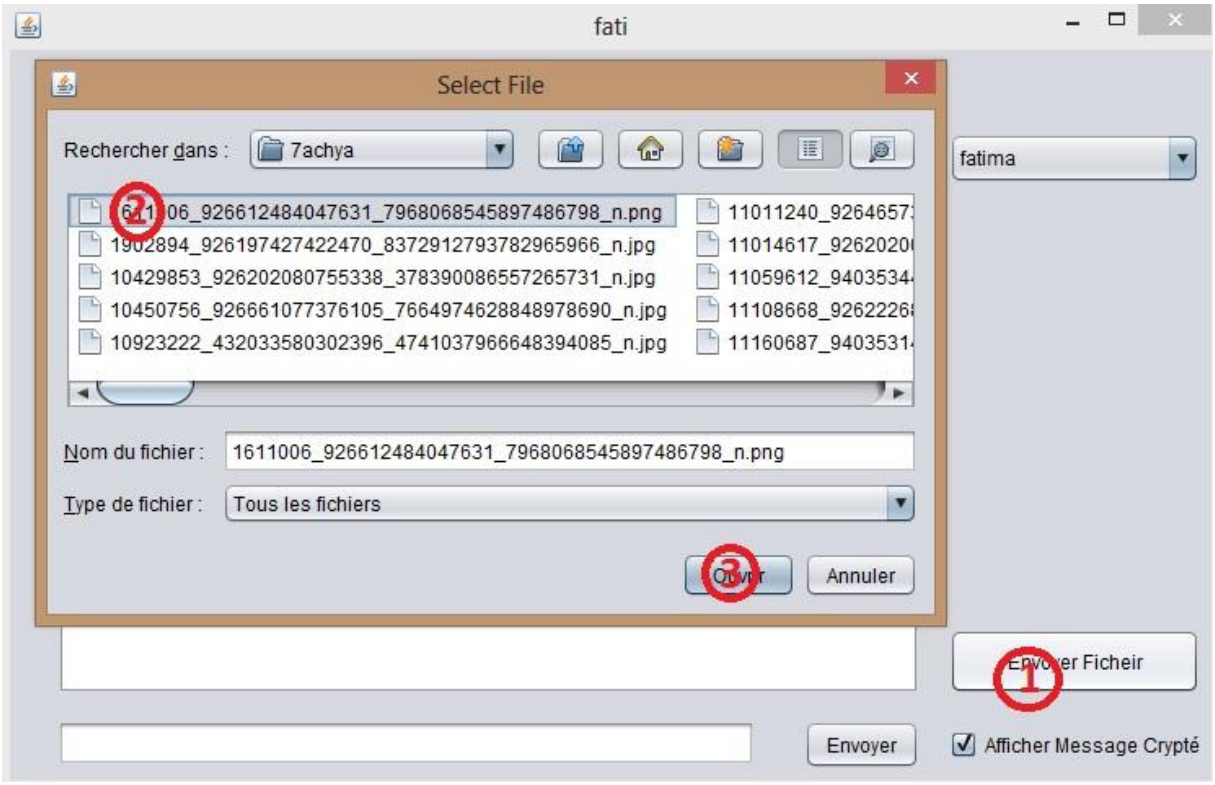

Figure 3.17: L'envoi d'un fichier

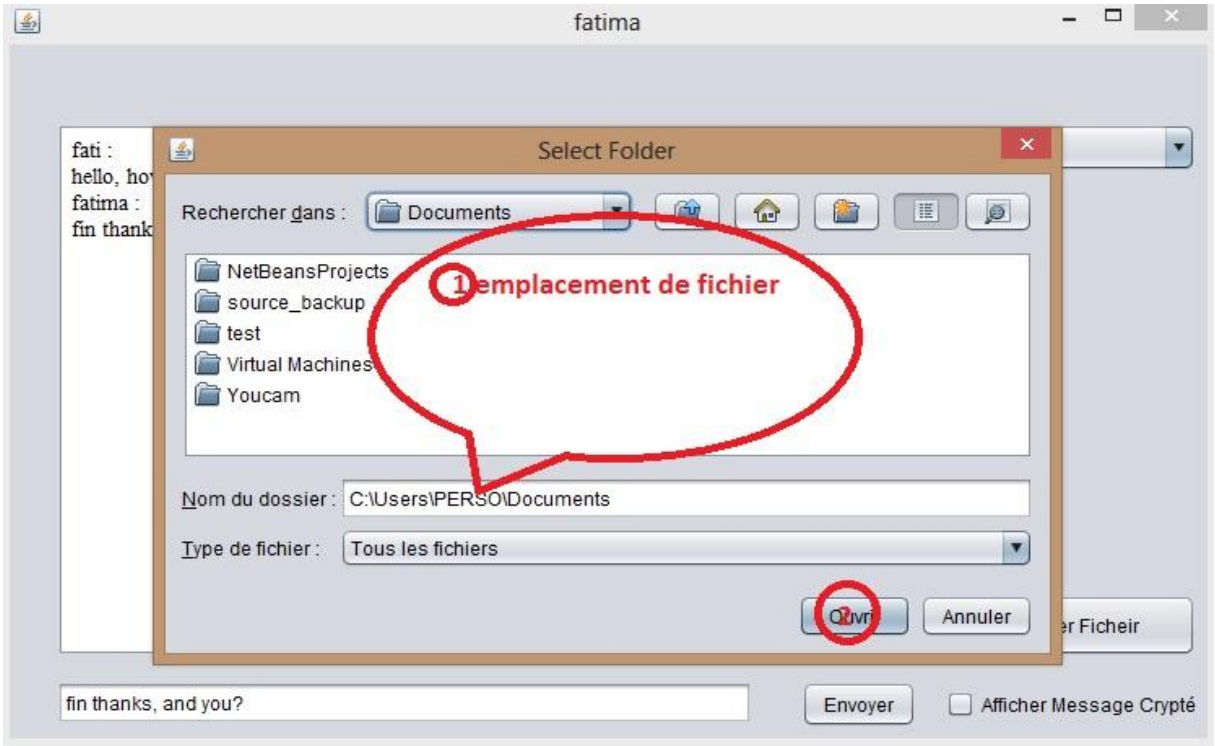

Figure 3.18: Recevoir "Emplacement "d'un fichier

5. Conclusion

Dans ce chapitre, nous avons présenté notre application et aborder les différentes étapes du fonctionnement de notre projet de fin d'étude. Notre travail s'estappuyé essentiellement sur la combinaison entre les algorithmes de chiffrement à clefs publiques-privées et les algorithmes à clefs secrètes dans les réseaux sans fil P2P, l'application que nous avons développée répond nettement à l'objectif initialementposé (sécurité), par la suite l'améliorée en rendons possible le partage de tous type de fichiers ainsi que le partage de vidéos et d'image. Et acquérir par cela la satisfaction d'un grand nombre d'utilisateur.

Conclusion générale

Ce travail a été principalement axé sur la sécurité des réseaux sans fil Peer to Peer, qui représente un vrai challenge, à cause des caractéristiques de ces réseaux.

En pratique un système est sur tant que personne ne l'a cassé et par conséquent le défi actuel est de fournir des paramètres efficace garantissant de manière sipossible prouvée une très forte sécurité qui ne sera pas détourné a des fin malhonnête La cryptographie est une science fondamentale et importante dans la sécurisation des informations transmission dans un réseau.

Au cours de ce projet, nous sommes intéressés au chiffrement des messages sur un réseau de communication. Donc, Notre objectif principal est de développer une application pour sécuriser la transmission des messages en utilisant une architecture Peer to Peer de système distribué.

Nous avons testé algorithme asymétrique de chiffrement RSA et algorithme symétrique AES afin d'assurer une sécurité et une protection de notre données qui est circulées dans notre réseau.

Finalement, nous envisageons comme perspectives du travail d'évaluer la capacité denotre proposition à résister à d'autres attaques dans des conditions supplémentaires.

Bibliographie

[1] https://www.techopedia.com/definition/18909/distributed-system,la date de consultation septembre 2017.

[2] Dijoux Alexandre Emma Samuel, Peer-To-Peer, Université Claude Bernard LYON 1, 2006, Disponible sur http://master-info.univ-lyon1.fr/M2SIR/2006/peer2peer.pdf, la date de consultation novembre 2008.

[3] Gabriel Antoniu, Luc Bougé, Thierry Priol, Partage de mémoire à très grande échelle sur des réseaux pair-à-pair, Editeur INRIA - Domaine de Voluceau - (France), N° 4410, Mars 2002, Disponible sur ftp://ftp.inria.fr/INRIA/publication/dienst/RR-4410.pdf, la date de consultation novembre 2008.

[4] H T Shen, B. Yu. Efficient Semantic-Based Content Search in P2P Network, IEEE TKDE 16(7), 2004.

[5] E. Adar, B. Huberman. Free Riding on Gnutella, Technical Report, Xerox PARC, septembre 2000.

[6] OtmaneBouhamida, « Modelisation et simulation du problem du trou noir dans les reseauxmobiles»these master de master, université de ouargala, 2013.

[7] Anne Benoit, « Cours Reseau Pair à Pair» université de lyon, 2006.

[8] Stoica. I, Morris .R, Karger. D, Kaashoek .M. F, Balakrishnan. H, Chord : A scalable peer-to-peer lookup service for internet applications, Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communication - SIGCOMM'01, ACM Press, 2001, p. 149-160.

[9] Liorens et al, 2003: C. Liorens et L. Levier, "Tableaux de bord de la sécurité réseau"**,** Eyrolles, Paris-France, 2003.

[10] **B**ing Wu et al, 2006: Bing Wu et al, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Department of Computer Science and Engineering, Florida Atlantic University,
springer, 2006.

[11] William Stallings. Cryptography and Network Security : Principles and Practice, 3rd ed. PrenticeHall, 2003.

[12] Didier Müller. Les Codes secrets décryptés. City Editions, 2007.

[13] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. Handbook of Applied Cryptography.CRC Press, Inc., Boca Raton, FL, USA, 1996.

[14] Philippe Oechslin. Les compromis temps-memoire et leur utilisation pour casser les mots de passewindows. 2004.

[15] Travis Spann. Fault induction and environmental failure testing, 2005.

[16] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks, 2002.

[17] Adi Shamir and Aran Tromer. Acoustic cryptanalysis : On nosy people and noisy machines, 2004.

[18] Li Zhuang, Feng Zhou, and J. D. Tygar. Keyboard acoustic emanations revisited. 2005.

[19] Jan C. A. van der Lubbe. Basic methods of cryptography. Cambridge University Press, 1998.

[20] Douglas R. Stinson. Cryptography: Theory and Practice, 2nd ed. CRC Press, Inc., 2002.

[21] G. Zennor, Cours de cryptographie, 2000.

[22] L. Ghislaine, Introduction à la cryptologie, 1998.

[23] Simon Guillem –Lessard projet de fin d'étude 2001-2002 Département des mathématiques et de l'informatique Université du Québec à Trois-Rivières.

[24] http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetriqueet-Asymétrique.

[25] http://glasnost.entrouvert.org/rubrics/45.html - la date de consultation juin 2017.

[26] Don Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnérabilités", Journal of Cryptologie, v. 10, n. 4, Dec. 1997 se trouve aussi ici http://habrahabr.ru/post/99376/http://habrahabr.ru/post/200858/

Gary L. Miller, "Riemann's Hypothesis and Tests for Primalit.

[27] https://www.oracle.com/fr/java/index.html -la date de consultation septembre 2017.

[28] https://netbeans.org/ -la date de consultation octobre 2017.

[29] http://www.wampserver.com/ -la date de consultation octobre 2017.