Ministère de l'Enseignement Supérieur et de Recherche Scientifique

Université Kasdi Merbah Ouargla

Faculté des Nouvelles Technologies de l'Information et de la Communication

Département d'Informatique et des Technologies de l'Information

Mémoire Master Académique

Domaine : Informatique et Technologie de l'Information

Filière : Informatique

Spécialité. Informatique Industrielle

Présenté par :

Melle BENATIA Anissa

Thème

Réalisation d'une application de TOIP (telephony over internet Protocol) chiffrée (avec un algorithme Chiffrement symétrique)

Soutenu publiquement le : 02/07/2017

Devant le jury composé de :

M BOUKHEMLA Akram	Président	UKM Ouargla
M KHALDI Amine	Encadreur/rapporteur	UKM Ouargla
M TOUMI Chahrazad	Examinateur	UKM Ouargla

Année : 2016/2017

Remerciement

En premier lieu je remercie ***DIEU*** *le tout puissant, le créateur, qui nous a facilité le chemin, et nous a donné la persévérance pour réaliser ce modeste travail; pour la deuxième fois louange à DIEU.*

*Je tiens à remercier en cette occasion tout le corps professoral et administratif de département d'informatique de l'****université Kasdi Merbah*** *de Ouargla pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.*

Je tiens à remercier sincèrement ***Dr Amine KHALDI*** *qui, en tant que encadreur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'orientation, la confiance, l'aide et le temps qu'il a bien voulu me consacrer et sans eux ce mémoire n'aurait jamais vu le jour.*

Je remercie également les membres de jury de me faire l'honneur de juger mon travail.

Je tiens à remercier ***Naam M.T*** *et* ***Mohammed BENSALM*** *pour vos efforts au cours de la période de préparation de mémoire à Dieu de faire dans l'équilibre de vos bonnes actions.*

Enfin, mes plus chaleureux remerciements pour toute personne ayant participé de prés ou de loin à la réalisation de ce modeste travail.

Anissa

Dédicace

Je dédie ce modeste travail :

A la mémoire de mon cher papa ***Aissa*** *qui était et restera toujours mon grand exemple, et sa chaleur paternelle a été toujours pour moi un grand réconfort ; Qu'Allah bénisse son âme.*

A ma chère maman ***Z. Zehari*** *qui n'a jamais cessé de ménager ses efforts pour que j'atteigne ce niveau. Ses sacrifices et privations ne l'ont pas empêchée d'accomplir son devoir de mères soucieuses de l'avenir de ses enfants.*

A ma sœur ***M*** *que je lui souhaiterai le succès dans sa étudiée et qu'elle aura un avenir scientifique prospère.*

Et mes frères ***Mohammed Taher, Mohammed Abed Alghani*** *et* ***Messaoud*** *pour leurs affections, compréhension et patience.*

Je dédie également ce travail à la mémoire de mon cher et ma chère défunte grand père et grand-mère « ***Massaoud*** et ***Ladjel Massaouda*** *» que Dieu ait leur âmes et l''accueillent en Son Vaste Paradis.*

Je dédie également ce travail à la mémoire de mon cher et ma chère Grand-père et grand-mère « ***Zehari CH et G.H****».*

A ma grande famille grande et petite, mes chères tantes et mes chers oncles, mes chers cousins et cousines et à ma sœur ***Sondos ALKHADEUR*** *qui m'a toujours encouragé ; je lui souhaite une bonne chance dans ses aviez.*

A mes ami (e)s et tous mes collègues de la promotion de master 2
« Industrielle », « Fondamental », «Réseaux Convergence et Sécurité».

Je tiens à remercier sincèrement et dédie également ce travail à

la mémoire de mon cher ***Dr Zehari Ossama Chikh.***

Table des matières

Chapitre II: La cryptographie

Chapitre III: Conception et réalisation

Liste des figures

Liste des tableaux

Liste des tableaux

Introduction générale

Introduction générale

Les applications multimédia interactives fournissent des environnements de communication très complets pouvant être utilisés dans le cadre du travail collaboratif synchrone ou encore dans un contexte ludique et familial. Cela va de la communication audio et/ou vidéo jusqu'aux applications partagées, en passant par les tableaux blancs. Ces applications, par leur aspect interactif, requièrent un service de qualité du système de communication sous jacent afin de fonctionner correctement. Au niveau réseau, ce service, variable selon les applications, s'exprime par exemple en termes de garanties sur le délai de bout en bout, le débit de transmission ou encore le taux de perte d'information.

Le problème d'échange de données secrètes a toujours existé, et ce depuis la naissance des grandes civilisations. Les problèmes de qualité de transmission de la VoIP : La VoIP étant transportée par " paquets ", certains peuvent s'égarer en route. Dans ce scenario le cryptage permet en utilisent un algorithme de chiffrage de protéger des données, celles-ci devenant illisibles. Pour les lire, il suffit de posséder le mot passe, ou une clef qui a servi à les crypter, ou un certificat qui permet d'assurer l'authenticité de la provenance des données reçues via son navigateur. Pour échanger des données secrètes.

La ToIP consiste donc en un ensemble de techniques qui, dans une entreprise ou un organisme, permettent la mise en place des services téléphoniques sur un réseau IP en utilisant la technique de la Voix sur IP (« *Voice over IP* » ou VoIP) pour la transmission de messages vocaux sur des réseaux de données à paquets utilisant le protocole IP. ToIP est de fait la première alternative réelle aux réseaux traditionnels de téléphonie qui utilisent une technologie dite de commutation de circuits (*voice switching*) vieille de plus de 100 ans.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

Dans notre travail nous allons réaliser une application de VOIP chiffrée, pour cela les deux interlocuteurs effectuerons un échange de clé Diffie-Hellman qui leur permettra de généré une clé commune, l'échange se fera via l'envoie de messages de synchronisation et ceux dés le

passage de l'appel. Et âpres de communiquer, c'est cette clé qui sera utilise comme une clé secret pour chiffrées les conversations avec un algorithme symétrique (AES).

L'utilisation un échange de clé Diffie-Hellman et un algorithme symétrique AES, dans notre VoIP pour crée un canal sécurisé par ce que la cryptographie sert à préserver la confidentialité des données aussi à garantir leur intégrité et leur authenticité.

Notre travaille va s'étendre sur trois chapitres respectivement intitulés et détaillés comme suit :

Dans le premier chapitre nous allons présenter la technologie TOIP et VOIP et ses caractéristiques ainsi que les différente technique d'acheminement de la voix via le protocole IP. Nous abonderons aussi les faiblesses de cette nouvelle technologie fine de prévoir des protocoles de sécurisation TOIP.

Le deuxième chapitre porte sur la cryptographie et ses mécanismes ainsi que les systèmes de chiffrements qui permettent les différentes familles cryptographiques.

Dans le troisième et dernier chapitre nous présenterons notre application ainsi que les outils nécessaire à sa réalisation et les expérimentations effectuées.

Enfin, nous avons conclu notre mémoire par une conclusion générale et nous avons exposé les perspectives pour de futurs travaux.

Chapitre I :

La téléphonie sur IP (TOIP)

I.1- Introduction

L'émergence de nouvelles technologies peut parfois être effrayante pour les entreprises qui ne savent pas toujours déterminer la voie à suivre. Bien souvent, elles sont en retard dans l'évolution de leurs réseaux ou de leur matériel informatique. Aujourd'hui, des standards sont en train d'émerger et des entreprises commencent à satisfaire le marché en fournissant des passerelles faisant le lien entre le monde IP et le monde RTCP.

Le but de la téléphonie sur IP est de finaliser la convergence voix/données autour d'un protocole unique IP. En effet, la téléphonie IP se base sur la même architecture que l'Internet et utilise les mêmes infrastructures. De plus en plus d'entreprises sont équipées de réseaux LAN et peuvent donc tirer profit de la voix sur IP à moindre coût. En intégrant voix et données, la téléphonie IP simplifie l'administration du réseau car tout est centralisé dans un unique réseau. Elle procure aussi des facilités pour le développement d'applications utilisant de la voix et des données en téléphonie, tout est basé sur le matériel alors que la téléphonie IP tire avantage d'une architecture basée sur du logiciel.

Ce chapitre va présenter : quelque définitions importante aussi les caractéristiques de la TOIP et VOIP, une technique nécessaire pour la transmission de signal audio, ainsi que les déférents type de TOIP son architecture dans les entreprises et nous aborderons aussi les faiblesse de cette nouvelle technologie a fin de prévoir les protocoles de sécurisation TOIP.

I.2- La téléphonie sur IP

Depuis les années quatre-vingt, les éditeurs de logiciels cherchent à utiliser le réseau informatique pour y véhiculer de la voix. Suite à l'apparition de protocoles comme H.323 ou SIP, les constructeurs d'autocommutateurs ont progressivement intégré cette dimension IP à leurs solutions dans une optique de convergence voix-données. Dans un premier temps, cette convergence a pris la forme de cartes optionnelles à intégrer dans les PABX (« *Private Automatic Branch eXchange* ») existants, pour être proposée aujourd'hui de façon native. C'est ce qu'on appelle la Téléphonie sur IP (« *Telephony over IP* » ou ToIP). La ToIP consiste donc en un ensemble de techniques qui, dans une entreprise ou un organisme, permettent la mise en place des services téléphoniques sur [1] un réseau IP en utilisant la technique de la Voix sur IP (« *Voice over IP* » ou VoIP) pour la transmission de messages vocaux sur des réseaux de données à paquets utilisant le protocole IP. ToIP est de fait la première alternative réelle aux réseaux traditionnels de téléphonie qui utilisent une technologie dite de commutation de circuits (*voice switching*) vieille de plus de 100 ans.

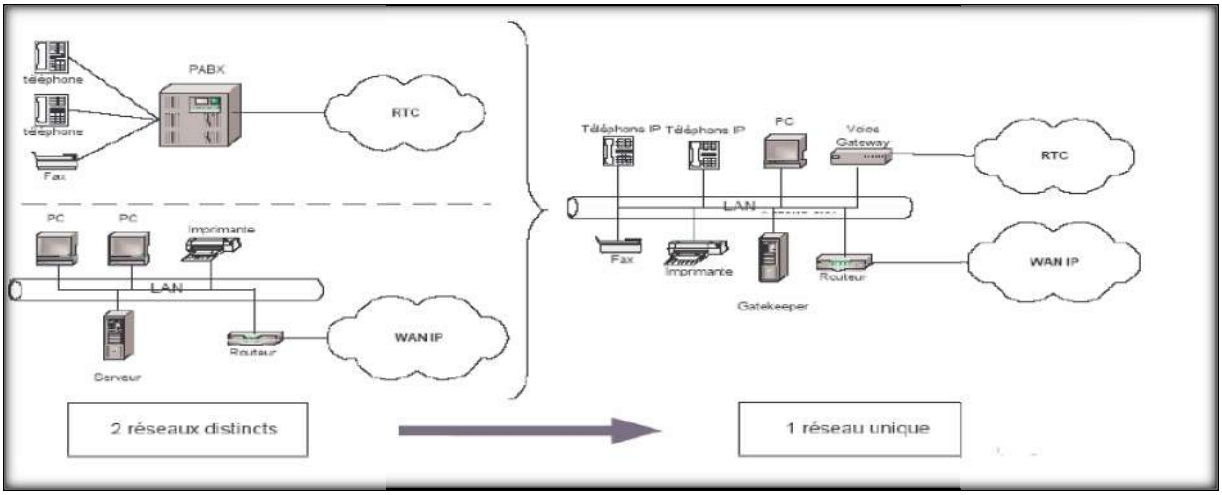

Figure I. 1: Schéma de convergence des réseaux.

ToIP n'est pas de la téléphonie sur Internet, malgré une confusion souvent entretenue dans les médias. Le terme « Téléphonie sur Internet » est spécifiquement utilisé lorsqu'on se sert du grand réseau public Internet pour établir des communications téléphoniques. L'Internet que nous utilisons tous les jours est un réseau de réseaux qu'aucune organisation ne contrôle ou ne gère dans son ensemble. Il n'y pas de garantie de qualité de service.

Au contraire, la téléphonie sur IP est confiée à un réseau géré par une entité unique, une entreprise pour ses besoins internes ou un opérateur télécom. La différence en terme de qualité de service est énorme or, la voix est très sensible à tout retard dans la diffusion du signal. C'est ainsi que nous avons souffert de la piètre qualité des appels téléphoniques transatlantiques transmis par satellite car le temps de retour du signal depuis le satellite produisait un écho nuisible à la qualité de la conversation. Pour être exhaustif, mentionnons le fait qu'il était déjà possible de faire passer de la voix sur des réseaux de données à paquets tels que Frame Relay (« *Voice over Frame Relay* » ou VoFR) ou ATM (« *Voice over ATM* » ou VoATM), ce qui permet de garantir la transmission de bout en bout de l'intégralité des paquets et qui plus est dans l'ordre d'émission. Mais pour autant, ces dernières technologies n'ont jamais atteint une échelle vraiment significative. [1]

I.2.1 - Téléphonie sur IP, ou Voix sur IP

Avant d'entrer dans les détails des différents atouts de la ToIP, il est nécessaire de la distinguer de la VoIP. Dans les deux cas, nous parlons d'équipements et de mécanismes permettant de transporter de la voix sur un réseau de données de type IP (*Internet Protocol*).

Dans le cas de la VoIP, on se contente d'interconnecter des PABXs en capsulant la voix numérisée, dans les paquets IP. Ces derniers sont ensuite véhiculés au sein du réseau de

données, de manière classique, comme des paquets de données. La voix est simplement « reconstituée » lorsque les paquets arrivent chez le destinataire. Un exemple « parlant » de VoIP se trouve dans le raccordement de deux sites via une ligne spécialisée qui transporte la voix et les données. Quant à la ToIP, elle va plus loin que la VoIP en terme de mécanismes et d'équipement, cherchant à apporter aux utilisateurs la qualité de service (qualité de transmission, qualité de voix, disponibilité du service) et les services que ces derniers sont l'habitude trouver du côté de la téléphonie classique (présentation du numéro, transfert d'appel, conférence, etc.) le tout sans faire appel aux PABXs.

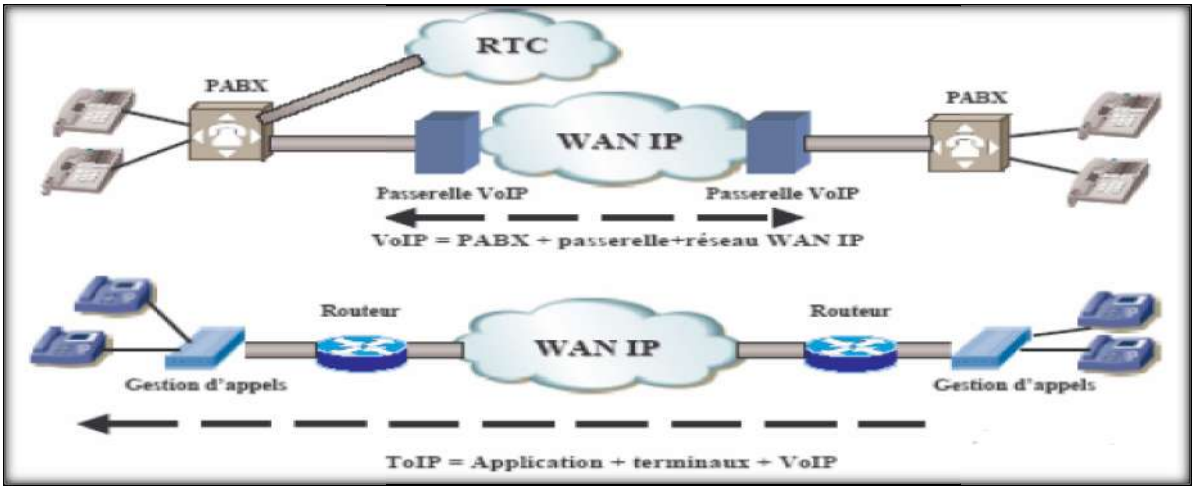

***Figure I. 2*:**Périmètres comparés de la VoIP et de la ToIP.

La VoIP est donc une composante de la ToIP et sa sécurisation est, par conséquent, la condition sine qua non de la sécurisation de la ToIP. Similairement au cas de la téléphonie, il faut distinguer la voix sur IP de la voix sur Internet, dépendamment du réseau IP utilisé pour le transport des paquets de la voix : s'il s'agit d'un réseau IP privé ou du réseau des réseaux, l'Internet. Il est aussi à noter que dans le cadre [1] de la téléphonie sur IP, l'on distingue la téléphonie fixe sur IP et la téléphonie mobile sur IP.

I.3 - La Voix sur IP

I.3.2 - Transmission de la voix en mode paquet

La téléphonie sur IP est une transmission de la voix en mode paquets au format TCP/UDP. Pour comprendre le traitement complexe de la voix analogique (signaux électriques) en signaux binaires, voici un synoptique explicatif :

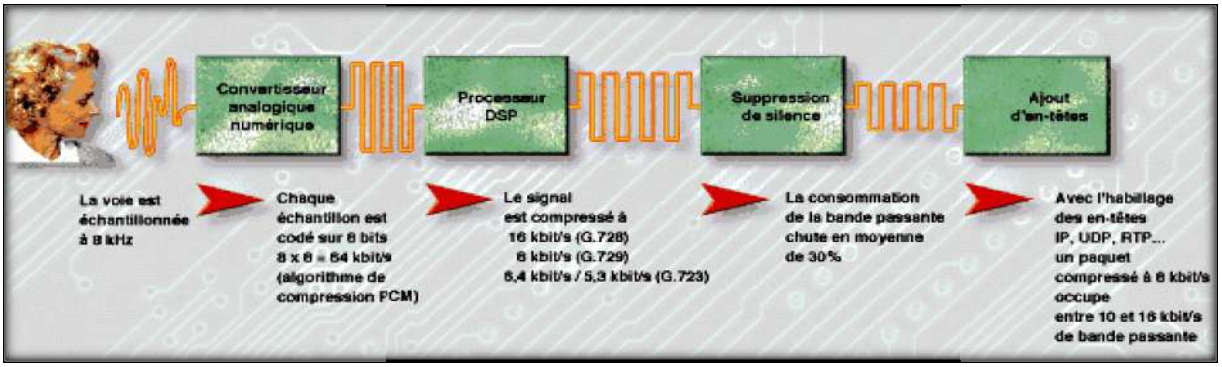

Figure I. 3:Synoptique de transmission de la voix analogique en mode paquet.

Explications du Synoptique : La bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz, elle est d'abord échantillonné numériquement par un convertisseur puis codé sur 8 bits, puis compressé par les fameux codecs (il s'agit de processeurs DSP) selon une certaine norme de compression variable selon les codecs utilisés, puis ensuite on peut éventuellement supprimer les pauses de silences observés lors d'une conversation, pour être ensuite habillé RTP,UDP et enfin en IP. Une fois que la voix est transformée en paquets IP, ces petits paquets IP identifiés et numérotés peuvent transités sur n'importe quel réseau IP (ADSL, Ethernet, Satellite, routeurs, switchs, PC, Wifi, etc...) [2]. A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine. [3]

I.3.3 - Les différents codecs et taux de compression

Le mot Codec vient du résultat de fusion des deux mots (**Co**deur/**Déc**odeur), son rôle est de compresser et décompresser un signal que ça soit analogique ou numérique, en un format de données. La finalité d'utiliser un codec est de diminuer l'utilisation de la bande passante lors du traitement d'un nombre important de données. Nous pouvons diviser les codecs en deux grandes catégories, suivant leurs manières de compresser/décompresser les données :

- ✓ ***La compression non-destructive*** : permet de retrouver le signal initial tel qu'il était avant le codage.
- ✓ ***La compression destructive*** : prend en compte les caractéristiques des données à compresser et peut retirer les informations les moins importantes du signal.

Les principaux taux de compression de la voix sont les codecs officiels suivants : [4] [5]

Tableau I. 1:Comparatif des caractéristiques des CoDecs ITU-T courants.

CoDec	Débit binaire (Kbps)	Délai de codage (ms)	MOS ou Qualité auditive perçue
G.711 PCM	64	0,125	4,1
G.726 ADPCM	32	0,125	3,85
G.728 LD-CELP	15	0,125	3,61
G.729 CS-ACELP	8	10	3,92
G.729a CS-ACELP	8	10	3,7
G.723.1 MP-MLQ	6,3	30	3,9
G.723.1 ACELP	5,3	30	3,65

Les différents codecs [6] retransmettent plus ou moins bien le signal original. Pour mesurer la qualité de la voix restituée, on parle de score MOS (Mean Opinion Score). C'est une note comprise entre 1 et 5 et attribuée par des auditeurs jugeant de la qualité de ce qu'ils entendent.

I.3.4 - Les contraintes de la VoIP

Les trois principales causes des difficultés et des limites associées à VoIP sont : le délai de latence, la gigue et le taux de perte des paquets.

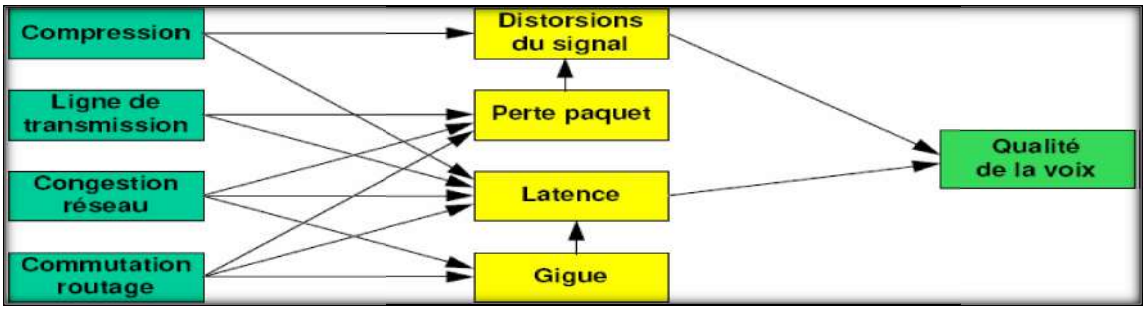

Figure I. 4:Les contraintes de la VoIP.

I.3.4. A- Le délai de latence

La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho (similaire aux désagréments causés par les conversations par satellites, désormais largement remplacés par les câbles pour ce type d'usage). Or la durée de traversée d'un réseau IP dépend de nombreux facteurs:

- ✓ Le débit de transmission sur chaque lien.
- ✓ Le nombre d'éléments réseaux traversés.
- ✓ Le temps de traversée de chaque élément, qui est lui même fonction de la puissance et la charge de ce dernier, du temps de mise en file d'attente des paquets, et du temps d'accès en sortie de l'élément.

- ✓ Le délai de propagation de l'information, qui est non négligeable si on communique à l'opposé de la terre. Une transmission par fibre optique, à l'opposé de la terre, dure environ 70 ms. [7]

I.3.4. B - La gigue *(ou « Jitter »)*

La variation de temps de transit, ou gigue de phase, est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Cela crée une déformation de la voix ou un hachage. La gigue de phase est indépendante du délai de transit. Le délai peut être court et la gigue importante ou inversement. La gigue est une conséquence de congestions passagères sur le réseau, ce dernier ne pouvant plus transporter les données de manière constante dans le temps. La valeur de la gigue va de quelques ms à quelques dizaines de ms. [8]

I.3.4. C - Le taux de perte des paquets

Lorsque les routeurs IP sont congestionnés, ils libèrent automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrants en fonction de seuils prédéfinis. La perte de paquets est préjudiciable, car il est impossible de réémettre un paquet voix perdu, compte tenu du temps dont on dispose. Le moyen le plus efficace de lutter contre la perte d'informations consiste à transmettre des informations redondantes (code correcteur d'erreurs), qui vont permettre de reconstituer l'information perdue. Des codes correcteurs d'erreurs, comme le Reed Solomon, permettent de fonctionner sur des lignes présentant un taux d'erreur de l'ordre de 15 ou 20 %. Une fois de plus, ces codes correcteurs d'erreurs présentent l'inconvénient d'introduire une latence supplémentaire. Certains, très sophistiqués, ont une latence très faible. [9]

I.4 - Architectures de ToIP

Trois grandes familles de ToIP traduisent le taux de convergence des réseaux voix-données [10,11] :

- ✓ La famille « de poste informatique à poste informatique » ;
- ✓ La famille « de poste informatique à téléphone » ;
- ✓ La famille « de téléphone à téléphone ».

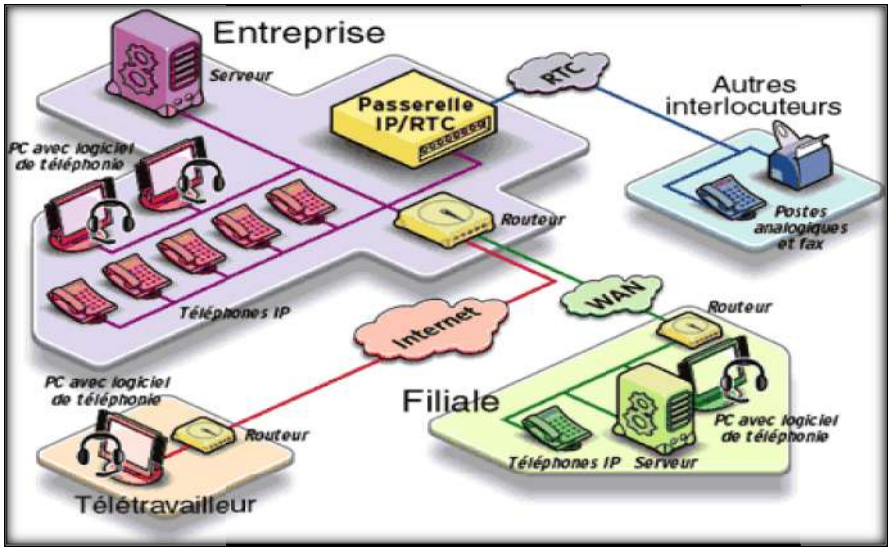

Figure I. 5:Convergence des réseaux voix-données.

I.4.1 - De poste informatique à poste informatique

Dans ce scénario le but sera de transformer son ordinateur en un poste téléphonique en lui ajoutant une carte son full-duplex pour garantir une conversation simultanée, un micro et un logiciel de voix sur IP compatible. Le correspondant quant à lui, doit disposer des mêmes outils et surtout du même logiciel de téléphonie. A cet instant, le poste numérique, compresse et encapsule les échantillons de voix dans des paquets IP avant de les envoyer sur Internet. L'accès se fait via un fournisseur d'accès à internet IAP/ISP. Les deux modes de connexion possible pour ce cas sont ainsi :

- ✓ ***Connexion directe*** En composant l'adresse IP du correspondant. Les deux usagers doivent ainsi fixer un rendez-vous préalable, à moins qu'ils soient connectés en permanence.
- ✓ ***Connexion serveur*** En sélectionnant le correspondant sur une liste d'usagers en ligne. Si quelqu'un se connecte au réseau, ses coordonnées (email, IP, etc.) sont automatiquement inscrites dans l'annuaire en ligne.

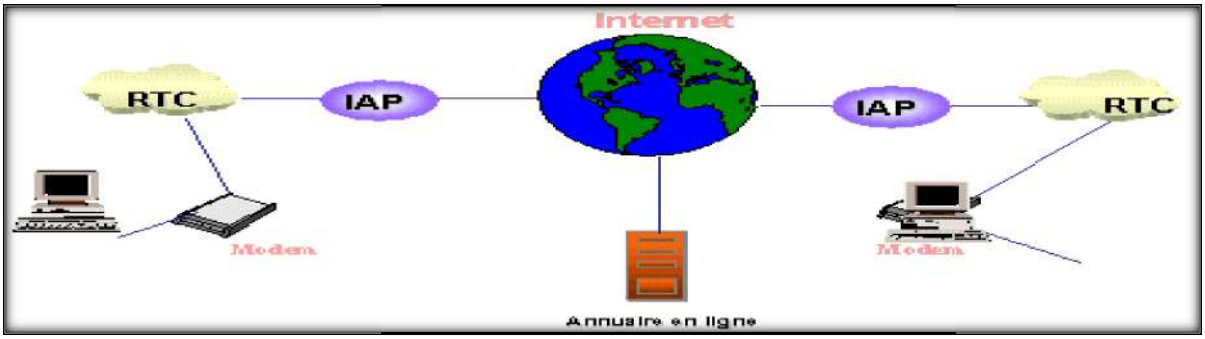

Figure I. 6:Téléphonie entre postes informatiques.

I.4.2 - De Poste informatique à téléphone (ou vice-versa)

Dans ce scénario, l'un des usagers dispose d'un ordinateur lui permettant de se connecter à internet via un réseau d'accès et un fournisseur d'accès à internet. Tandis que l'autre usager est un abonné normal d'un réseau téléphonique fixe ou mobile. Lorsque l'usager (disposant de l'ordinateur) souhaite appeler un correspondant sur un poste téléphonique, il doit d'abord se connecter à internet de manière classique grâce au réseau de voix ISP. Une fois connecté, il utilise le service d'un fournisseur de téléphonie sur internet ITSP qui opère une "passerelle" permettant d'accéder au plus prés du central téléphonique de l'abonné demandé. C'est cette passerelle qui se chargera de l'appel du correspondant et de l'ensemble de la signalisation relative à la communication téléphonique du coté du correspondant demandé.

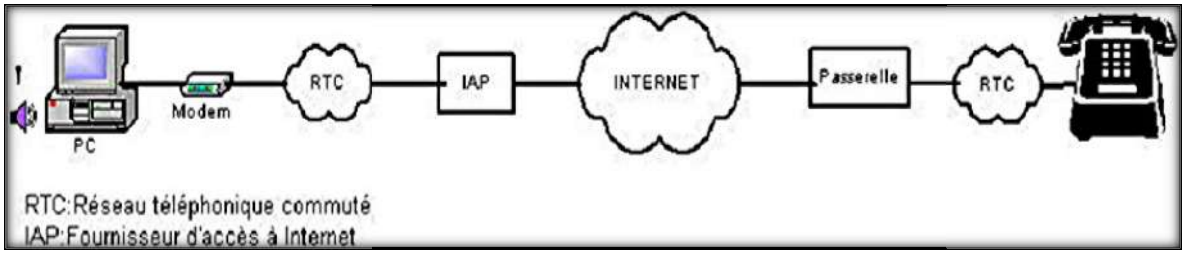

***Figure I. 7*:**Téléphonie entre poste informatique et téléphone.

I.4. 3 - De téléphone à téléphone

Dans ce cas l'appelant et l'appelé sont tous les deux des abonnées du réseau téléphonique commuté public (RTCP) et utilisent de manière classique leur appareil téléphonique pour la communication vocal. On peut distinguer deux méthodes pour faire dialoguer deux postes téléphoniques ordinaires via un réseau IP ou internet :

- ***En utilisant des passerelles :*** Dans ce cas, les passerelles ainsi que le réseau IP géré pourraient appartenir à des acteurs différents selon qu'il s'agit :

- ✓ D'un usage purement interne de la voix sur IP au sein du réseau d'un opérateur téléphonique unique (usagers A et B ainsi gérés).
- ✓ De la fourniture d'un service de voix longue distance par un opérateur longue distance utilisant la technologie de la voix sur IP (les usagers A et B appartenant alors à des réseaux distincts).

Figure I. 8:Téléphonie entre postes de téléphones.

- ***En utilisant des boitiers d'adaptation*** **:** Pour faire bénéficier de ce service, un certain nombre de sociétés commercialisent des boitiers ressemblant à des modems et qui s'interpose entre le poste téléphonique de l'usager et son branchement au réseau téléphonique public commuté. Le correspondant demandeur lance sa requête comme sur un réseau de télécommunication classique. La communication est d'ailleurs établie dans une première phase sur ce réseau mais, aussitôt après, les boîtiers s'échangent les informations nécessaires à la deuxième phase, la communication traditionnelle est alors rompue et les boîtiers établissent, grâce aux informations qu'ils se sont échangées et aux paramètres inscrits, une connexion de chacun des deux correspondants à son fournisseur respectif d'accès à internet. Une fois la communication établie, les boitiers assurent localement la conversion de la voix en paquets IP pouvant être transporté sur le réseau internet comme illustré ci-dessous.

Figure I. 9:Téléphonie entre postes de téléphones « boitier ».

I.5 - Les équipements clés d'une communication ToIP

Les principaux équipements d'une communication IP sont : les terminaux téléphoniques IP, le « *Gatekeeper* » et la « *Voice Gateway* ».

I.5.1 - Les terminaux téléphoniques

Dans le domaine des Télécommunications, un Terminal est un équipement situé en extrémité d'un Réseau de télécommunication, capable de communiquer sur ce réseau et souvent d'assurer l'interface avec l'utilisateur. [12]

I.5.1.A- Le « hardphone » IP

L'« *IP-phone* » ou « *hardphone* » :c'est un terminal téléphonique fonctionnant sur le réseau LAN IP à 10/100 avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs pour l'audio, et il peut disposer d'un écran monochrome ou couleur, et d'une ou plusieurs touches soit programmables, soit préprogrammées. IL est en général doté d'un hub passif à un seul port pour pouvoir alimenter le PC de l'utilisateur (l'IP-PHONE se raccorde sur la seule prise Ethernet mural et le PC se raccorde derrière l'IP-PHONE). [13]

Figure I. 10:Modèles de « hardphone » IP.

I.5.1.B - Le « Softphone » IP

Le Softphone **:** c'est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP. [13]

Figure I. 11:Modèles de « softphone » IP.

I.5.1.C - L'alimentation des postes IP

Un poste IP (ou « *IP-phone* ») a besoin d'une alimentation :

- ✓ Soit ***locale*** : le poste dispose alors d'une alimentation externe DC de 48Volts, ce qui nécessite l'utilisation d'un petit transformateur 220V~/48VDC pouvant être facilement oublié et débranché avec [1] une fausse manipulation.
- ✓ Soit ***distante*** : le poste est alors télé-alimenté :
  - Soit par le commutateur Ethernet selon la norme 802.3af d'IEEE Computer Society.
  - Soit par un équipement intermédiaire appelé MID-SPAN, situé entre le Switch et le panneau de câblage. Il est à noter qu'en cas de panne secteur, il n'y a plus de téléphone (c'est normal) et aucun appel d'urgences n'est donc possible.

I.5.2 - Les « gatekeeper »

Le « *gatekeeper* », ou garde-barrière, il effectue les translations d'adresses (identifiant H323 et @ IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action. [14]

I.5.3 - Les « voice gateway »

C'est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX (en QSIG, RNIS ou E&M), soit des opérateurs de télécommunications local, national ou international. Plusieurs passerelles peuvent faire partie d'un seul et même réseau, ou l'on peut également avoir une passerelle par réseau local (LAN). La passerelle peut également assurer l'interface de postes analogiques classiques qui pourront utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants). [14]

I.5.4 - Les équipements complémentaires

D'autres équipements peuvent entrer aussi dans la composition des réseaux de ToIP :

I.5.4.A- Le PABX-IP, PABX

Un PABX est un autocommutateur téléphonique privé (définition anglaise : Private Automatic Branch eXchange) destiné à alimenter et à mettre en relation une certaine quantité de postes téléphoniques internes dans une entreprise ou dans une administration. En d'autres termes, il représente l'élément central qui :

- Distribue les appels téléphoniques arrivés.
- Autorise les appels téléphoniques départs.
- Gère les terminaux téléphoniques qui peuvent être des postes numériques ou Analogiques.

- Gère toutes les autres fonctionnalités ou options (CTI, CSTA, Taxation...) Un PABX travaille aussi bien en numérique qu'en analogique. [15]

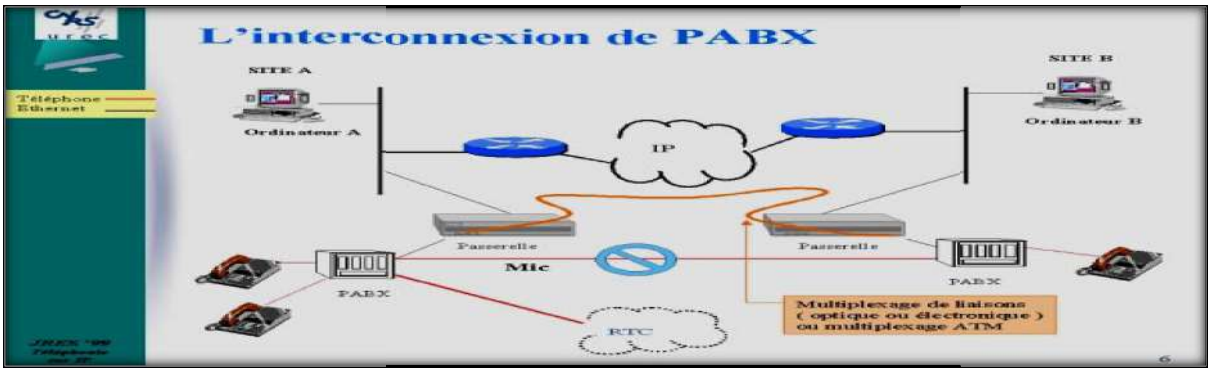

Figure I. 12:Interconnexion de PABX.

I.5.4.B- Le serveur de communications

Il gère les autorisations d'appels entre les terminaux IP ou softphone et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (gateway). [15]

I.5.4.C- le MCU « Multipoint Control Unit »

Est un composant très important d'un système de conférence multimédia**.** Il peut s'agir d'un appareil à part entière ou d'une fonctionnalité spécifique d'un poste de vidéoconférence. En effet, la notion de conférence étant implicitement associée à la collaboration de 3 participants ou plus, ceci implique une croissance exponentielle du nombre de connexions point à point à réaliser afin que chacun des participants puisse émettre et recevoir les flux audio, vidéo ou de partage de données.

C'est pour simplifier et optimiser la mise en œuvre d'une conférence que le MCU entre en piste. Sa tâche est de transformer la relation point à point qui existent entre chacun des participants en une relation point à point unique: une communication avec le MCU.

Chaque participant a alors pour seul et unique interlocuteur la conférence qui est créée au sein du MCU. [16]

I.6 - Les différents protocoles utilisés

Il existe [1] plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche pair-à-pair avec l'intelligence répartie à la périphérie (terminal de téléphonie IP,

passerelle avec le réseau téléphonique commuté...). Chacune à ses avantages et ses inconvénients, et ces diverses approches se déclinent au travers de différents protocoles. Les 3 protocoles utilisés pour la VoIP, à savoir :

• Le protocole H.323 ;

• Le protocole SIP ;

• Les protocoles pour terminaux simples : MCGP/MEGACO.

I.6.1 - Le protocole H.323

En 1996 naquît la première version voix sur IP appelée H323. Issu de l'organisation de standardisation européenne ITU-T sur la base des travaux de la série H.320 sur la visioconférence sur RNIS (signalisation voix Q.931), ce standard a été développé pour les centraux téléphoniques sur la base de PBX et a maintenant donné suite à de nombreuses évolutions, quelques nouveaux standards prenant d'autres orientations technologiques. En réalité, H.323 est une famille de protocoles constituant déjà une norme stabilisée ayant de nombreux produits sur le marché (terminaux, gatekeeper, gateway, logiciels) et existe actuellement en cinq versions (v.1 à v.5). [1]

I.6.2 - Le protocole SIP

En 1997, l'IETF conçoit un système de signalisation SIP (« *Session Initiation Protocol* ») adapté à la philosophie IP, contrairement à H.323 qui s'inspire des circuits télécoms. SIP se base en premier lieu sur le principe [1] de l'invitation à participer à une session. C'est un protocole svelte, basé sur le texte (similaire à e-mail ou http : « *HTTP-like* »), permettant l'implémentation dans un environnement IP. A l'heure actuelle, il est moins riche que H.323 au niveau des services offerts, mais il suscite un très grand intérêt dans la communauté Internet et télécom et entre donc en concurrence directe avec H.323.

I.7.3 - Les protocoles pour terminaux simples : MCGP/MEGACO

Le protocole MGCP « *Media Gateway to Media Controller Protocols* » a été introduit par l'IETF. Il est complémentaire à H.323 ou SIP et traite des problèmes d'interconnexion avec le monde téléphonique.

Le protocole Megaco « *Media Gateway Control* » a été défini à la fois à l'IETF (RFC 3015) et à l'ITU (recommandation H.248). Il constitue une évolution de l'ancien MGCP. Comme son développé en anglais le suggère, [1] la centralisation des fonctions téléphoniques

est effectué dans le contrôleur de passerelle de média (serveur) ; l'équipement d'utilisateur (téléphone IP et/ou passerelle de média) ne prend en charge que les fonctions de base comme le codage et la mise en paquets de la voix.

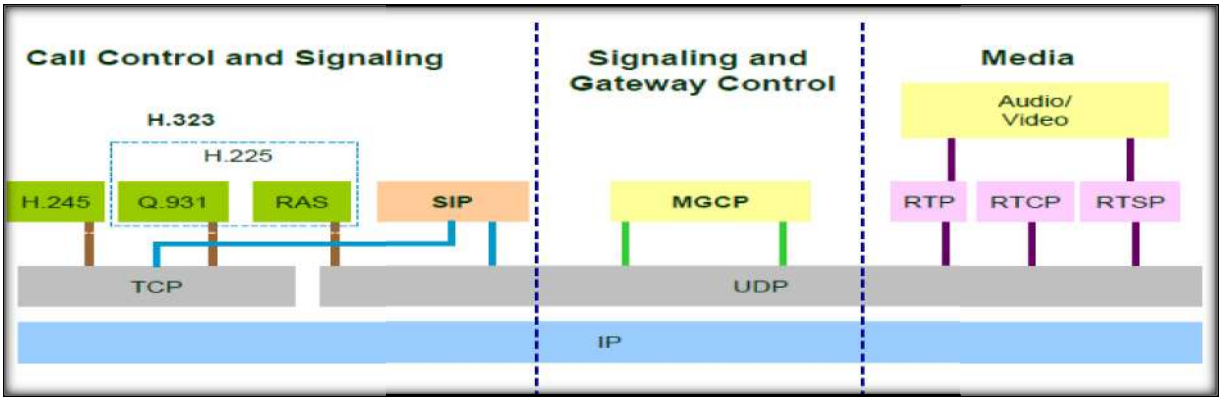

Figure I. 13:Les différents protocoles utilisés pour la VoIP.

I.7 - Les faiblesses de la Téléphonie sur IP

Pour gagner sa place parmi les applications d'entreprises, la technologie ToIP devra d'abord résoudre ses insuffisances techniques. Tour d'horizon de ses principaux ***points faibles.*** [17]

I.7.1 – Fiabilité

VoIP n'est pas encore suffisamment fiable et le protocole IP en est le principal responsable. De larges segments de la population Internet utilisent des versions IP, comme la version IPv4 qui ne fournit pas un bon support pour un routage fiable. Or la question est la suivante : combien de temps accepte-t-on d'attendre la tonalité lorsque l'on décroche le téléphone ? Tant qu'IPv6, la future génération de protocole IP, n'est pas largement implémentée, VoIP ne sera pas une option intéressante pour les entreprises. Il faudrait l'utiliser avec d'autres solutions hybrides qui combinent l'IP avec des protocoles plus fiables, comme l'ATM. Bien qu'IPv6 soit déjà intégré à un certain nombre de solutions Internet et à des systèmes d'exploitation comme Linux, peu d'entreprises ont migré de l'IPv4 à l'IPv6. Mais cela devrait changer dans les trois années à venir, où nous assisterons à l'utilisation conjointe d'IPv4 et d'IPv6 sur Internet, le temps que les entreprises mettent à jour leurs équipements. [17]

I.7.2 - Une qualité de son médiocre

Pour le moment, il n'y a pas de garantie de qualité sonore pour la VoIP. Elle est souvent plus mauvaise que celle d'un téléphone cellulaire utilisé dans une zone à la couverture

médiocre... La qualité des liaisons téléphoniques sur réseau IP dépend en grande partie de la qualité de la maintenance et du suivi. Les temps de latence sur le réseau, la perte de paquets de données vocales, les problèmes de compression, l'écho et un résultat sonore peu fidèle affaiblissent grandement la qualité sonore de la VoIP et sont donc des paramètres à maîtriser. La tâche devrait être facilitée avec l'implémentation à grande échelle d'IPv6 d'ici les trois prochaines années, et l'intégration des dernières normes de qualité de service et des nouveaux standards par des organismes regroupant des industriels des télécoms. [17]

I.7.3 - Améliorer l'utilisation

VoIP doit offrir des fonctionnalités telles que la mise en attente d'un appel et l'identification de l'appelant, des services de base de la téléphonie traditionnelle. Aujourd'hui, l'implémentation de la VoIP nécessite souvent que l'appelant tape jusqu'à 25 chiffres (numéro d'accès, numéro d'identification personnel, code et numéro de téléphone du destinataire) avant de pouvoir passer son appel. Tant que VoIP ne peut pas proposer la facilité d'utilisation et les services fournis par les systèmes vocaux traditionnels, il aura du mal à convaincre les entreprises. [17]

I.7.4 – Localisation

Le nombre et la localisation des passerelles IP, qui fournissent les services de routage VoIP, limitent également le développement de la VoIP. Les fournisseurs de service doivent supporter un nombre suffisant de passerelles situées dans les zones de gros trafic pour réussir à faire des économies de coûts. Mais ce sont notamment les clients internationaux qui seront pénalisés : le manque de passerelles signifie que les fournisseurs d'accès Internet sont obligés d'acheter et de revendre des services de routage via une autre entreprise (particulièrement pour les routages longue distance). Les coûts de la solution VoIP augmentent d'autant. [17]

I.7.5 – Standards

La ToIP dépend *principalement* du standard H.323, qui permet de mélanger la voix, la vidéo et les données. Cependant, le H.323 est un standard globalement difficile à implémenter pour les fournisseurs VoIP. Bien souvent, ils choisissent une solution propriétaire afin d'obtenir un déploiement plus rapide. Ce qui peut entraîner des problèmes d'interopérabilité pour les utilisateurs. [17]

I.7.6 - Support administratif

Les systèmes administratifs de comptabilité, de facturation et de gestion du réseau pour la ToIP doivent être implémentés à des niveaux qui sont au moins parallèles à ceux de la téléphonie traditionnelle. Mais pour l'instant, ces derniers détiennent l'avantage dans le domaine des systèmes administratifs évolutifs qui gèrent les services administratifs. [17]

I.8- La sécurisation de la VoIP

La figure I.14 montre les différents protocoles de sécurité utilisés pour transporter et sécuriser une communication VoIP basée sur les normes de la famille H.323. H.235 définit les conditions de sécurité dans un environnement H.323 où TLS est utilisé pour sécuriser le canal de signalisation. Le trafic de voix se sert du transport RTP pour des communications de bout-en-bout entre des points terminaux. Par conséquent, il peut utiliser SRTP pour sécuriser les paquets de voix. Les trafics de ***signalisation*** et de voix peuvent être sécurisés avec IPSec. [1]

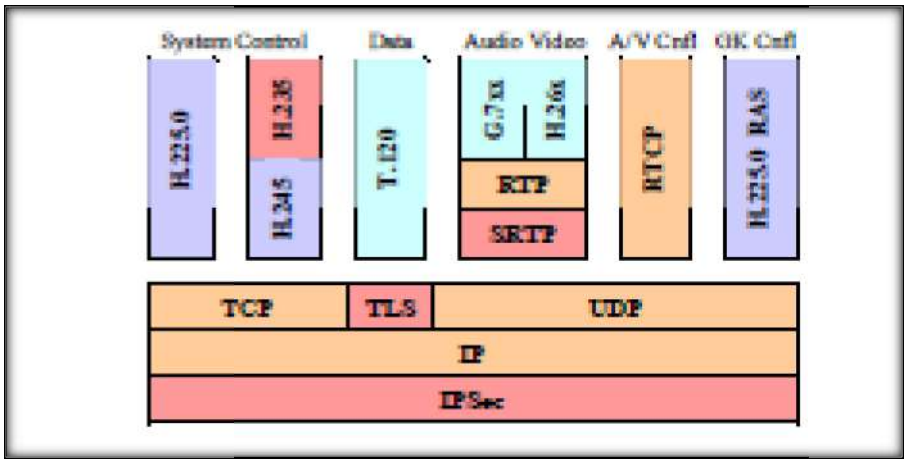

Figure I. 14: Les différents protocoles de sécurité.

I.8.1 - La sécurité avec H.235

H.235 est la partie sécurité du standard H.323, préparé par le groupe d'études numéro 16 de l'ITU-T. Son but est de fournir un support pour les fonctionnalités essentielles de sécurité dans les communications H.323, comme l'*authentification*, la *confidentialité*, l'*intégrité* et parfois la *non répudiation*, dépendamment du profil utilisé.

En effet, la recommandation H.235 propose en annexe des profils de sécurité qui utilisent les champs de H.235 pour fournir des services de sécurité au trafic H.323 en se basant sur des clés symétriques, sur des signatures digitales, ou sur des PKI.

Cependant, [1] cette recommandation n'est pas un standard de sécurité en elle-même. Pour assurer des mécanismes de sécurité pour la voix et pour la signalisation, elle repose sur des solutions de sécurité déjà existante, comme IPSec ou TLS et de plus, elle ne traite pas tous les problèmes de la sécurité.

I.8.2 - La sécurité avec IPSec

Le protocole IPSec est une suite de protocoles désignés pour sécuriser les communications au niveau de la couche réseau. La suite de protocoles est constamment en évolution depuis 1995. De nouveaux drafts sont proposés au sein du groupe de travail à l'IETF. IPSec propose deux protocoles de sécurité du trafic IP : *Authentication Header* (*AH*) et *Encapsulating Security Payload* (*ESP*). Chaque protocole AH ou ESP peut fonctionner en mode transport ou en mode tunnel :

- ✓ ***Le mode transport :*** réalise une simple encapsulation sans changement d'entête. Ce mode protège uniquement le contenu du paquet IP et pas son en-tête. Il n'est utilisable que sur les équipements terminaux (serveurs, postes clients) ;
- ✓ ***Le mode tunnel*** :est utilisé par les équipements réseaux pour les applications VPN. Il réalise une encapsulation plus complète avec changement de l'entête d'origine du datagramme. Ce mode protège la totalité du paquet IP.

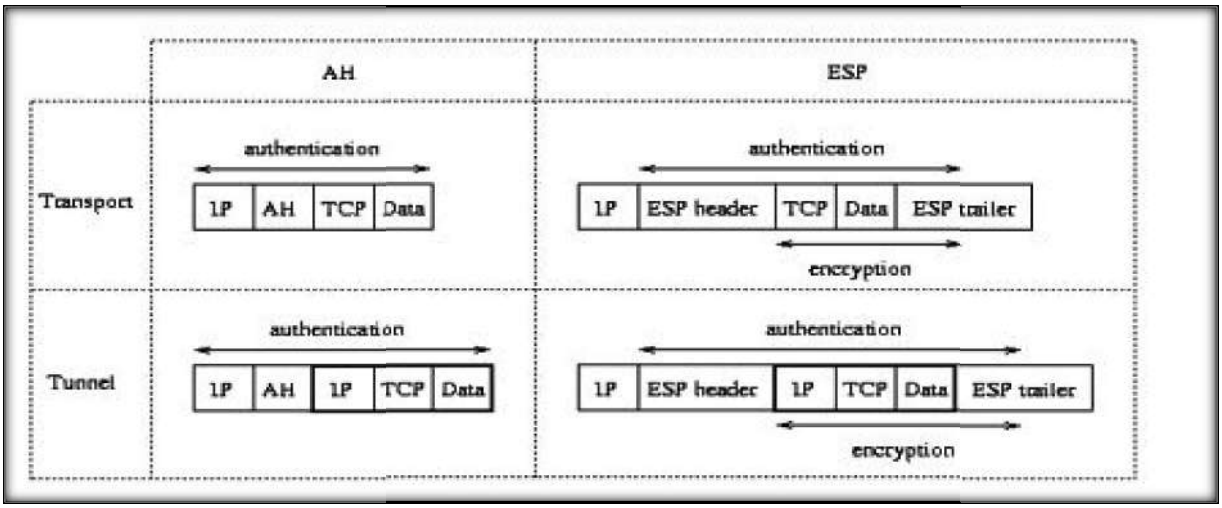

Figure I. 15:Les Protocoles AH et ESP en mode transport et en mode tunnel.

Ci suit les services de sécurité offerts par les deux protocoles d'IPSec :

- ✓ ***En ce qui concerne l'authentification des données,*** elle est assurée de la même façon avec AH et ESP à la seule différence que dans le mode *transport* de ESP, l'entête IP est transmise en clair et n'est pas couverte par la fonction d'authentification. Voici

alors comment est assurée l'*authentification* des données avec le protocole AH : elle l'est par le mécanisme de l'entête AH (champ donnée d'authentification, etc.). AH calcule une fonction d'authentification sur tout le datagramme IP en utilisant une clé secrète d'authentification. L'algorithme d'authentification appliqué est négocié dans une association de sécurité. L'émetteur calcule une donnée d'authentification avant d'envoyer le paquet IP authentifié. Le récepteur vérifie les données authentifiées à la réception. Certains champs du paquet IP (TTL (IPv4), Hop Limit (IPv6)) en transit sur le parcours entre l'émetteur et le récepteur et qui doivent changer de valeur ne seront pas inclus dans le calcul de la fonction d'authentification assurée par le protocole AH. Ces champs-là n'influencent pas la sécurité assurée au paquet authentifié. L'algorithme d'authentification par défaut utilisé par AH est le MD5. L'utilisation de AH augmente le temps de traitement au niveau du processeur ainsi que le délai dû au calcul des données d'authentification par l'émetteur et au calcul et comparaison des données d'authentification par le récepteur.

- ✓ ***Le protocole ESP assure la confidentialité*** et ce par le chiffrement des données utiles jusqu'au champ *NEXT* inclus (ce champ contient un identifiant du protocole de niveau supérieur). L'algorithme de cryptage appliqué est négocié dans une association de sécurité. ESP est désigné pour être utilisé avec des algorithmes de cryptage symétrique. Puisque les paquets IP n'arrivent pas en séquence chez le récepteur, chaque paquet IP doit transporter des données spécifiques de synchronisation cryptographique nécessaires au déchiffrement. L'algorithme de cryptage utilisé peut être par bloc ou par flux. ESP introduit de la complexité au niveau de l'utilisateur lors de son implémentation.

- ✓ ***Les deux protocoles AH et ESP assure l'intégrité*** de la même façon, en mode non connecté. Elle est obtenue par calcul de la valeur d'un ICV (*Integrity Check Value*) sur certains champs de l'entête IP, sur l'entête AH (ou ESP) et sur les protocoles de niveau supérieur encapsulés dans ce paquet IPSec. L'algorithme utilisé pour le calcul de ICV est basé sur un algorithme à clé symétrique (DES) ou sur une fonction de hachage à sens unidirectionnel (MD5 ou SHA-1).

- ✓ ***La protection contre le rejeu est définie dans IPSec de façon optionnelle*** : elle est négociée à la demande du récepteur dans une association de sécurité et est assurée de

la même façon avec AH et ESP par le numéro de séquence inclus dans l'entête de AH (ou ESP). Ce numéro s'incrémente avec chaque émission d'un paquet IPSec ;

- ✓ ***Seulement le protocole AH garantit la non-répudiation***, qui peut être présente par l'utilisation de certains algorithmes d'authentification (algorithme aysmétrique RSA où les clés de l'émetteur et du récepteur sont utilisées dans le calcul des données d'authentification) lors de l'application du protocole.

Il est à signaler qu'une implémentation IPsec gère une base de données des associations de sécurité (SAs). Une association de sécurité détient la façon de traiter un paquet IP, elle est unidirectionnelle. Pour assurer la sécurité de la communication entre deux entités, deux associations de sécurité seront négociées. Les informations incluent des paramètres tels la transformée de cryptage et les clés, etc. Par ailleurs, deux facteurs principaux affectent la transmission de la voix quand IPSec est utilisé :

- ✓ L'augmentation de la taille des paquets, essentiellement causée par les entêtes ESP et le nouvel en-tête IP nécessaire pour le tunnel.
- ✓ Le temps nécessaire pour crypter les en-têtes et les données utiles et la construction de nouveaux paquets.

D'un point de vue pratique, IPSec est un protocole relativement difficile à implémenter d'une part à cause de sa complexité intrinsèque (multiples sous-protocoles...) et d'autre part à cause de ses interactions avec les processus réseaux courants. Cela rend ce standard assez lourd et compliqué à implémenter et à maintenir dans un environnement de la téléphonie sur IP. [1]

I.8.3 - La sécurité avec TLS

Le protocole de sécurité de la couche transport (TLS) est une norme ouverte de l'IETF, conséquence naturelle de SSL (*Secure Sockets Layer*). TLS repose actuellement au-dessus de la couche transport et fournit la sécurité du niveau applicatif pour les communications. Un avantage de TLS est qu'il est indépendant du protocole d'application. TLS fournit des facilités pour l'authentification, l'intégrité et l'intimité entre les entités communicantes. L'utilisation de TLS exige un mécanisme fiable de transport tel que le TCP et donc TLS ne fonctionne pas au-dessus de UDP. L'implication évidente pour la téléphonie sur IP est la signalisation basée sur TCP et d'autres communications hors-bande peuvent se servir de TLS mais la signalisation non basée sur TCP et les flots de médias basés sur UDP ne le peuvent

pas. Puisqu'il exige une couche de transport sous-jacente appropriée (c.-à-d. pas UDP), TLS ne peut pas sécuriser le flot de médias.

Les protocoles de niveau plus élevé peuvent reposer sur le protocole TLS d'une manière transparente. La norme TLS, cependant, n'indique pas comment les protocoles ajoutent la sécurité avec TLS ; les décisions sur la façon d'initier le handshaking de TLS et la façon d'interpréter les certificats d'authentification échangés sont laissés au jugement des concepteurs et de ceux qui implémentent des protocoles fonctionnant au-dessus de TLS.

TLS soutient trois modes d'authentification :

- ✓ L'authentification des deux parties ;
- ✓ L'authentification du serveur avec un client non authentifié ;
- ✓ L'anonymat total.

Si le serveur est authentifié, son message de certificat doit fournir une chaîne de certificat valide, menant à une autorité de certification acceptable. De même, les clients authentifiés doivent fournir au serveur un certificat acceptable. Chaque partie est responsable de vérifier que le certificat de l'autre est valide et n'a pas expiré ou été révoqué. Le but premier du protocole TLS est de fournir l'intimité et l'intégrité des données entre deux applications communicantes. Le protocole se compose de deux couches : le protocole *TLS Record* et le protocole *TLS Handshake*. Au niveau le plus bas, reposant sur un certain protocole de transport fiable (par exemple, TCP), se trouve le protocole *TLS Record*.

Il fournit la sécurité de connexion qui a deux propriétés de base :

- ✓ ***Confidentialité*** : la cryptographie symétrique est utilisée pour le chiffrement des données (par exemple, DES, etc.) Les clefs pour ce chiffrement symétrique sont produites de façon unique pour chaque connexion et sont basées sur un secret négocié par un autre protocole (tel que le protocole *TLS Handshake*). Le protocole *TLS Record* peut également être utilisé sans chiffrement.

- ✓ ***Intégrité*** : le transport de messages inclut un contrôle d'intégrité de message en utilisant une fonction MAC (*Message Authentication Code*) à clé. Les fonctions sécurisées de hachage (par exemple, SHA, MD5, etc.) sont utilisées pour des calculs de MAC. Le protocole *TLS Record* peut fonctionner sans MAC, mais est généralement utilisé seulement en ce mode, alors qu'un autre protocole utilise le protocole *Record* comme un transport pour les paramètres de négociation de sécurité.

Les données sortantes sont protégées avec un MAC avant transmission. Pour protéger le message des attaques par rejeu ou par modification, le MAC est calculé à partir du secret du MAC, du numéro de séquence, de la longueur du message, du contenu du message et de deux chaînes fixes de caractères. Le champ du type du message est nécessaire pour garantir que les messages prévus pour un client de la couche *TLS Record* ne soient pas réorientés vers un autre client. Le numéro de séquence garantit que les tentatives de suppression ou réordonnancèrent des messages seront détectées. La *non répudiation* n'est pas spécifiée dans TLS, elle pourrait cependant être fournie par l'utilisation d'un certain algorithme tel que RSA. [1]

I.8.4 - La sécurité avec SRTP

SRTP (*Secure Real-time Transport Protocol*) est un profil et une amélioration du standard RTP pour assurer la confidentialité, l'intégrité et l'authentification des messages et la protection contre le rejeu. SRTP est un nouveau mécanisme de sécurité considéré pour sécuriser les réseaux de Voix sur IP. SRTP crypte les données utiles d'un paquet VoIP (payload d'un paquet RTP) mais garde l'en-tête en clair. Il ne crypte pas les paquets de signalisation de la voix.

Le but de SRTP est d'assurer la confidentialité des champs utiles des paquets RTP et RTCP, l'intégrité de tout le paquet RTP et RTCP avec protection contre le rejeu. Ces services de sécurité sont optionnels et mutuellement indépendants.

Le but de cette sécurité introduite par SRTP dans un contexte multimédia temps réel inclut la vitesse, le parallélisme, la non propagation des erreurs de bits et la limitation de l'expansion des paquets Cependant SRTP présente quelques points faibles :

- ✓ SRTP n'adresse aucune sécurité de la signalisation. Ce qui requiert un mécanisme séparé pour tous les autres types de communications.
- ✓ Besoin d'une gestion de clé séparée, tel IKE, ISAKMP/Oakley, Kerberos ou de mécanismes de point à point tel Diffie-Hellman .
- ✓ Besoin de changer la programmation du protocole dans les téléphones IP.
- ✓ Manque d'authentification des utilisateurs dans des sessions RTP groupées ou multicast. [1]

I.9-Conclusion

Le développement des réseaux informatique et aussi de domaine de télécommunication a donné naissance à une nouvelle technologie tel que la TOIP qui va remplacer notre téléphonie classique par ce qu' elle présente plusieurs avantage de sorte qu'elle est une bonne solution en matière d'intégration de fiabilité , d'évolution et de coût, mais malgré tout les avantages de téléphonie IP il reste quelque inconvénients ,pas proprement dit des inconvénients mais des difficultés tel que la QoS. Mais il est évident que la TOIP va dépassera tous ces difficultés. Bientôt nous téléphonerons tous sur IP, dans les entreprises et même chez nous.

Chapitre II :

La cryptographie

II.1 - Introduction

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer. Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégique liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

II.2- Définition de la cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. [18]

II.3 -Les quatre buts de la cryptographie

- ✓ **Confidentialité** : mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
- ✓ **Intégrité** : mécanisme pour s'assurer que les données reçues n'ont pas été amodiées durant la transmission.
- ✓ **Authentification** : mécanisme pour permettre d'identité des personnes sou des entités et décrier cette identité.
- ✓ **Non-répudiation** : mécanisme pour enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement. [19]

II.4-Vocabulaire de base

- ✓ **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.
- ✓ **Chiffrement** : 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 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'un chiffrement 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.
- ✓ **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.
- ✓ **Cryptosystème** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

L'algorithme est en réalité un triplet d'algorithmes :

- L'un générant les clés K.
- Un autre pour chiffrer M.
- Un troisième pour déchiffrer C. [20]

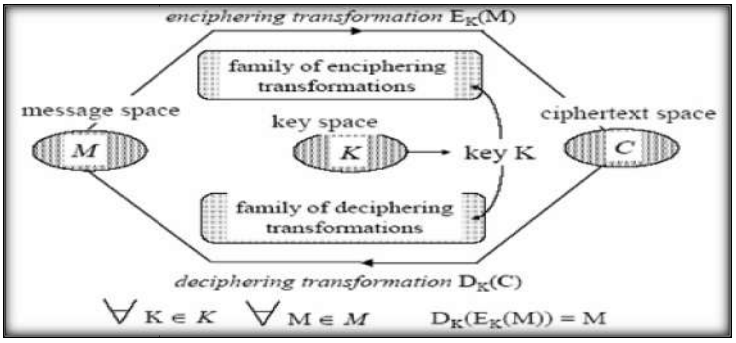

Figure II. 1:Schéma d'un cryptosystème.

II.5 - Cryptographie classique

Il existe des centaines de façon de chiffrer des données représentées par l'alphabet classique, tout en gardant les opérations réalisées secrètes. Ici on ne va pas présenter toutes ces méthodes, mais plutôt les concepts mathématiques (connus depuis très longtemps) qui sont à la source de celles-ci. On va ainsi voir que finalement il n'y en a pas tant que l'on pouvait le penser, et surtout qu'elles sont extrêmement simples. [21]

II.5.1- Substitution

La substitution consiste effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial. La complexité des systèmes à substitutions dépend de trois facteurs :

- ✓ La composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer,
- ✓ Le nombre d'alphabets utilisés dans le cryptogramme,
- ✓ La manière spécifique dont ils sont utilisés. [21]
- ✓ On distingue couramment quatre types de substitutions différentes :

- ❖ **Substitution mono alphabétique :** Chaque lettre est remplacée par une autre lettre ou symbole. Parmi les plus connus, on citera le chiffre de César, le chiffre affine, ou encore les chiffres désordonnés. Tous ces chiffres sont sensibles à l'analyse de fréquence d'apparition des lettres (nombre de fois qu'apparait une même lettre dans un texte). De nos jours, ces chiffres sont utilisés pour le grand public, pour les énigmes de revues ou de journaux. [21]

- ❖ **Substitutions polyalphabétiques:** Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans ou plusieurs alphabets aléatoires associés.L'exemple le plus célèbre est l'algorithme de VIGENERE et de BEAUFORT. L'illustration la plus simple qui corresponde à ce principe st l'utilisation d'une fonction à base de ou exclusif (XOR). [21]

- ✓ ***Vigenère (1568***) : Vigenère a tiré le premier codage à substitution polyalphabétique de l'histoire : le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer

un message. On peut résumer ces décalages avec un carré de Vigenère (voir ci-dessous). Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans). [22]

Exemple : chiffrer le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair)

Tableau II. 1: Application du carré de Vigenère.

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

- **Substitution par polygrammes** : les caractères du texte en clair sont chiffrés par blocs. Par exemple, " ABA " peut être chiffré par " RTQ " tandis que " ABB " est chiffré par " SLL ". Les exemples les plus célèbres sont les algorithmes de PLAYFAIR et de HILL inventés en 1854 et utilisés pendant la première guerre mondiale par les anglais. [21]

Figure II. 2:Substitution par poly-grammes.

II.5.2- Transposition

Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise [21] le principe mathématique des **permutations**. Plusieurs types différents de transpositions existent :

- **Transposition simple par colonnes** : on écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement (cf. la figure ci-dessous). Le destinataire légal pour décrypter le message réalise le procédé inverse. L'algorithme allemand ADFGFX est fondé sur ce principe et fut utilisé pendant la première guerre mondiale. Il fut cassé par une jeune étudiante française.[21]

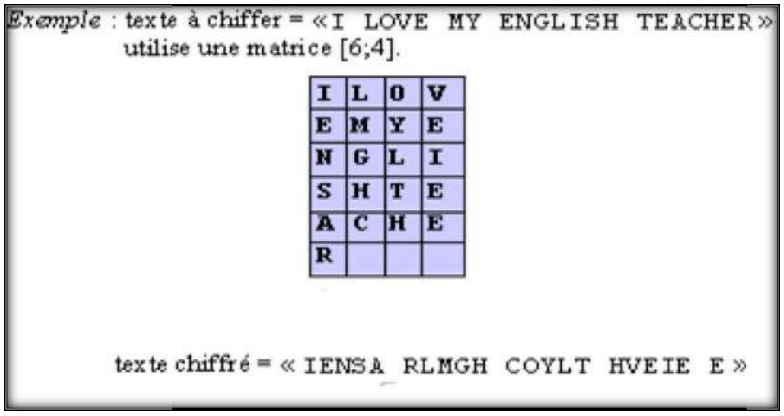

Figure II. 3:Transposition simple par colonnes.

- **Transposition complexe par colonnes** : un mot clé secret (avec uniquement des caractères différents) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet. Une fois que le séquence de transposition est obtenue, on chiffre en écrivant d'abord le message par lignes dans un rectangle (comme le dessin ci-dessous le montre), puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence. [21]

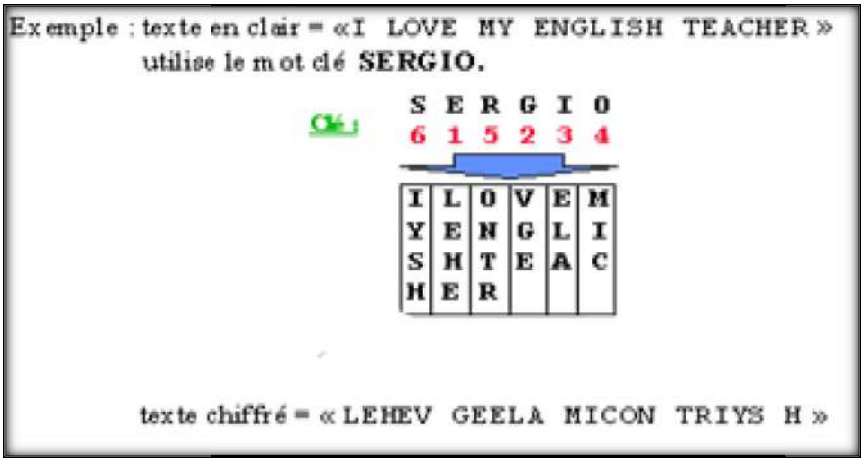

Figure II. 4:Transposition complexe par colonnes.

- **Transposition par carré polybique** : un mot clé secret est utilisé pour construire un alphabet dans un tableau. Les coordonnées des lignes et des colonnes correspondant au lettres du texte à chiffrer sont utilisés pour transcrire le message en chiffres. Avec ce procédé chaque lettre du texte en clair est représentée par deux chiffres écrit verticalement. Ces deux coordonnées sont ensuite transposées en les recombinants par deux sur la ligne ainsi obtenue. [21]

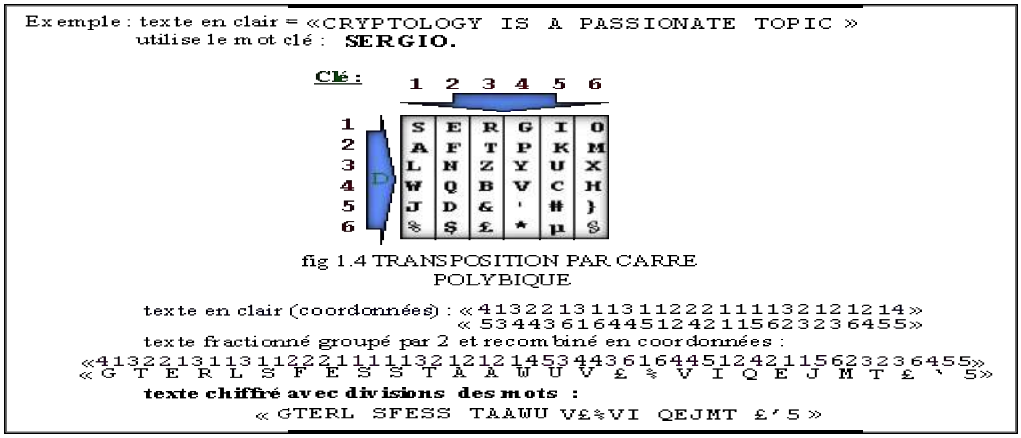

Figure II. 5:Transposition par carré pylobique.

II.5.3-Machines à rotor

La machine allemande Enigma a joué un grand rôle pendant la guerre de l'Atlantique, et son décryptement par les Alliés leur a assuré bon nombre de victoires (notamment parce que les Allemands ne se doutaient pas que leurs messages étaient déchiffrés) [23]. Enigma ressemble à une machine à écrire : on frappe le clair sur un clavier, et des petites lampes s'allument pour éclairer les lettres résultant du chiffrement.

Le principe de [24] chiffrement qu'utilise Enigma est à la fois simple et astucieux. Simple, car il ne s'agit ni plus ni moins d'une substitution de lettres : par exemple, A devient Q, P devient N, etc. Et astucieux, parce que **la substitution change d'une lettre à une autre** : si la lettre A correspond à Q la première fois qu'on la saisit, elle pourrait correspondre à M, K, H, ou tout autre lettre différente de Q à la fois suivante (ce principe est possible grâce à un système de rotors). De plus, un autre avantage non négligeable que possède Enigma est la réversibilité : si on tape le message clair, on obtient le message code, et avec le message codé, on obtient le message clair. L'inconvénient majeur est que jamais la lettre A ne sera codée par A....

Figure II. 6:Machines à rotor.

II.6- Cryptographie actuelle

De tous temps, les services secrets ont utilisé toutes sortes de codages et de moyens cryptographiques pour communiquer entre agents et gouvernements, de telle sorte que les "ennemis" ne puissent pas comprendre les informations échangées.

La cryptologie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Ainsi, très peu de gens, voire personne n'utilisait la cryptographie à des fins personnelles. C'est pourquoi, pendant tant d'années, la cryptologie est restée une science discrète. De nos jours en revanche, il y a de plus en plus d'informations qui doivent rester secrètes ou confidentielles.

En effet, les informations échangées par les banques ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir les déduire. C'est pourquoi ce genre d'informations est crypté.

Finalement, la cryptologie est de plus en plus utilisée sur le réseau mondial Internet. Avec l'apparition du commerce en ligne, c'est-à-dire la possibilité de commander des produits directement sur Internet, la cryptographie est devenue nécessaire. [25] Le chiffrement est toujours associé au déchiffrement, l'action inverse. Pour ce faire, le chiffrement est opéré avec un algorithme à clé publique ou avec un algorithme à clé privée. [26]

II.6.1- Fonction de hachage

Il s'agit de la troisième grande famille d'algorithmes utilisés en cryptographie. Aussi appelée fonction de condensation. Permet à partir d'un texte de longueur quelconque, de calculer une chaîne de taille inférieure et fixe appelé condensé ou empreinte (message digest ou hash).

- Utilisée seule, elle permet de vérifier l'intégrité d'un message.
- Associé à une clé privée, elle permet le calcul d'un sceau ou MAC (Message Authentification Code), pour assurer : Intégrité des données et Authentification de la source.
- Associé à un chiffrement asymétrique, elle permet le calcul de signatures, pour assurer : Intégrité des données, Authentification de la source et Non-répudiation de la source.

Une fonction de hachage doit être : à sens unique, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original. Sans collisions, impossibilité de trouver deux messages distincts ayant la même valeur de condensé. La moindre modification du message entraîne la modification de l'empreinte. [27]

- **Exemples** :

MD5 (Message Digest 5 - Rivest1991-RFC 1321) : calcul une empreinte de 128 bits

SHA-1 (Secure Hash Algorithm 1 - NIST1994) : plus sûr que MD5 - empreinte de 160 bits.

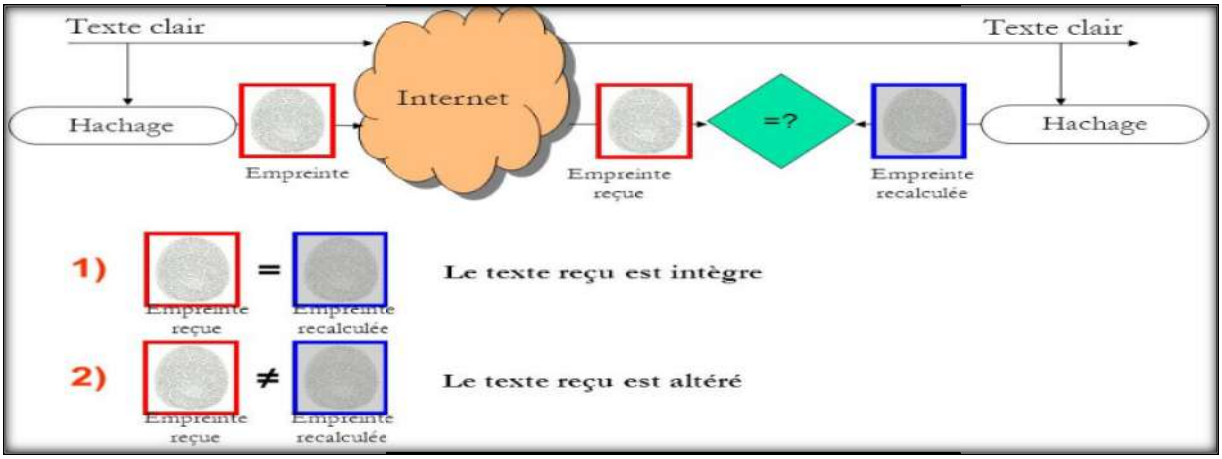

Figure II. 7:Fonction hachage.

II.6.2- Les chiffrements symétriques

Sont les héritiers des méthodes anciennes des cryptographies (comme les substitutions, les transpositions ou le chiffre de Vigénère). L'expéditeur et le destinataire disposent chacun d'un algorithme pour respectivement chiffrer et déchiffrer. Ces algorithmes sont inverses l'un de l'autre. Ils dépendent d'une clé que doivent s'échanger expéditeur et destinataire. Le terme "symétrique" vient de cette particularité. C'est la même clé qui sert au chiffrement et au déchiffrement. En particulier, expéditeur et destinataire doivent s'échanger cette clé, qui doit rester secrète sous peine qu'un tiers parvienne à déchiffrer les correspondances.

Voilà pourquoi on parle aussi de chiffrement à clé secrète. [28] L'échange des clés secrètes, qui doit se faire par un canal sécurisé, est souvent le point faible de ces méthodes de chiffrement.

On distingue deux types d'algorithmes de chiffrement symétrique: par blocs ou par flot.

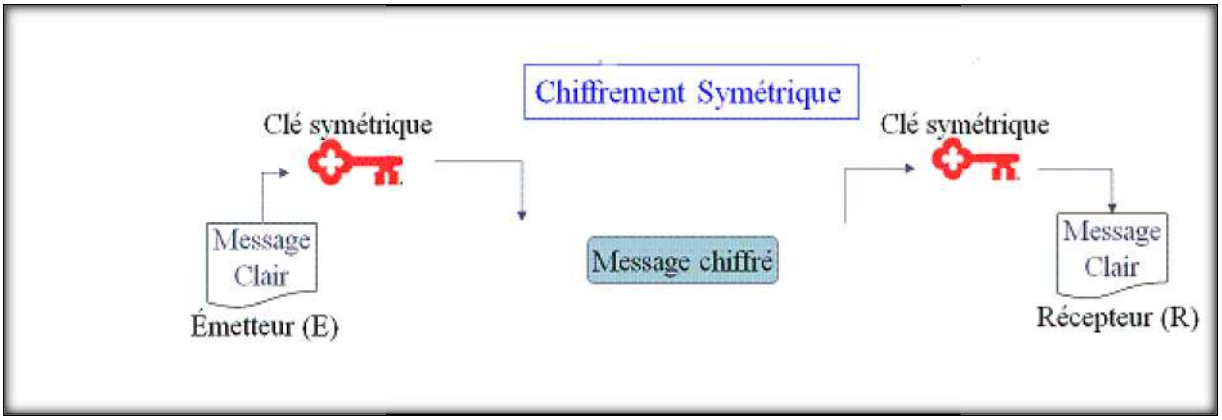

Figure II. 8:Les chiffrements symétriques.

II.6.2.1- Le chiffrement par bloc

Permet de travailler sur des blocs de taille fixée (le plus souvent 16 octets).On traite un message long comme une succession [29] de blocs. Ces algorithmes nécessitent en général d'ajouter du bourrage lorsque le message initial n'est pas un multiple de la taille de bloc.

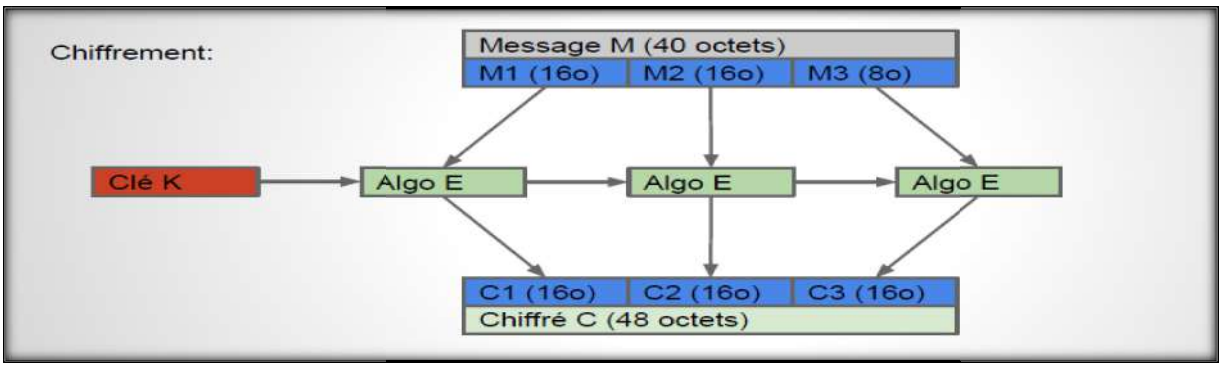

Figure II. 9:Chiffrement par bloc.

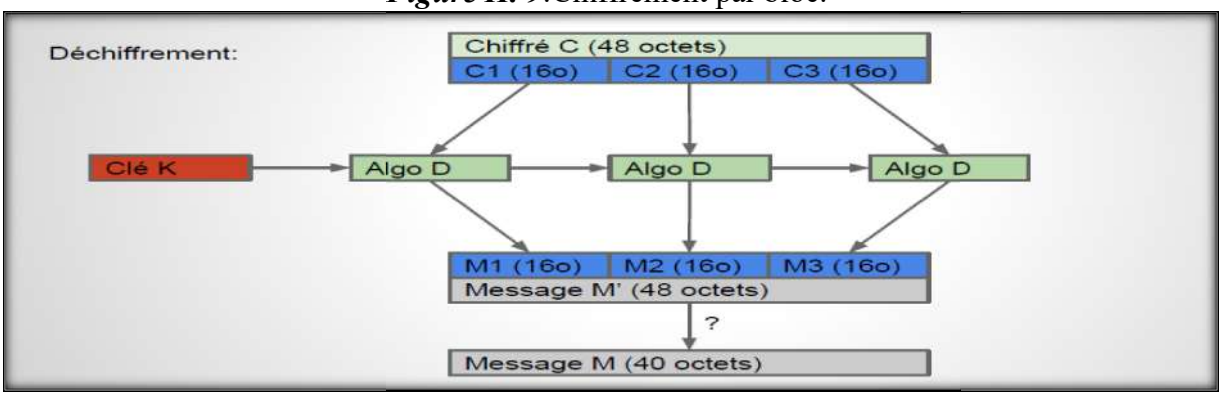

Figure II. 10:Déchiffrement par bloc.

II.6.2.1.A-Exemple d'algorithme symétrique : DES

DES a été officialisé pour la première fois en 1977 (FIPS-PUB 46). Même si il est maintenant possible de casser un chiffrement DES "en temps raisonnable", Triple DES reste relativement résistant. Structure: une permutation statique, suivie par un réseau de Feistel (16

tours), puis une seconde permutation statique du résultat. La fonction utilisée dans le réseau de Feistel est principalement basée sur des S-Box (boîtes S).[29]

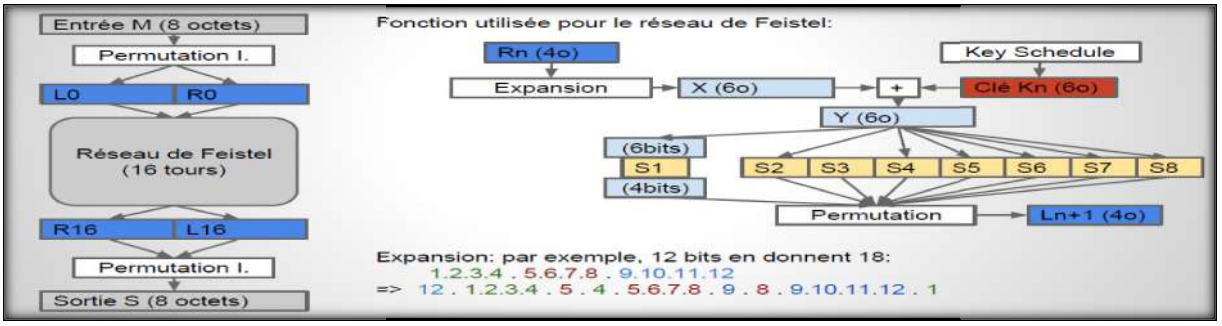

Figure II. 11:Algorithme DES.

II.6.2.2 -Le chiffrement par flot

Permet de travailler sur un message de taille arbitraire, et la traite octet par octet (voir bit par bit). Ces algorithmes sont généralement plus rapides mais moins résistants que les chiffrements par blocs. [29]

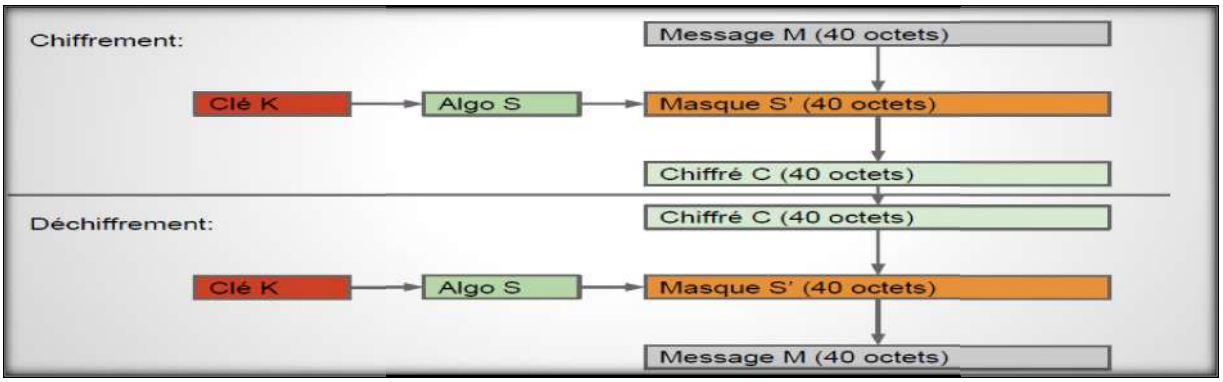

Figure II. 12:Chiffrement et déchiffrement par flot.

Quelques exemples : Chiffrement par flot (ou chiffrement en continu, Stream cipher)

- A5/1 (chiffrement GSM): clé=64bits (seulement 54 pour le GSM)
- RC4 (WEP): clé variable
- E0 (Bluetooth): clé=128bits en général

II.6.2.2.A- Exemple d'algorithme Symétrique : RC4

RC4 est système de chiffrement à flot dû à Ron Rivest, couramment utilisé dans les protocoles SSL et Wifi. RC4 peut utiliser des clés de taille variables jusqu' à 2048 bits.La description de RC4 n'est officiellement pas publique. La suite chiffrant est produite à partir d'un tableau S de 256 octets, initialisions à partir de la clé secrète, et dont l'état évolue au cours de la production. [30]

❖ **Chiffrement**

Deux étapes sont nécessaires pour le chiffrement : l'initialisation à l'aide de la clé et le chiffrement du texte clair. La 1ère étape génère deux tableaux de 256 octets en fonction de la clé. Un tableau K initialisé avec les octets de la clé et un tableau S (table d'états = flux appliqué sur le texte clair) initialisé avec les nombres de 0 à 255 permutés pseudo-aléatoirement.

✓ **Description de l'Algorithme**

Phase : Initialisation

Tableau K contient N octets de la clé et S contient les nombres 0…255

```
Pour i=0 à 255 faire
        S[i]=i
 FinPour
         j=0
Pour i=0 à 255 faire
         j=(j+S[i]+K[i mod N]) mod 256
         Echanger(S[i],S[j])
FinPour
```

Phase : Keystream

```
    i=j=k=0;
Pour k=0 à m faire
    i=(i+1) mod 256
j=(j+S[i]) mod 256
    Echanger(S[i],S[j])
    t=(S[i]+S[j]) mod 256
     KS[k]=S[t]
FinPour
```

Phase : Chiffrement & Déchiffrement

Soit M un message de longueur m (octets) et soit

Chiffrement :

```
Pour i=0 à m faire
   Mc=M xor KS

FinPour
```

❖ **Déchiffrement**

```
Pour i=0 à m faire
   M=Mc xor KS
FinPour
```

La clé RC4 permet d'initialiser un tableau de 256 octets en répétant la clé autant de fois que nécessaire pour remplir le tableau.

Les octets sont déplacés dans le tableau, des additions sont effectuées. Le but est de mélanger autant que possible le tableau. [31]

II.6.3-Les chiffrements asymétriques

L'expression «cryptographie à clé publique» ou cryptographie asymétrique, est une méthode de chiffrement qui utilise deux clés qui se ressemblent mathématiquement mais qui ne sont pas identiques : une clé publique et une clé privée. A l'inverse des algorithmes de cryptographie symétrique qui dépendent d'une seule clé pour le chiffrement et le déchiffrage, les clés de la cryptographie asymétrique ont chacune une fonction bien spécifique : la clé publique sert à chiffrer et la clé privée sert à déchiffrer. [32]

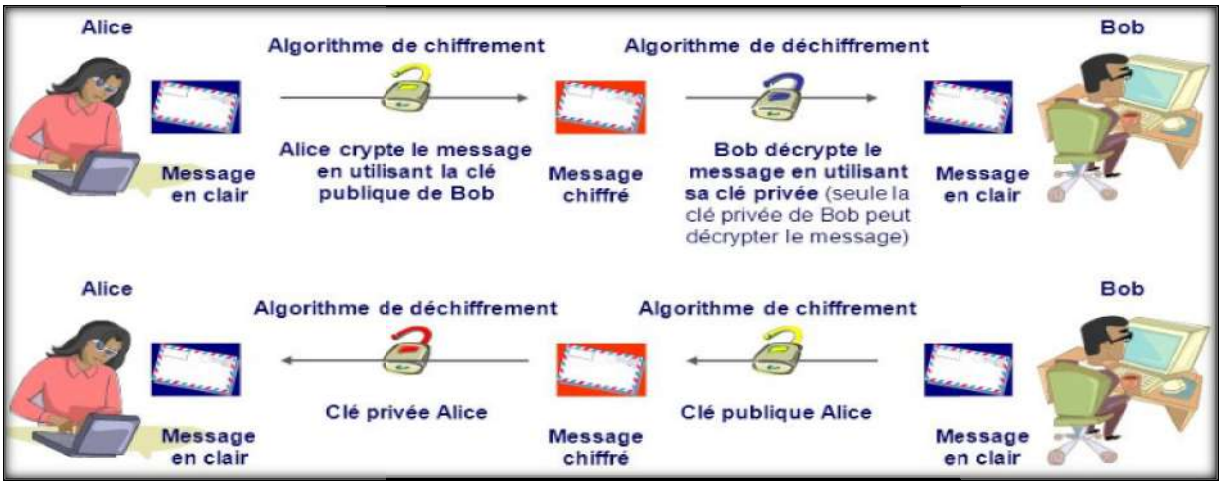

Figure II. 13:Les chiffrements asymétriques.

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

- Chiffrement/déchiffrement : cela fournit le secret.
- Échange de clés (ou des clefs de session).
- Signatures numériques : cela fournit l'authentification.[33]

II.6.3. A- Exemple d'algorithme asymétrique : le RSA

L'algorithme RSA (du nom de ses inventeurs Ron Rivest, Adi Shamir et Len Aldeman, qui ont imaginé le principe en 1978) [34]. Un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

Cet algorithme est fondé sur l'utilisation d'une paire de clés composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles

- **Chiffrement d'un message:** L'expéditeur crée le texte chiffré c à partir du message

m Calculer :

$$c \equiv m^{\wedge e} \bmod n,$$

Où (e,n) est la clé publique du destinataire

Le message chiffre c peut alors être transmis.

- **Déchiffrement d'un message** Le destinataire reçoit x et effectue le déchiffrement
  Calculer :

$$m \equiv c^{\wedge d} \bmod n.$$

où (d,n) est la clé privée du destinataire. [35]
m = message en clair.
c = message encrypté.
(e,n) constitue la clé publique.
(d,n) constitue la clé privée.
n est le produit de 2 nombres premiers.
^ est l'opération de mise à la puissance (a^b : a puissance b).
mod est l'opération de modulo (reste de la division entière). [33]

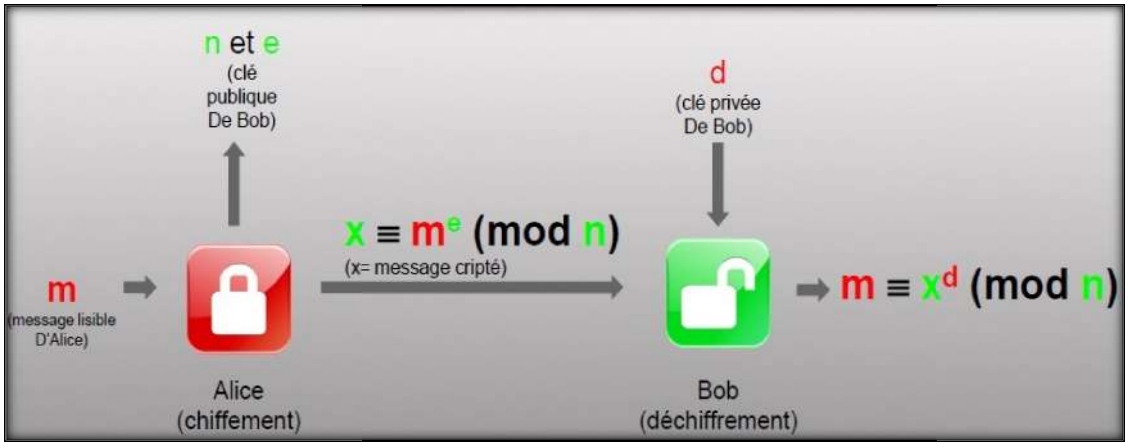

Figure II. 14:Chiffrement et déchiffrement RSA.

II.6.3. B- L'échange de clés Diffie-Hellman

L'échange de clés Diffie-Hellman est un protocole cryptographique a d'abord été publiée par Whitfield Diffie et Martin Hellman en 1976. [36]C'était la première méthode qui permet à deux parties n'ayant aucune connaissance préalable de l'autre d'établir une clé secrète

partagée, qui généralement cipher. Sa sécurité repose sur la difficulté de calculer des logarithmes discrets par rapport à la facilité de calculer les exponentielles.

Principe de l'algorithme :

- ✓ Soient 2 personnes A et B désirant communiquer sans utiliser une clef secrète.
- ✓ Ils se mettent d'accord sur un canal qui n'est pas forcément sécurisé, sur deux grands entiers premiers entre eux, n et g, tels que n > g > 1.
- ✓ Pour que l'échange de clefs soit sécurisé, il faut que n ait une taille de l'ordre de 512 ou 1024 bits.

Etape 1: A choisit un grand nombre entier aléatoire x.

Etape 2: A calcule X = g^x mod n. et l'envoie à B.

Etape 3: B choisit un grand nombre entier aléatoire y.

Etape 4: B calcule Y = g^y mod n. et l'envoie à A.

Ensuite, chacun de leur coté :

- A calcule k=Y^x mod n
- B calcule k'=X^y mod n

On constate alors que k = k' = g^xy mod n et donc que A et B sont parvenus à établir une clef secrète commune qui sera ensuite utilisée par un algorithme symétrique (comme le AES part exemple notre application « VoIP »).

La clef publique correspond aux valeurs X et Y échangées par les deux protagonistes.

La clef privée correspond aux valeurs x et y conservées par les deux protagonistes. [37]

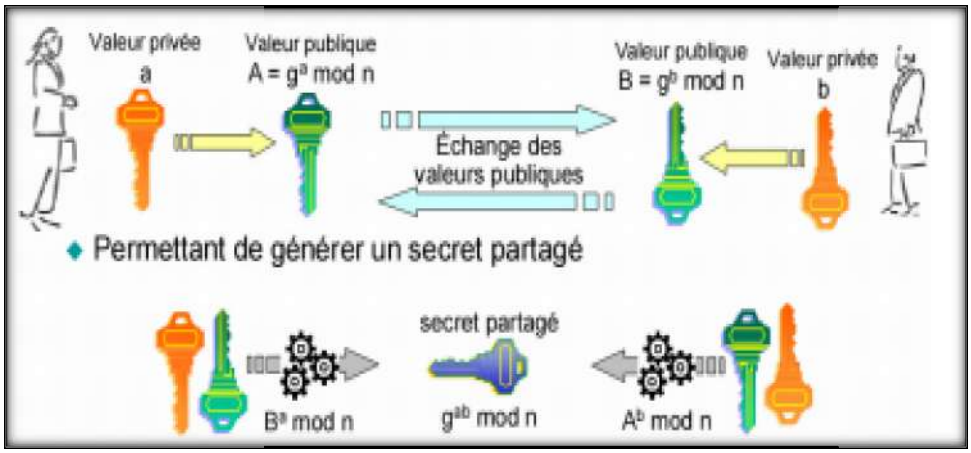

Figure II. 15:Principe L'échange de clés Diffie-Hellman.

II.6.3. C -Protocoles de signature

Les concepts de [38] signature numérique sont principalement basés sur la cryptographie asymétrique. Cette technique permet de chiffrer avec un mot de passe et de déchiffrer avec un autre, les deux étant indépendants.

Supposons que A veut envoyer un message M à B. Comment B peut-il être sûr que le message reçu a bien été envoyé par A. Pour résoudre ce problème, RSA peut être utilisé aussi bien pour transmettre un message que pour le signer. Tout d'abord, A utilise la clé publique (N_B, e_B) de B pour transmettre le message chiffré C et produire une signature S du message à l'aide de sa propre clé privée (N_A, d_A). [39]

Algorithme de Signature d'un message

Entrées : Un message clair M et clé privée (N_A, d_A) ,fonction de hachage h .

Sorties : Un message chiffré C et sa signature S.

A transforme le message en un nombre entier M de l'intervalle $[0, N_B - 1]$.

Calculer $D = h(M)$

Calculer $S \equiv D^{d_A} \bmod N_A$

Retourner le message C et la signature S.

Figure II. 16:Algorithme de signature d'un message.

Vérification d'une signature : Pour vérifier la signature, nous utilisons alors l'algorithme suivant :

Algorithme de Vérification d'une signature

Entrées : Un message chiffre C, une signature S et la clé publique (N_A, e_A), et la clé privée (N_B, e_B)

Sorties : Vérification d'une signature.

B déchiffre le message C : Calculer $M \equiv C^{d_B} \bmod N_B$

B Calcule $D' \equiv S^{e_A} \bmod N_A$ et D=h(M)

Si $D' = D$ Alors la signature est vérifiée.

Figure II. 17:Algorithme de Vérification d'une signature.

II.6.4-Cryptographie hybride

La cryptographie hybride utilise des algorithmes à clé publique et des algorithmes à clé privée, d'où l'adjectif hybride. Ce faisant, il combine les avantages des deux systèmes et pallie à certains inconvénients. En effet, un chiffrement hybride est rapide mais ne présente pas de faiblesse au niveau de la clé comme un chiffrement à clé publique. [40]

II.6.4. A -Principe des systèmes hybrides

Le principe est assez simple. La communication entre A et B se fait par système cryptographique symétrique, ce qui rend la communication assez rapide à chiffrer et

déchiffrer. Mais la lacune de la sécurité [41] de transmission de la clé symétrique de chiffrement/déchiffrement est palliée par un chiffrement de cette clé, qui lui est asymétrique.

- ✓ ***Avantage et inconvénient :*** La rapidité d'un système symétrique grâce à une clé secrète (One Time Session Key) valide le temps du transfert de l'information, ou le temps d'une session. La possibilité de transmettre la clé secrète par une crypto asymétrique. [42]

II.6.4.B - Exemple d'algorithme systèmes hybrides : PGP

PGP : (Pretty Good Privacy) est un programme de cryptage créé par Philip Zimmermann. La première version de PGP date de 1991. Il est très rapidement devenu l'un des crypto systèmes les plus populaires du monde. PGP offre toutes les fonctionnalités d'un cryptosystème complet : cryptage, décryptage, signature, certificat. Aux yeux des utilisateurs, il fonctionne comme un cryptosystème à clefs publiques alors qu'il s'agit d'un crypto système hybride. [43]

- ❖ ***Le principe de PGP*** : PGP est un système de cryptographie hybride, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique.

  - ➢ La plupart des cryptanalyses exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.

Ensuite, l'opération de chiffrement se fait principalement en deux étapes :

- ➢ PGP crée une clé secrète IDEA de manière aléatoire, et chiffre les données avec cette clé.
- ➢ PGP crypte la clé secrète IDEA et la transmet au moyen de la clé RSA publique du destinataire.

L'opération de décryptage se fait également en deux étapes :

- ➢ PGP déchiffre la clé secrète IDEA au moyen de la clé RSA privée.
- ➢ PGP déchiffre les données avec la clé secrète IDEA précédemment obtenue. [44]

- ***Fonctionnement de PGP :*** PGP pour Pretty Good Privacy remplacé aujourd'hui par GPG, GNU Privacy Guard, et S/Mime. Tous les deux utilisent différents algorithmes de cryptographie pour remplir toutes les conditions nécessaires à la protection du courrier :

- Un algorithme de chiffrement symétrique de type IDEA, CAST ou Triple-DES pour chiffrer la session,
- Un algorithme de chiffrement asymétrique de type RSA, DH (Diffie-Hellman), or DSA (Digital Signature Alg) pour chiffrer la clé de session et signer, • un condensat comme MD5, SHA-1, RIPEMD160 ou Tiger pour vérifier l'intégrité. Pour des raisons de performance, les messages sont donc chiffrés à l'aide d'un système à clé symétrique dite clé de session. Cette clé est elle-même chiffrée avec la clé publique du destinataire, ainsi lui seul pourra la récupérer avec sa clé privée et donc lire le message.

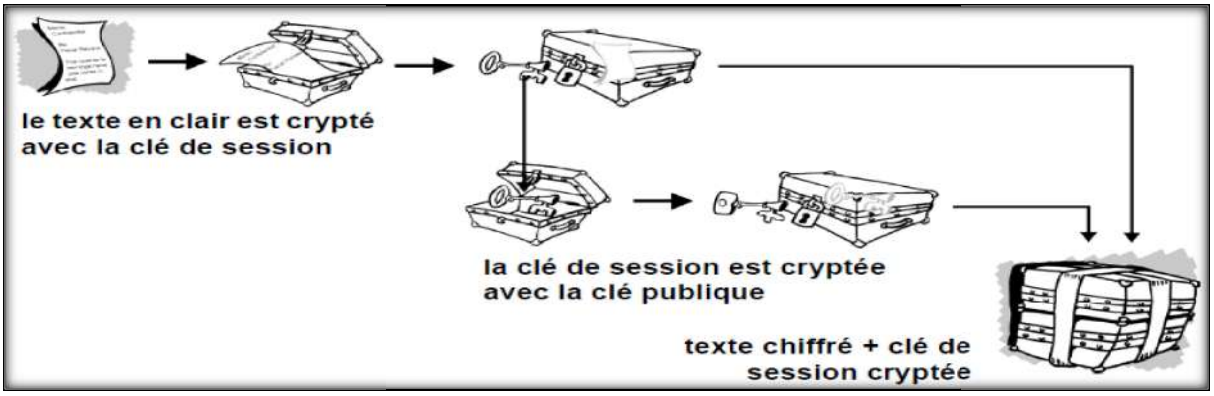

Figure II. 18:Fonctionnement du cryptage PGP.

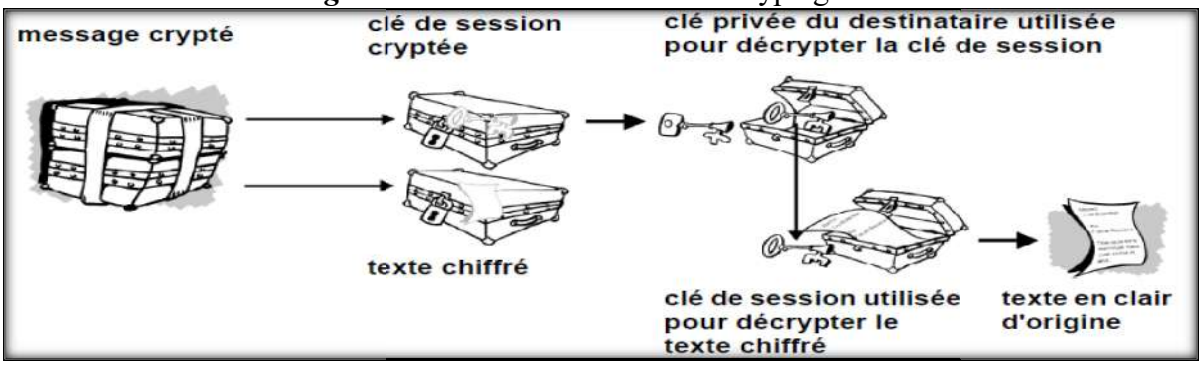

Figure II. 19:Fonctionnement du décryptage PGP.

Pour signer et vérifier l'intégrité du courrier, l'émetteur fait un condensat du courrier et le chiffre avec sa clé publique. Ainsi le destinataire peut générer le condensat du courrier déchiffré et le comparer avec le condensat que lui a envoyé l'émetteur après l'avoir déchiffré avec la clé publique de l'émetteur. [45]

II.6.5-Les Certificats

Un certificat permet d'associer une clé publique à une entité (une personne, une machine) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé Certification Autorité.

L'ensemble des informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations. Puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification.

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.

Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.

❖ **Types de certificat :**

✓ Le certificat client, stocké sur le poste de travail de l'utilisateur.

✓ Le certificat serveur installé sur un serveur web.

✓ Le certificat VPN est un type de certificat installé dans les équipements réseaux. [33]

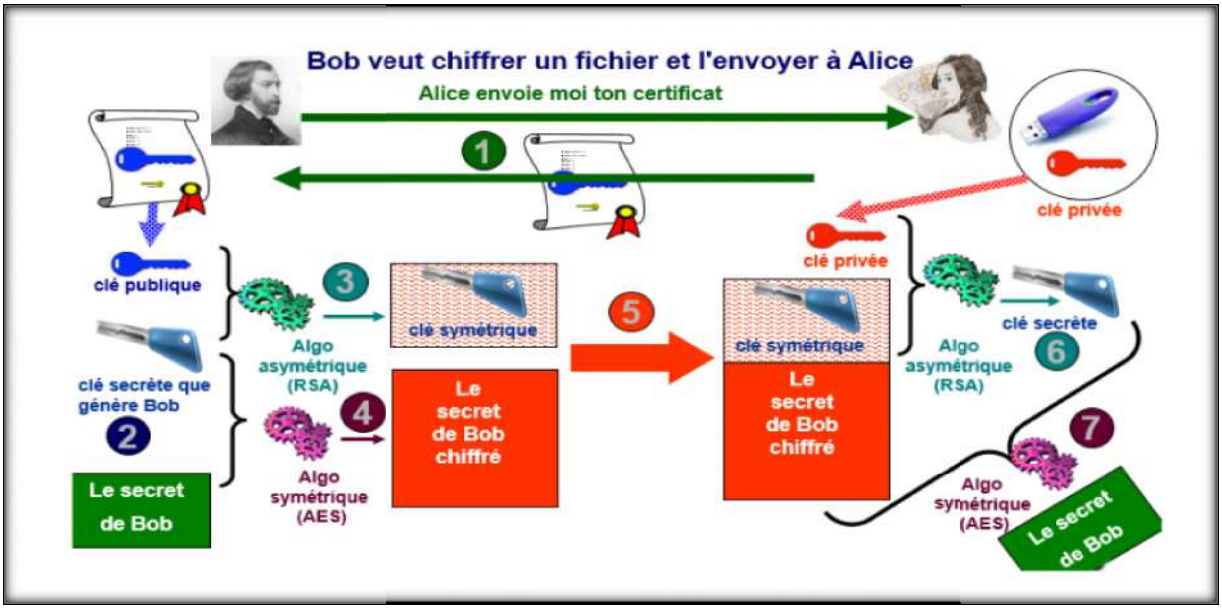

Figure II. 20:Explique l'envoyer du certificat numérique qui contient la clé publique.

II.7- Cryptographie Récent à fort potentiel

Tous les systèmes étudiés précédemment prenaient pour acquis que les communications numériques pouvaient être toujours espionnées d'une façon passive (c'est à dire sans détecter une modification éventuelle de l'intégrité des données échangées), ou enregistrées par un tiers pour un usage futur, même si ce dernier ne peut en comprendre le sens.

L'enregistrement d'une communication chiffrée incompréhensible peut servir à quelqu'un qui espérerait découvrir à une date ultérieure la clé secrète ou l'algorithme lui même dans le cas du chiffrement restreint, car peut-être que celui-ci après avoir accumulé suffisamment de textes chiffrés pourra plus facilement mener à terme sa cryptanalyse, ou bien par simple corruption ou espionnage découvrira la clé secrète, et sera alors en mesure de décoder tous les messages secrets accumulés. [21]

II.7.1- ECC (Elliptic Curve Cryptography)

Techniquement a déjà été inventé, mais est considéré par l'auteur pour être une technique d'avenir parce que la cryptographie les avantages et les inconvénients ne sont pas encore pleinement compris. ECC est une approche de cryptage qui utilise la nature complexe des courbes elliptiques dans les corps finis. Généralement ECC utilise les mêmes types d'algorithmes comme celui de l'échange de clés Diffie-Hellman et le cryptage RSA. La différence est que les nombres utilisés sont choisis à partir d'un champ fini défini au sein d'une expression de la courbe elliptique.

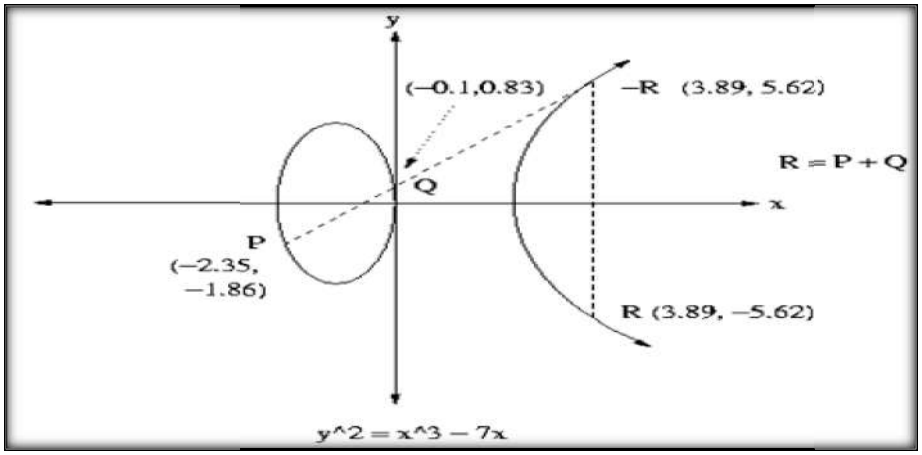

Figure II. 21:ECC (Elliptic Curve Cryptography).

La figure II.25 montre un exemple d'une courbe elliptique. Cet exemple pourrait être utilisé de concert avec un algorithme de type RSA dans lequel deux nombres premiers, "P" et

"Q", sont choisis. Lorsque les primes sont choisies à l'aide d'une courbe elliptique prédéfinis dans un corps fini, les différentes tailles des clés peuvent être beaucoup plus petit et toujours donner le même montant de la garantie. Cela permet au temps qu'il faut pour effectuer le cryptage et décryptage d'être considérablement réduit, permettant ainsi une plus grande quantité de données à transmettre avec une sécurité égale. Tout comme d'autres méthodes de chiffrement ont, ECC doivent également être testés et éprouvés avant la sécurité, il est accepté à des fins commerciales, gouvernementales et privées. [46]

II.7.2 - Calcul quantique

Calcul quantique est effectué dans un ordinateur quantique ou le processeur, qui est un processeur qui permet l'utilisation de phénomènes de la mécanique quantique, comme l'intrication quantique et superposition quantique. Les ordinateurs modernes stockent les données en utilisant un format binaire appelé un "bit" dans lequel un "1" ou "0" peut être enregistré. Les calculs dans les ordinateurs modernes travaillent généralement dans un petit à petit la mode. Les ordinateurs quantiques stockés des données à l'aide d'une superposition quantique d'états multiples. Ces multiples d'une valeur membres sont stockés dans des "bits quantiques" ou "qubits." Selon la conception quantique, Chaque qubit peut enregistrer un ensemble de valeurs numériques simultanément .Ceci permet le calcul de nombres à plusieurs ordres de grandeur plus rapide que les processeurs à transistors.

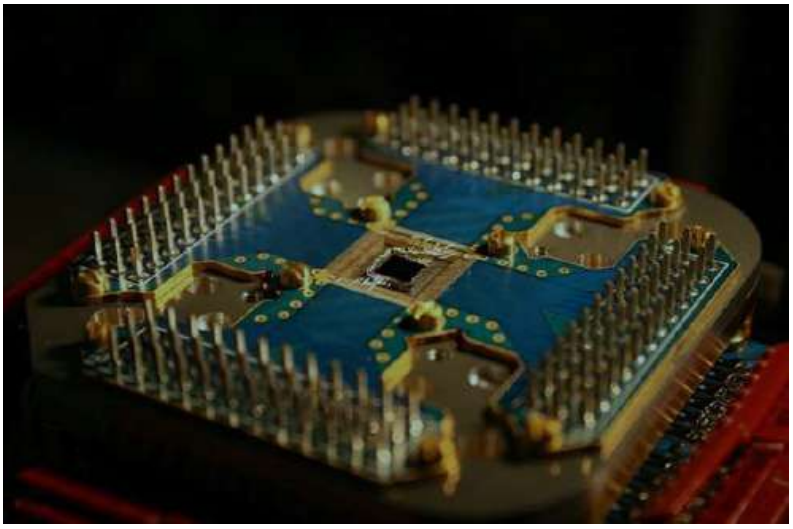

Figure II. 22:Calcul quantique.

La figure II.26 montre le premier processeur quantique commercialement disponible. Ses capacités sont environ 1 000 fois inférieures à celle d'un processeur transistor moderne.

L'informatique quantique est encore à ses débuts. Les processeurs quantiques fabriqués aujourd'hui sont très petits et n'ont pas la taille de calcul que les processeurs à transistors. [46]

II.8-Conclusion

Par l'étude de la cryptographie et le chiffrement, un pays pourrait renforcer ses défenses et disposer des moyens nécessaires pour survivre dans un monde hostile. Une compréhension de chiffrement peut également aider les individus à la sécurisation des données privées et de l'information. Même si elle est gravement contraire à l'éthique, notre communication avec l'autre est constamment surveillée. Ceux qui surveillent notre communication peut inclure les gouvernements, les fournisseurs de services internet, les pirates, les voleurs d'identité, et plus encore. En apprenant à utiliser la cryptographie pour sécuriser les communications, nous pouvons protéger nous-mêmes d'être compromis par ceux qui pourraient voler nos informations.

Chapitre III:
Conception et réalisation

III.1 Introduction

Ce chapitre décrit l'évaluation et l'expérimentation réalisées sur notre application, qui consistait Outils et algorithmes utilisés dans l'application Voix sur IP sécurise

III.2 Outils et algorithmes utilisés

III.2.1 Le langage de programmation Java

Java est un langage de programmation à usage général, évolué et orienté objet dont la syntaxe est proche du C. Ses caractéristiques ainsi que la richesse de son écosystème et de sa communauté lui ont permis d'être très largement utilisé pour le développement d'applications de types très disparates. Java est notamment largement utilisée pour le développement d'applications d'entreprises et mobiles. [47]

Notre choix s'est porté sur ce langage pour différentes raisons :

- 97% des machines d'entreprises ont une JVM installée
- Java est téléchargé plus d'un milliards de fois chaque année
- Il y a plus de 9 millions de développeurs Java dans le monde
- Java est un des langages les plus utilisés dans le monde
- Plus de 3 milliards d'appareils mobiles peuvent mettre en œuvre Java

Plus de 1,4 milliards de cartes à puce utilisant Java sont produites chaque année.

III.2.2 Le protocole UDP

Protocole de datagramme utilisateur (User Datagram Protocol) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, il appartient à la couche 4, comme TCP.

Ce protocole est de permettre la transmission de données de manière très simple entre deux terminaux (deux pc), et un même réseau.

L'envoi et la réception est effectuée simultanément (Full Duplex) et chaque terminal a des paramètres (adresse IP et port) comme récepteur et émetteur,

Tous les terminaux fonctionne comme un récepteur (RECEIVER) server et aussi comme un émetteur (TRANSMITTER).

III.2.3- L'échange de clé de Diffie-Hellman

L'échange d'une clé secrète est fondamental en cryptographie. En effet tout chiffrement d'une grande quantité de données ne peut se faire qu'avec du chiffrement à clé secrète, surtout si cet échange a lieu en temps réel, [47] en raison de la lenteur relative des chiffrements à clé publique. L'algorithme DH spécifie une méthode d'échange de clé publique qui permet à deux homologues (A et B) d'établir une clé secrète partagée qu'ils sont les seuls à connaître, bien qu'ils communiquent sur un canal non sécurisé. Comme pour tous les algorithmes cryptographiques, l'échange de clés DH est basé sur une séquence mathématique d'étapes :

Les données publiques sont : P et G tels que P > G > 1.

Etape 1: EQ1 choisit un grand nombre entier aléatoire a.

Etape 2: EQ1 calcule A = G^a mod P. et l'envoie à B.

Etape 3: EQ2 choisit un grand nombre entier aléatoire b.

Etape 4: EQ2 calcule B = G^b mod P. et l'envoie à A.

Ensuite, chacun de leur coté :

EQ2calcule k= A^b mod P

EQ1 calcule k'= B^a mod P

On constate alors que k = k' = g^ab mod P et donc que A et B sont parvenus à établir une clef secrète commune qui sera ensuite utilisée par un algorithme symétrique.

EQ : Equipement.

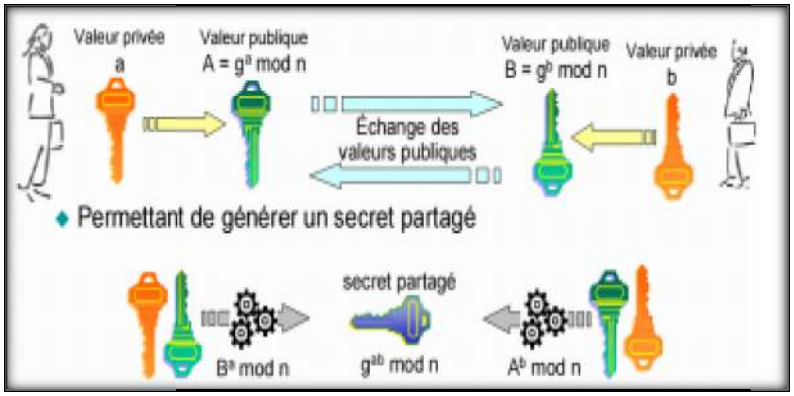

Figure III. 1:L'échange de clé de Diffie-Hellman.

III.2.4 - Algorithme AES

Nous avons utilisé l'algorithme AES (Advanced Encryption Standard) avec clé de 128 bits, vous avez la possibilité d'utiliser 192 ou 256 bits.

C'est un algorithme de chiffrement symétrique. L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne.

Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours. [48]

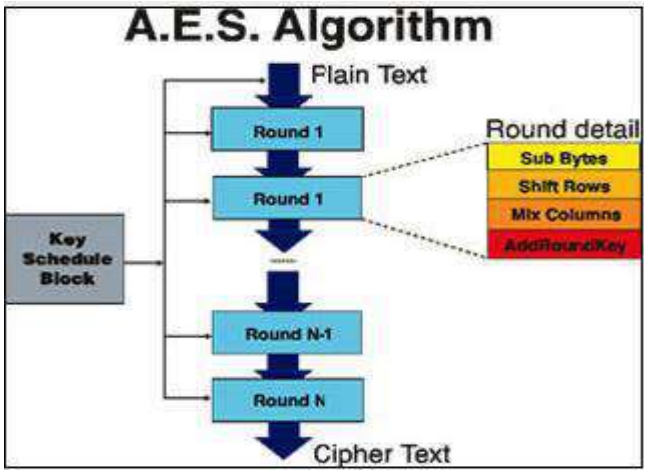

***Figure III. 2**:* Structure Advanced Encryption Standard (AES).

III.3 - Application voix sur IP sécurise

- ✓ Dans notre application le système se compose de deux bornes (2 PC), et un même réseau.
- ✓ L'utilisateur commence par se connecté via un Adresse IP et un port.

- ✓ Le bouton "Voix" est désactivé jusqu'à ce que EQ1 connecté au EQ2.
- ✓ Les deux grands nombre premiers P, G.
- ✓ L'utilisateur EQ1 commence par choisir l'élément secret a. EQ1 calcule ($A= G^a \% P$), et envoi A à EQ2.
- ✓ L'utilisateur EQ2 commence par choisir l'élément secret b et calculé B ($B= G^b \% P$). et envoi B à EQ1.
- ✓ L'utilisateur EQ1 peut se connecter à EQ2 en cliquant simplement sur le bouton "START CONNECTION " et attend jusqu'à ce que EQ2 se connecté et échange A et reçu par là la clef B.
- ✓ Apres ces échanges, les deux partie EQ1 et EQ2 dispose tout deux des informations nécessaire pour calculé la clé « K », l'utilisateur EQ2 calculera $K= A^b \% P$ et l'utilisateur EQ1 calculera $K= B^a \% P$.

Figure III.3 : Login interface.

Figure III.4 : Interface d'inscrire des utilisateurs.

Figure III.5 :Interface d'application EQ1.

Figure III.6:Interface d' application EQ2.

Figure III.7 : Commencer la connexion avec EQ2

Figure III.8 : Commencer la connexion avec EQ1

Figure III.9 : Entamer une discussion avec EQ2.

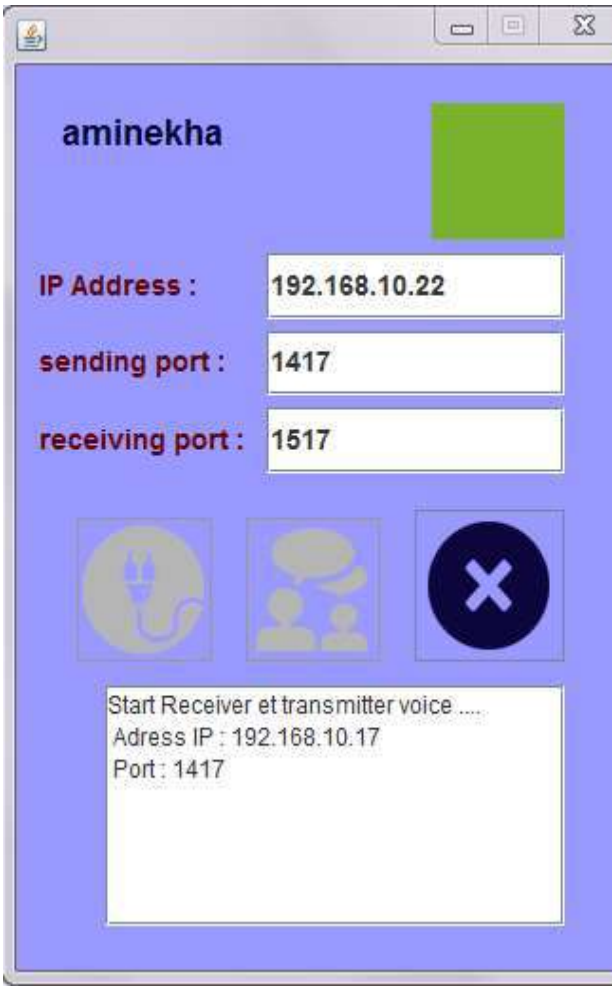

Figure III.10:Entamer une discussion avec EQ1.

- ✓ La conversation est cryptes par AES qui permet à la fois de chiffrer et déchiffrer à l'aide d'un même clé. C'est ici « K » résultat de l'échange Diffie-Hellman.

- ✓ Java fournit un moyen de capturer des données audio (numérique). Les données saisies sont enregistrées dans une mémoire tampon d'octets et le processus de chiffrement effectué sur ce tableau en utilisant l'algorithme AES et enfin il est envoyé via le socket UDP au récepteur. Sur le côté du récepteur, le paquet est reçu et convertie à partir de sa forme cryptée et envoyé les données vocales à l'Orateur.

III.4-Organigramme de l'application.

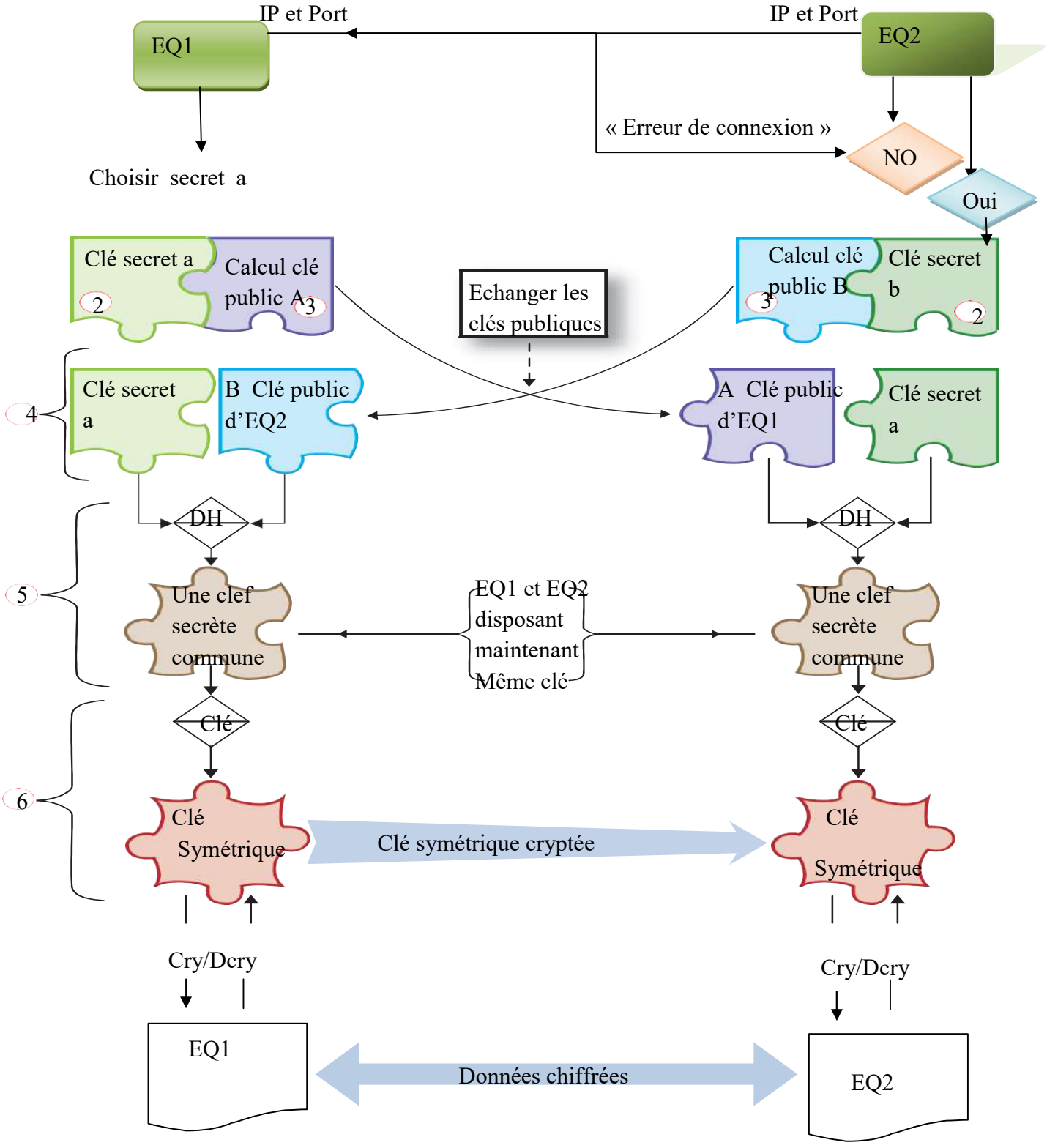

Figure III. 11:Organigramme de l'application.

Cette application présente une technologie numérique qui se développe sur un réseau et fonctionne par la transformation de la voix en données de paquets numériques sécurisé. Cette dernière offre de nombreux avantages, elle sert à préserver la confidentialité des données aussi à garantir leur intégrité et leur authenticité. Son inconvénient majeur est de devoir désactive pare-feu pour établir la communication.

III.5-Conclusion:

La phase de conception et réalisation est l'étape la plus importante dans le cycle de vie de toutes les applications. Ce chapitre a été consacré à la présentation de l'architecture fonctionnelle et technique de notre application et des outils utilisés pour la réalisation, et la description de l'utilisation de notre application, et dans la fin de ce chapitre on a montré les différentes parties de ce travail par quelques captures d'écran.

Conclusion générale

La téléphonie sur IP est un mode de téléphonie utilisant le protocole de télécommunications créé pour Internet (IP pour Internet Protocol). La voix est numérisée puis acheminée sous forme de paquets comme n'importe quelles autres données.

De nos jours en revanche, il y a de plus en plus d'informations qui doivent rester secrètes ou confidentielles, la cryptologie est de plus en plus utilisée sur le réseau mondial Internet, et elle est devenue nécessaire pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux.

L'objectif de notre travail est de réalisé une application VoIP sécurisé qui permet la transmission de données de manière sécurisé entre deux terminaux (deux pc), en un même réseau. Elle est implémentée en utilisant langage java sous l'environnement Netbeans. Ce projet a fait l'objet d'une expérience intéressante, qui nous a permis d'apprendre et d'améliorer nos connaissances et nos compétences dans le domaine de la programmation et de l'apprentissage.

La solution permettant une sécurité de bout-en-bout des appels. L'analyse des solutions applicatives comme « Secure Voice over IP Simple Protocol » nous a permis de formaliser les spécifications des méthodes permettant la protection des conversations des réseaux de ToIP. Cette approche crypte les paquets d'informations voix en toute sécurité, ce qui rend cette solution complètement compatible avec les infrastructures existantes. Par ailleurs notre étude atteste de l'intérêt de mettre en place des entités de confiance dédiées à la sécurité des appels. Les résultats expérimentaux de notre application créent un canal sécurisé. Les informations doivent rester secrètes et confidentielles.

Le prolongement de notre travail permettra de crée un nouveau protocole à partir des bons points de toutes les solutions possibles de sécurisation de la voix, n'est pas à exclure pour servir l'intérêt du sujet. Il serait par exemple possible de penser à développer un nouveau protocole générique, de niveau applicatif dont le but est d'être déployé pour sécuriser un échange de communication de voix et essentiellement la voix sur IP et qui proposerait deux mécanismes nécessaires à la sécurité de la voix, l'authentification de l'utilisateur et le non répudiation de l'appel.

Bibliographie

[1] Marguerite Fayçal, « *La sécurisation de la téléphonie sur IP* », Diplôme d'Etudes Approfondies Réseaux de télécommunications. Universitaire de la Francophonie AUF, 20 décembre 2004

[2] Marc Chutet, « *Téléphonie sur IP – TOIP* », document électronique ,Le 06 octobre 2003

[3] Denis TSHIMANGA , « *Etude d'implémentation d'une solution VOIP sécurisée dans un réseau informatique d'entreprise* », Mémoire d'ingénieur en génie électrique, Cas de l'ISTA de Kinshasa. 2012-2013

[4] « codec- AMV France Wiki,» Article. Disponible sur URL : http://wiki.amv france.com/wiki/Codec. Consulté le 02/2017

[5] Maroua LABIDI, « Etude et mise en place d'une solution Voix sur IP sécurisée » PFE .2012/2013

[6] Yannick YANI KALOMBA. « *Etude et mise au point d'un système de communication VOIP : application sur un PABX-IP open source* ». Mémoire Ingénieur en réseaux et télécoms. Université protestante de Lubumbashi .2009

[7] SebF, « *Voix sur IP - VOIP* » ?document électronique ,Création Le 14 novembre 2004.

[8] Accellent, « La Qualité de Service le la Voix sur IP Principes et Assurance ».

[9] Violeta FELEA, « *VoIP Et Asterisk / Trixbox* », rapport de stage, Université De Franche- Comté, 2007-2008

[10] Mourad EL ALLIA. « *Développement d'un environnement de communication multicast (voix et vidéo)* ». Mémoire présenté à l'école de technologie supérieur. Université du QUÉBEC, 09 octobre 2002

[11] Didi Souhila et Guerriche Meryem. « *La Téléphonie sur IP (ToIP)* ». Mémoire de fin d'études du diplôme de Licence en Informatique. Université Abou Bakr Belkaid. Tlemcen. 09 Juin 2014.

[12] ENCYCLOPEDIE.FR : http://www.encyclopedie.fr/definition/terminal . Consulté le 05/2017

[13] Soumia BACHIRI et Baraka BELARBI, « *Déploiement d'une application de TOIP* », Mémoire de fin d'études du diplôme de Licence en Informatique. Université Abou Bakr Belkaid. Tlemcen, 01 juin 2015

[14] PABX-FR, « *PABX* », Présentation , Disponible sur URL : http://www.pabx-fr.com/toip/index2.php -Consulté le 07/2017

[15] Zahia TAHRA « *Etude et simulation d'un réseau de téléphonie sur IP (TOIP)* », Mémoire de fin d'étude du Diplôme d'ingénieur d'état en Informatique, Université KASDI MERBAH. Ouargla, juin 2008

[16] AWT (Agence Wallonne des Télécommunications), Fiche de l'AWT la téléphonie sur IP, Article crée le 18/04/06.

[17] BIGGS Maggie, « *Téléphonie sur IP : les 6 faiblesses qui rebutent les entreprises* », Article, Vendredi 26 Octobre 2001.

[18] Laurent FLAUM « *Principe du Cryptage PGP* » chapitre 1 de document : Introduction à la cryptographie.

[19] X.-F. Roblot. « *Module Cryptographie du Master-Pro d'Ingénierie Mathématique* ». Cour chapitre 1. Université Claude Bernard Lyon I. France.

[20] Renaud DUMONT, « *Cryptographie et Sécurité informatique* », Université de Liège

[21] Serge DELESTN & Lionel LEJEUNE, «*Chiffrement & cryptographie*», Université joseph fourrier, Janvier 1998.

[22] La cryptographie, « *Historique des techniques de cryptographie* ».2003-2004. Disponible sur URL : http://wakaziva.pagesperso-orange.fr/crypto/2.htm Consulté le 02/2017.

[23] Dr. Noureddine BOUJNAH, « *Introduction à la cryptographie* », Cours sécurité informatique, Faculté des Sciences de Gabès. 2 novembre 2014

[24] CryptAGE. « *La machine Enigma* ». Novembre 2006 et est hébergé par OVH , Disponible sur URL : http://www.cryptage.org/enigma.html Consulté le : 02/2017.

[25] « *Cryptographie et sécurité cryptographique* ». URL : http://wallu.pagespersoorange.fr/cryptologie.pdf -Consulté le : 02/2017.

[26] HSC. « *Bienvenue dans le monde du cryptage* ». Cours de Cryptologie.

[27] Ahmed MEHAOUA. « *Cryptographie et services de sécurité* ». Présentation.

[28] Bibm@th.net, « *Les chiffrements symétriques* » .Disponible sur URL : http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/clesec Consulté le : 03/2017.

[29] Gabriel RISTERUCCI, «*Cryptographie* », Cours 2/8- Chiffrement Symétrique

[30] Eric Wegrzynowski. « *Chiffrement à flot* », Licence et Master mention informatique, Université de Lille 1.France. 3 avril 2009

[31] LAZAAR, « *Alogrithme RC4 et tests de sécurité* », ENSA

[32] GlobalSing, « *Qu'est-ce que la cryptographie à clé publique* » .Disponible sur URL : https://www.globalsign.fr/fr/centre-information-ssl/cryptographie-cle-publique/ -Consulté le : 02/2017.

[33] Anime KHALDI, « *La cryptographie* », Cour résume-chapitre-2, master1, 2016.

[34] FUTURA TECH. « *RSA* ». Disponible sur URL : http://www.futura-sciences.com/tech/definitions/tech-rsa-1787/ Consulté le : 03/2017.

[35] Yacine CHALLAL & Hatem BETTAHAR. « *Introduction à la sécurité informatique* ». Cours 15/10/2008

[36] Cryptographie. « *Méthodes modernes de cryptographie* » Disponible sur URL : http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/clepub - Consulté le : 02/2017.

[37] Les systèmes à clé publique. Disponible sur URL :http://wakaziva.pagesperso-orange.fr/crypto/4.htm -Consulté le : 03/2017.

[38] Benoît DEPAI, « *La signature numérique* ». Exposés de Système/Réseaux. Université de marne-la-vallée. France.2006

[39] Nadjiba MAHAMMEDI et Houda MAHDADI, « Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques $Æ_p$ et$Æ_{2^n}$ », mémoire master académique, Université Khasdi Merbah Ouargla, 06/2013

[40] CRYPTOLOGIE MODERNE : http://cryptologie-moderne-tpe.e-monsite.com/pages/theorie-et algorithme/cryptographie-hybride.html -Consulté le : 03/2017.

[41] Centrale Nantes. « *Principes de la cryptographie moderne* ». Article .18 décembre 2010

[42] Suzan OUN. « *Chiffrement Hybride* ». Le 31 mai 2014.

[43] Bourgeois MORGAN. « *Initiation à PGP : GnuPG* ». Article publié le 1er janvier 2006.

[44] Sylvain LORIN, « *PGP - Pretty Good Privacy* », Article, crée Septembre 2015.

[45] Olivier RICOU, « Les coulisses de l'Internet, cour chapitre 4 : La communication », 16 décembre 2015

[46] Nicholas G. McDonald. « *Past, Present, and Future methods of cryptography and data encryption* », Department of Electrical and Computer Engineering, University of Utah.

[47] Abderazak DLILI et Mouatez Billah BENZINA « Échange de clé Diffie-Hellman par échange d'images Stéganographiée »,Mémoire Master Professionnel, UNIVERSITÉ KASDI MERBAH OUARGLA,2015/2016.

[48] Salomon N'DRI «*Quel est l'algorithme de cryptage le plus robuste au monde?* », Article, lundi 11 octobre 2010

Résume

La téléphonie sur IP (ToIP) est une technologie qui s'impose progressivement dans tous les secteurs, elle consiste à faire transiter les communications téléphoniques par le réseau IP.

Ce travail a pour objectif de fournir une communication VOIP chiffrée entre deux interlocuteurs, un échange de clé est effectué au préalable via un algorithme asymétrique (Diffie-Hellman) après cet échange toutes les communications seront chiffrées en AES en utilisant la clé généré des deux cotés.

MOTS-CLES *:*

TOIP, VOIP, H323, SIP, GMCP, IPSEC, LAN.

Abstract

Telephony over IP (ToIP) is a technology which is gradually imposing itself in all the sectors, it consists in making transit the telephone calls by the IP network.

The goal of this work is to provide a VOIP communication encrypted between two interlocutors, a key exchange is made in advance via an asymmetric algorithm (Diffie-Hellman) after this exchange all communications will be encrypted with AES by using the key generated on both sides.

KEY-WORDS:

TOIP, VOIP, SIP, GMCP, IPSEC, LAN.

الملخص

الاتصال عبر البروتكول إنترنيت هي تكنولوجيا بدأت تفرض نفسها تدريجيا في جميع القطاعات وتتمثل في المكالمات الهاتفية بواسطة الشبكة

الهدف من هذا العمل هو تنفيذ وإنشاء تطبيق محادثة مشفرة بين محطتين وذلك بتشفير الاتصال بخوارزمية الغير تناظر (Dffie-hellman) وبعد الإتصال نقوم باستخدام مفتاح لتشفير المحادثة والتي ستُشفر ب خوارزمية التناظر(AES).

الكلمات المفتاحية

الإتصال عبر بروتوكول إنترنت . الصوت عبر الإنترنت.بروتوكول بدء جلسة . بروتوكول التحكم في بوابة الوسائط . بروتوكول الأمن للاتصالات عبر الشبكات .الشبكات المحلية