REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU

Faculté de génie électrique et d'informatique
Département d'électronique

Mémoire
De fin d'études
En vue de l'obtention du diplôme
d'Ingénieur d'Etat en Electronique
Option : Communication

THEME

Implémentation de l'algorithme de cryptage IDEA dans le réseau téléphonique de nouvelle génération NGN de la wilaya de Tizi-Ouzou

Proposé et dirigé par :

Mr : A.MOUALEK

Promoteur :

Mr M.TAHANOUT

Etudié par :

Melle : AIT AIDER Malika

Melle : TAMAZIRT Nedjma

Promotion 2008

Remerciements

Nous tenons à remercier notre promoteur Mr M.TAHANOUT qui a accepté la charge et la direction de cette étude. Son soutien, ses orientations et conseils nous ont été d'un apport précieux, depuis la définition et structuration du sujet jusqu'à sa concrétisation, et Mr A.MOUALEK, chef de centre de l'HONET au niveau de complexe des télécommunications d'ALGERIE TELECOM Nouvelle Ville, Tizi-Ouzou d'avoir accepté de nous encadrer, de nous avoir suivis pendant toute la durée du travail

Nos vifs remerciements vont à Mr Y.AIT BACHIR et Mr H.HAMICHE qui nous ont prodigué sans réserve avis et conseils tout au long de notre travail et dont nous avons tiré de très grands profits.

Nos remerciements vont également au président et aux membres de jury qui feront l'honneur d'évaluer notre modeste travail. Ainsi qu'à tous les enseignants qui ont contribué à notre formation.

Que toute personne qui d'une manière ou d'une autre, nous a aidé et encouragé pour l'aboutissement de ce travail, trouve ici l'expression de notre gratitude.

Dédicace

Il est bien trop modest comme travail
mais c'est le fruit de tant d'éffort tout au long
de ce semestre,je le dédie :

Tout d'abord à mes très chéres parents qui m'ont
beaucoup aidé financiérement et encouraggée pour
que je puisse mener mes études .

A mes fréres : Tahar.Boualem, ,Nadir , Hakim
A mes sœurs adorées :Siham, Lydia qui m'a cassé la tête ,Souad ,
Safia et son marie Azzedine,et surtout Djahida qui m'a vraiment suivie.
A mes deux anges Amoune et Nanita.

A mes amis : Mouloud et Karim .
A mes amies : Chahira,Dalila k ,Dalila B,
Nedjma, Malika , Lamia B…
je les remercie tous pour leurs soutiens

Sans oublier ma grande mére que Dieu la Protége.
A mon binôme et fidele amie Kahina et sa famille.
Bien sur sans t'oublier à Kamel et merci pour tes
encouragement.
A toute la prômo 2007/2008.

Mounia
Chabane

Remericements

Nous tenons à remercier :

- *Le bon Dieu qui nous a donné la bonne santé et la persévérance durant notre cursus.*
- *Nos parents et tous ceux qui nous ont aidé pour mener à terme ce travail .*
- *Notre promoteur Mr Haddab.S.*
- *Les membres de jury.*
- *Et touts les lecteurs.*

Dédicace

Il est bien trop modest comme travail mais c'est le fruit de tant d'éffort tout au long de ce semestre,je le dédie :

- *A ma très chère mère qui n'a jamais cessé de m'encourager et de me soutenir,que Dieu la protège.*
- *Mon père que Dieu le protège.*
- *Mes merveilleux frères : Mahmoud, Hacène, Houcine , Boualem, Mohand, Rachid et Khaled qui m'ont soutenue tout au long de mes études.*
- *Mes chère sœurs :Nacèra et Zohra.*
- *Mes belles sœurs.*
- *Mes nièces et neveux.*
- *Mon équipe du club sporting Freha de Vô-Vietnam.*
- *Mes amies surtout :Ouiza,Taous,Lila,Ouarda,Sonia,Rosa,Kahina et Mounia.*
- *Mes amis surtout :Mansour,Omar,Boualem et Maher.*
- *Ma très chère amie et binôme Nedjma et sa grande famille.*
- *La promo 2007/2008*
- *Tous ceux qui m'ont soutenue et encouragée.*

Malika.

SOMMAIRE

INTRODUCTION GENERALE

La sécurité de l'information présente un élément important dans la transmission des données dans un réseau téléphonique ou informatique. En effet, selon le niveau de protection exigé par l'utilisateur, on doit effectuer le transport de l'information, sans pertes certes, mais aussi, en assurant l'accès à cette information uniquement aux concernés pour des raisons de secret professionnel dans le cas des entreprises, de défense militaire ou simplement pour une raison de liberté individuelle dans les transmissions grand publique. Pour ce faire, on peut procéder selon deux méthodes, la protection physique du canal de transmission ou la protection des données par voie logicielle transformant les données en claire en données illisible ou cryptées.

Dans cette étude nous nous sommes intéressés aux méthodes de cryptage de données et leurs possibilités d'implémentation dans le réseau de télécommunication NGN d'Algérie Télécom. Le réseau NGN offre différent services d'échange de données sur la voie IP, la parole ou la téléphonie, la vidéo et les données informatiques. Selon le type de données, le réseau doit assurer des traitements en temps réel et un débit suffisant pour la transmission de ces données. Le cryptage de données, dans ce type de réseau, doit être effectué par des algorithmes très rapides avec une fiabilité suffisante.

Pour illustrer cette étude, dans le premier chapitre, nous donnons des généralités sur le réseau RTC, la signalisation sémaphore SS7, la migration du réseau RTC vers le réseau de nouvelle génération NGN. Dans le deuxième chapitre, nous présentons le réseau NGN et ses différents protocoles. Le troisième chapitre concerne des généralités sur la sécurité dans réseau. Le quatrième chapitre est consacré à l'étude de quelques algorithmes de cryptages. Enfin, le cinquième chapitre présente notre application qui consiste à l'étude de l'algorithme de cryptage IDEA et son implémentation sous Matlab.

I. Réseau téléphonique commuté RTC [1]

I.1. Introduction

Un réseau de télécommunication est un système complexe. Il constitue un moyen de communication véhiculant des informations (voix, données, image etc …) est constitué de deux types de niveau : un niveau fonctionnel comportant la commutation et la transmission, un niveau géographique comportant le réseau de distribution, le réseau sectoriel et le réseau d'interconnexion.

Il existe plusieurs réseaux de télécommunication parmi les quels on distingue le réseau téléphonique commuté RTC, qui a pour but de la mise en relation de deux postes d'abonné. L'échange d'information nécessaire à l'établissement, au maintien et à la rupture de la relation s'appelle « la signalisation ».

I.2.Organisation du RTC

Le RTC est organisé en trois parties (figure I.1) :

1. **Distribution** : c'est l'organisation technique mise en œuvre pour relier les abonnés au commutateur le plus proche (commutateur de rattachement), l'ensemble de dispositif permettant cette liaison est le réseau de distribution.

2. **Commutation** : c'est la partie centrale du réseau, elle permet la mise en relation entre les abonnés.

3. **Transmission** : c'est l'ensemble des techniques mises en œuvre pour relier les commutateurs entre eux .L'ensemble des commutateurs et de support de transmission entre commutateur est appelé « réseau de transmission » ou « réseau de transport ».

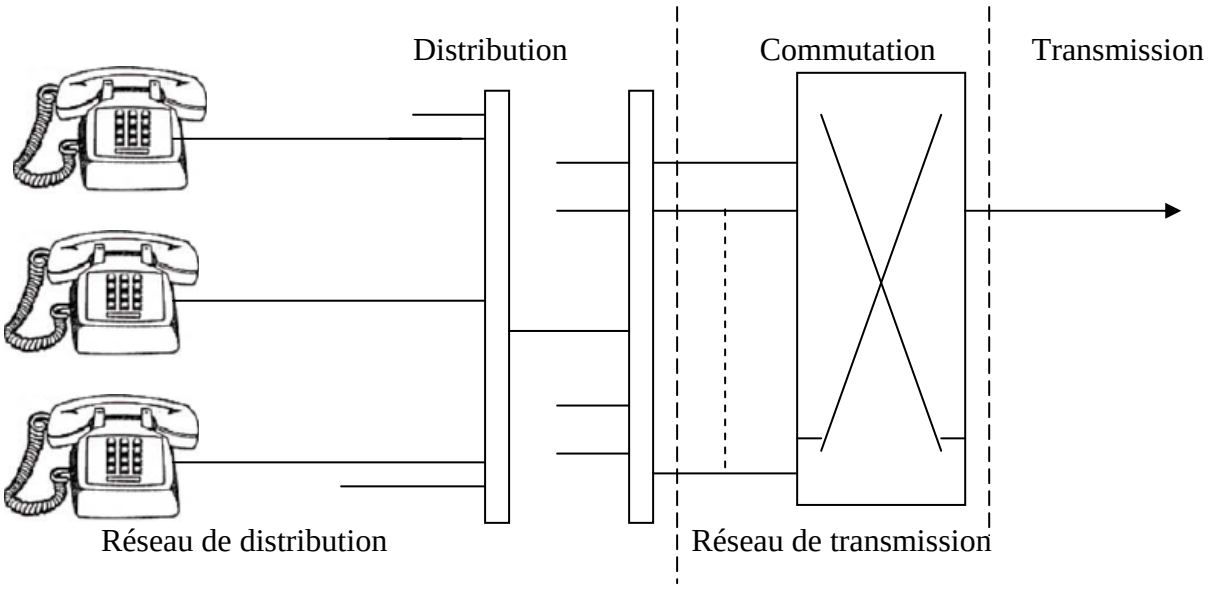


Figure I.1. Schéma général du réseau téléphonique.

I.3. Commutateurs [2]

I.3.1. Définition

Les commutateurs sont des nœuds s'échangeant des informations du moyen de protocoles de communication basés la plus part du temps sur l'émission de fréquence. Il y a plusieurs types de commutateurs, chacun ayant une fonction spécifique :

Le Commutateur à Autonomie d'Acheminement (CAA) ou Commutateur Local (CL) permet de mettre en relation les clients de même zone géographique. Un appel régional passe par le commutateur local qui envoie un signal au commutateur régional appelé « centre de transit (CT) » qui permet d'écouler les communications téléphoniques d'un CAA à un autre CAA. Si le numéro composé est destiné à l'international, c'est un centre de transit international (CTI) qui traite l'appel.

Les supports de transmission pour l'acheminement du signal entre commutateurs peuvent être faite par :

- des conducteurs métalliques (paire torsadée, câbles coaxiaux).
- par les liaisons en espace libre avec des faisceaux hertziens (via des antennes et des satellites).
- par fibre optique

I.3.2. Fonction d'un commutateur

Sa principale fonction est la connexion c'est-à-dire la liaison temporaire entre deux jonctions qui peuvent être un circuit ou une ligne d'abonné.

L'établissement des connexions est assuré par l'unité de commande (Ordinateur) qui nécessite :

- l'échange de signalisation entre les commutateurs
- une suite d'actions appelée « traitement de signal »
- Le commutateur local comprend les unités de raccordement d'abonné (URA) assurant les fonctions suivantes :
  - fournissent l'énergie de l'alimentation des postes téléphoniques et adaptent les caractéristiques électriques.
  - détectent le décroché et le raccroché d'un poste.
  - génèrent une sonnerie vers un poste et exécutent des testes des lignes d'abonnés.
  - offrent une fonction de concentration.

I.4.Architecture du réseau téléphonique commuté RTC

Le réseau téléphonique est organisé en trois zones:

1. **Zone à Autonomie d'Acheminement (ZAA)** : au bas de la hiérarchie les commutateurs (CAA) accueillent les abonnés et peuvent établirent différents types de communications.

2. **Zone de Transit Secondaire (ZTS)** : comporte les commutateurs (CTS) .Les abonnés ne sont pas reliés aux (CTS) .Ils assurent les passages des circuits lorsqu'un (CAA) ne peux pas atteindre le (CAA) destinataire directement.

3 .Zone de Transit Principal (ZTP) : cette liaison assurent la commutation des liaisons longues distances. L'un des commutateurs (CTP) est relié au commutateur international de transit(CTI).Dans les zones à faible densité, les abonnés sont rattachés à des commutateurs locaux (CL) dits aussi « concentrateur de trafic ».

La figure (I.2) représente les trois zones du réseau téléphonique :

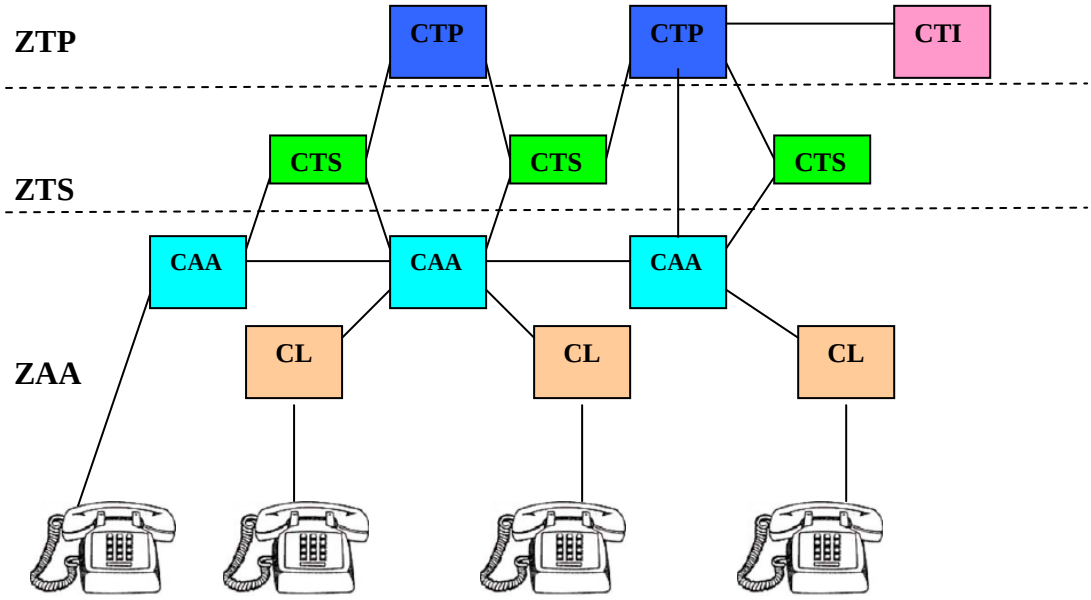


Figure I.2 : Hiérarchie du réseau téléphonique.

Pour un numéro donné, le faisceau de premier choix est choisi de telle manière qu'il conduise l'appel vers le commutateur le plus proche de l'abonné appelé en empruntant les faisceaux de plus faible hiérarchie.

I.5. Architecture d'un central téléphonique

La figure(I.3) représentel' architecture d'un central téléphonique :

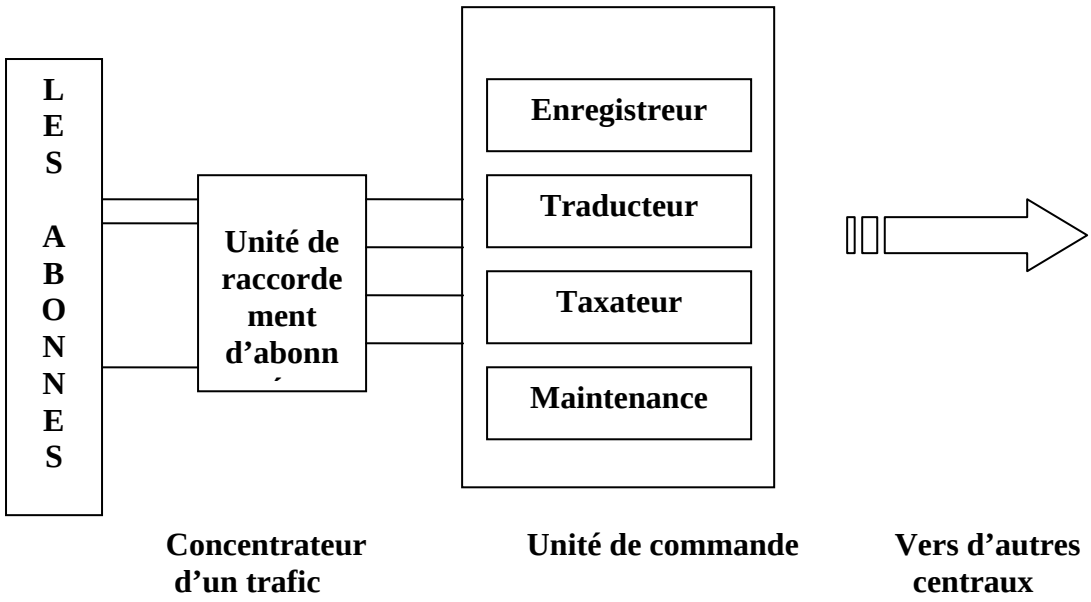


Figure I.3. Architecture D'un central téléphonique.

I.6. Communication téléphonique

L'appel téléphonique s'établie de la manière suivante (Figure(I.4)).

Considérons l'appel de A vers B au travers du commutateur local CL1, des centres de transit CT1et CT2, et du commutateur local CL2.

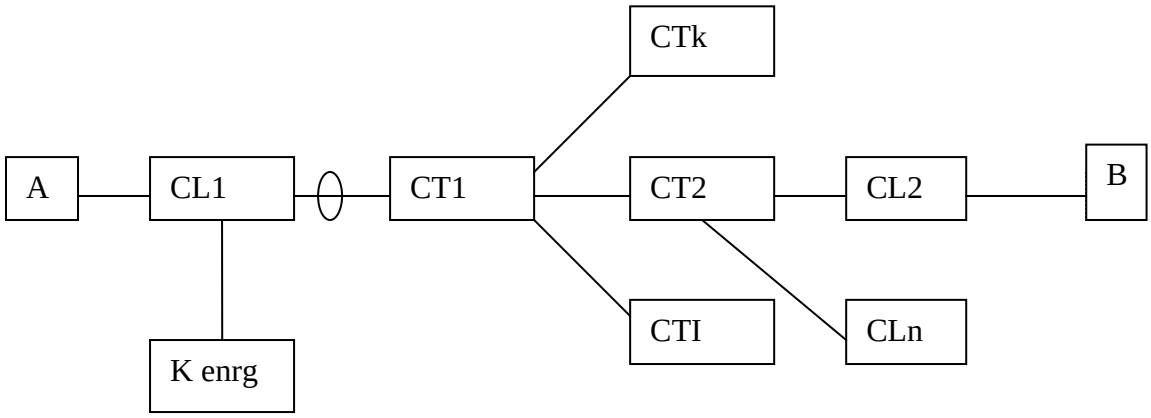


Figure I.4. Etablissement d'un appel.

Les différentes phases de l'appel sont les suivantes :

1) **décrochage** :

   L'appelant A décroche. La boucle locale est fermée. Le commutateur local de rattachement CL1, qui supervise la ligne, détecte le décrochage.

2) **présélection :**

   CL1 va rechercher un enregistreur dans un pool pour lui permettre de recevoir le numéro envoyé par A Il y a beaucoup moins d'enregistreurs que de lignes locales attachées au commutateur (concentration) : le dimensionnement est lié au trafic. Si un enregistreur est libre, A reçoit la tonalité d'invitation à numéroter ("dial-tone").

3) **enregistrement et analyse :**

   CL1 enregistre les chiffres émis par A et les analyse (traduction). L'analyse a 2 fonctions :

   - déterminer la **taxation.**

- déterminer la route qui doit être prise par l'appel : l'**acheminement** ("trafic routing").

4) sélection et acheminement :

Ayant déterminé que l'appel doit être établi vers le commutateur de transit CT1, CL1 va essayer de prendre un circuit sortant libre dans un ensemble de circuits disponibles entre CL1 et CT1 (appelé faisceau de circuits « circuit group »).

A l'intérieur du commutateur, CL1 va aussi devoir trouver un chemin reliant la ligne de A avec le circuit sortant choisi (sélection).

5) établissement de l'appel à travers le réseau :

CL1 va devoir dialoguer avec CT1 pour lui signaler le circuit choisi, lui transmettre le numéro de B,... ; l'ensemble des signaux échangés et leur protocole constituent la signalisation dans le réseau. CT1 analyse le numéro de B, en détermine l'acheminement vers CT2 et prend un circuit libre vers CT2. Le processus continu de même entreCT2 et CL2.

6) arrivée :

CL2 reconnaît B comme un de ses abonnés et connecte le circuit venant de CT2 vers la ligne d'abonné de B, achevant ainsi la mise en place d'un circuit de bout en bout entre A et B:l'ensemble des opérations exécutées jusqu'à présent constitue la phase d'établissement d'appel (le "call setup"). Trois cas peuvent se présenter :

- B est disponible.
- B est déjà en communication.
- B ne peut établir la communication.

Si B est libre**,** CL2 envoie le courant de sonnerie sur la ligne d'abonné de B et émet en arrière une tonalité de sonnerie vers A.

7) réponse de B :

Si B décroche, l'évènement est envoyé en arrière jusqu'à CL1 par la signalisation du réseau : on passe alors en phase de communication (phase active de l'appel) et on démarre la taxation...

8) **supervision** :

Pendant la phase de communication, les commutateurs supervisent la communication pour détecter le raccrochage de A ou de B.

9) **libération :**

Lorsqu'une des 2 parties A ou B raccroche, le circuit établi entre A et B est libéré (ou relâché) : c'est la phase de libération du circuit qui à nouveau met en oeuvre la signalisation. La taxation est aussi arrêtée.

I.7.Réseau sémaphore numéro 7 [3]

Parallèlement à la numérisation du réseau téléphonique commuté, la nécessité d'améliorer la rapidité des échanges de signalisation a été ressentie.

De nouveaux services comme le transfert d'appel ont été ouverts. Ils peuvent nécessiter un échange de signalisation sans établissement réel d'un circuit de communication .Il a fallu donc séparer la signalisation de la transmission et faire transiter cette signalisation sur des liaisons spécifiques, c'est la signalisation par canal sémaphore (CCS Commun Chanal Signaling) dans lequel l'information de signalisation, se rapportant à des circuits ou à des messages de gestion et de supervision, est transmise sous forme de trame sémaphore.

L'ensemble des canaux sémaphores forme un réseau spécifique dans le transfert de la signalisation appelé SS7 (Signaling System 7). Ce réseau sémaphore numéro 7 fonctionne suivant le principe de la commutation par paquets. Il est constitué des éléments suivants :

- **Points sémaphore (PS ou SP Signaling Point) :** ce sont des terminaux (des centraux téléphoniques, des serveurs et des bases de données) qui traitent la signalisationSS7.

- **Point de transfert sémaphore (PTS ou STP Signlaling Transfert Point) :** ce sont les commutateurs de paquets de réseauSS7 .Ils reçoivent et routent les messages de signalisation entrants vers la destination appropriée.

- **Point de commutation de service (SSP Service Suitching Point) ou commutateurs (CAS) :** ce sont des commutateurs à autonomie d'acheminement équipés de logiciels compatibles SS7 et relier aux extrémités des liens de signalisation, permettant l'établissement des appels .des service à valeurs ajoutées et

des échanges avec des bases de données.

- **Point de contrôle de service SCP Service Contrôle Point) :** ce sont des bases de données qui fournissent l'information nécessaire aux fonctions avancées de traitement des appels tels que les numéros spéciaux.

I.7.1.Structure d'un réseau sémaphore

I.7.1.1. Modes sémaphores

Trois modes sémaphores peuvent être utilisés, qui dépendent de la relation entre le canal et l'entité qu'il sert :

- **mode associé** : c'est la plus simple dans le quel le canal sémaphore est parallèle au circuit de parole pour lequel il permet l'échange de signalisation .il est forcément établi entre deux points sémaphores (SP). ce mode requiert un canal sémaphore entre un SP donné et tous les autres SP, ce qui n'est pas idéal .les messages de signalisation suivent alors la même route que la voix mais sur des supports différents.

- **mode non associé**:ce mode utilise un chemin différent de celui de la voix, un grand nombre de noeuds intermédiaires, à savoir les points de transfert sémaphores (STP) et impliquée dans l'acheminement des messages de signalisation les STPs sont utilisés afin de router des données de signalisation entre SPs .par ailleurs les messages à destination d'un point sémaphore peuvent empreinter des routes différentes, le fonctionnement du mode non associé et ressemblable à celui du protocole IP.

- **un mode quasi-associé**: ce mode utilise au maximum deux STP pour atteindre la destination finale, ce qui permet de minimiser le temps nécessaire à l'acheminement du message. Par ailleurs les messages acheminés vers une destination donné empruntent tous la même route.

I.7.2.Pile de protocole SS7

La structure du réseau SS7 en couches à été influencée par le mode OSI (Open System Interconnexion). SS7 est devisé en quatre niveaux représentés à la figure ci-dessous(le terme

niveau est utilisé afin de différencié du concept de couches OSI :

- niveau 1 physique
- niveau 2 liaison de donnée
- niveau 3 réseau
- niveau 4 partie utilisateur

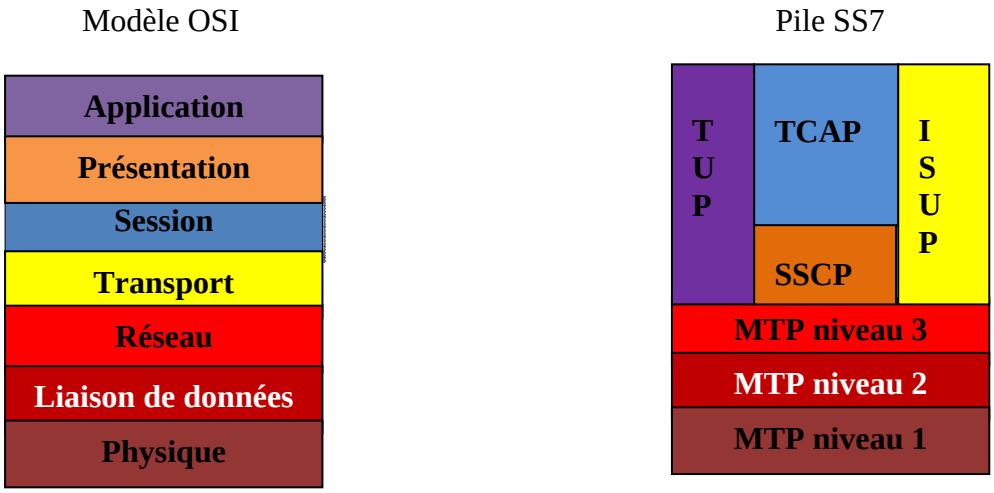


Figure. I.5. Le modèle de référence OSI et la pile de protocole SS7.

Les niveaux, un à trois, sont appelés sous-système de transfert de message (MTP Message Transfert Part) de SS7.

I.7.3. Pièce de transfert de message (MTP Message Transfer Part)

MTP prennent en charge le transfert de message de signalisation entre deux neouds de réseau sémaphore et ce de façon fiable, les principales fonctions de chacun sont présentés ci-dessous:

- **MTP niveau 1 :**MTP1 est la liaison sémaphore de données (SDL:Signaling Data Link) qui consiste en partie de canaux de transmission numérique opérant à 64kb/s et qui transporte les unités de données SS7 entre deux points sémaphores (SP).

- **MTP niveau 2**:(MTP2) concerne la procédure de contrôle de ligne nécessaire afin de fiabiliser la transmission de messages sémaphores et s'appelle un canal sémaphore .Il permet ainsi :
  - délimitation des trames sémaphores : car leurs longueurs sont variables.
  - l'alignement des trames sémaphores
  - la détection et la correction d'erreur

- la surveillance de taux d'erreur sur le canal.
- alignement initial.
- contrôle de flux.

❖ **MTP niveau 3:(**MTP3) il fournit l'acheminement et l'orientation des messages **entre** les points de signalisation grâce à l'étiquette d'acheminement et la gestion du réseau sémaphoreSS7

I.7.4.Fonction de couches applicatives (le niveau 4)

Le niveau 4 concerne les services de signalisation. Plusieurs blocs fonctionnels au niveau 4 représentent des applications spécifiques et utilisent les services de MTP. Ce niveau est subdivisé en parties suivantes :

➢ **TUP (Téléphone User Part)**

Le protocole TUP gère les fonctions de base pour le téléphone uniquement.TUP manipule les circuits analogique seulement,à cause de ce fait ,de plus en plus,ISUP remplace TUP.

➢ **ISUP (ISDN User Part)**

Offre le service de base d'établissement et de libération de circuit ainsi que des services complémentaires (identification de la ligne appelante, renvoi d'appel sur occupation, renvoi d'appel sur non réponse, renvoi d'appel inconditionnel, etc...

➢ **TCAP (Transaction Capabilité Application Parts)**

Il offre les services d'invocation à distance .un exemple d'invocation est l'interrogation d'une base de donnée du numéro vert afin d'obtenir la traduction entre un numéro vert et le numéro physique correspondant (service libre d'appel).

Différentes applications utilisent le service TCAP :

- **INAP (Intelligent Network Application Part) :** est le protocole permettant l'exécution de services à valeurs ajoutées (numéro vert, réseau privé virtuel, carte prépayée, etc...).

- **MAP (Mobile Application Part):**offre le service de mobilité du terminal ainsi que les

services complémentaires.

- **OMAP (Opération Maintenance and Administration Part) :** offre un service de gestion du réseau sémaphore N°7.

- **SCCP Signaling Connexion Control Part):**est aussi un utilisateur de MTP, il peut être considéré comme un enrichissement de MTP .il fournit avec MTP les fonctionnalités offertes par les trois couches basses du model OSI SCCP à son tour, sert des utilisateurs du niveau 4 .ISUP peut être un utilisateur de SCCP ou directement du niveau 1, 2,3 (MTP).

I.7.5.Point de transfert sémaphore STP

Les messages de signalisation sont émis d'un point sémaphore SP à un autre point sémaphore SP et transitent à travers des points de transfert STP qui peuvent jouer le rôle à la fois de SP et de STP (on parle alors de STP intégré) ou bien seulement le rôle de STP dans ce cas on parle de STPs autonomes, ces derniers ne sont pas utilisés indépendamment de leurs nature intégré ou autonome, il existe trois types de STP:

- **le STP national :** il est présent au sein d'un réseau sémaphore national, utilisée seulement le protocole national pour le réglage des messages.

- **le STP international :** il est présent au sein d'un réseau sémaphore international, il interconnecte tous les pays en utilisant les protocoles sémaphores défini par l'ITU-T.

- **le STP passerelle :** permet de traduire un protocole national et le protocole international (comme les STPs internationaux) ou encore un protocole national en un autre protocole, le type de STP est utilisé en particulier dans les réseaux cellulaires.

I.7.6. Canaux sémaphores

Un canal sémaphore est un support bidirectionnel qui permet le transfert fiable de trames sémaphores entre deux entités sémaphores adjacentes, ces canaux fonctionnent à 64 kb/s.

Les canaux sémaphores sont placés dans des groupes appelés faisceaux sémaphores.

I.7.6.1. Performances des canaux sémaphores

Les canaux sémaphores doivent être disponibles en permanence pour prendre en charge le trafic de signalisation lorsqu'un STP chute, l'autre STP de la paire (deux STPs d'une même région) doit traiter le trafic dérouté. Ainsi, lorsqu'un canal chute les autres canaux de même faisceau doivent prendre en charge son trafic, c'est pour cette raison qu'un canal sémaphore ne peut pas utiliser en situation normal plus de 40% de son débit nominal.lorsqu'un canal chute son trafic est alors renvoyé vers un autre canal qui sera utilisé à 80% au maximum de son débit nominal.Les 20% restants sont utilisés pour transporter des messages de gestion.

I.7.7.Avantage et inconvénient de signalisation SS7

Les avantages de signalisation sémaphore sont les suivants :

- possibilité de transférer de la signalisation pure indépendamment de l'établissement d'un circuit.
- forte réduction des délais de transfert de la signalisation grâce à la transmission numérique permettant de déminuer le temps d'occupation iniffecace des circuits et d'offrir un meilleur service à l'utilisateur.
- possibilité de réserver des circuits pour un appel seulement lorsque le correspondant demandé est réellement joignable.

Les inconvénients sont :

- une plus grande complexité puisqu'il faut designer le circuit auquel le message de signalisation s'attache.
- une grande sensibilité aux pannes car l'établissement d'un circuit ne garantit pas que celui-ci fonctionne réellement de plus la rupture d'un canal sémaphore entraine l'impossibilité d'établir un ensemble de communication .il faut donc mettre en place des mécanismes de défense.

I.8. Migration du réseau RTC vers le réseau NGN

Du point de vue de services offerts, l'architecture du réseau existant RTC ne fournit pas assez. Afin d'enrichir et d'améliorer la qualité des services, l'architecture du réseau de nouvelle génération (NGN) a été conçue pour fournir des services intégrés à haut débit basés sur des paquets IP.

Grace à ce concept de réseau nouvelle génération (NGN), il a été rendu possible de transmettre la voix, les données, la vidéo sur des réseaux IP.

II.1. Introduction [4]

La problématique de passage à une architecture NGN (Next Generation Network) du cœur de réseau fixe des opérateurs historiques s'inscrit avant tout dans une logique de diminution des coûts, avec le passage à une infrastructure unique basée sur IP pour le transport de tout type de flux, voix ou données, et pour toute technologie d'accès (RTC, WiFi, etc.). L'impact majeur d'un passage à une architecture NGN pour les réseaux de téléphonie commutée est que le commutateur traditionnel est scindé en deux éléments logiques distincts : le media Gateway pour assurer le transport et le soft switch pour assurer le contrôle d'appel. Cette évolution permet théoriquement des gains en termes de performance et d'optimisation des coûts, mais elle peut aussi faciliter le déploiement de nouveaux services. Les solutions apportées par le NGN ne sont pas déployées dans une perspective de remplacement complet des solutions de réseau commuté traditionnelles, utilisées pour le transport du trafic voix. Dans certains cas, l'utilisation de soft switch est contingentée aux services voix sur IP, et dans d'autres, l'utilisation de soft switch n'intervient qu'en des nœuds de commutation dont les équipements TDM sont arrivés en fin de vie. Dans ce dernier cas, les opérateurs sont dans une logique de remplacement de leurs solutions.

II.2. Définition et description d'un réseau NGN [4]

L'acronyme NGN (Next Génération Network) est un terme générique qui englobe différentes technologies visant à mettre en place un concept, celui d'un réseau convergent multiservices.

De nouvelles solutions technologiques sont déployées dans les réseaux NGN. Ce dernier utilise un ensemble d'équipements qui jouent le même rôle qu'un commutateur traditionnel, mais qui sont désormais séparés en composants distincts :

- **Le « softswitch » :** est la solution qui gère dans un réseau NGN l'intelligence du service de commutation (gestion de tables d'appels, gestion des plans de numérotation). Toutefois, ce softswitch n'est plus associé à un point physique du réseau, et ne gère plus les liens physiques du réseau, comme c'était le cas dans un réseau TDM.

- **Le « media gateway » :** dont le rôle est d'assurer la gestion (disponibilité, détection de fautes) de la couche physique du réseau. Cette couche physique peut être le réseau

de transmission, ou le réseau d'accès. Dans le cas où il s'agit du réseau d'accès, la fonction de media gateway peut être embarquée dans l'équipement d'accès lui-même.

II.2.1. Modèle d'architecture NGN en couche [4]

Le passage à une architecture de type NGN est notamment caractérisé par la séparation des fonctions de commutation physique et de contrôle d'appel. L'architecture NGN introduit un modèle en couches, qui scinde les fonctions et équipements responsables du transport du trafic et du contrôle. Il est possible de définir un modèle architectural basé sur cinq couches successives, représenté dans la figure (II.1):

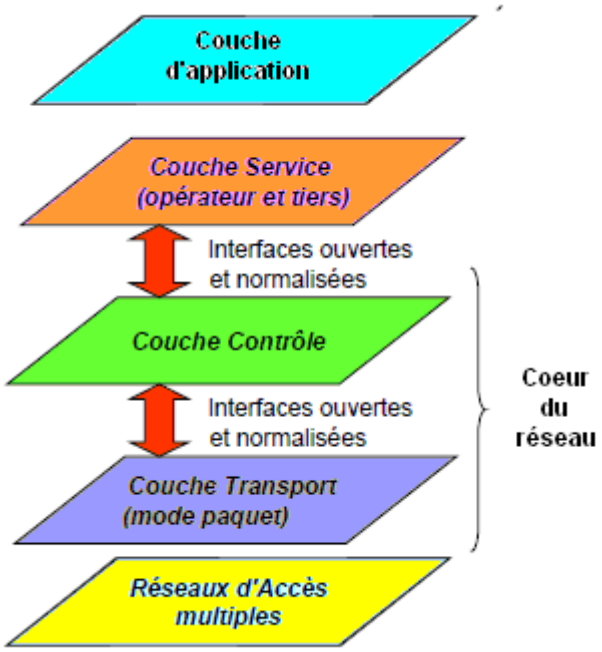


Figure.II.1. Architecture générale d'un réseau NGN.[4]

- **Couche d'accès :** qui regroupe les fonctions et équipements permettant de gérer l'accès des équipements utilisateurs au réseau via des supports de transmission (câble, fibre optique, xDSL, boucle locale radio et réseaux mobiles). Les entités de cette couche sont le Media Gateway (MG) et Signaling Gateway (SG) :
  - **Media Gateway** est responsable de l'adaptation des protocoles de transport aux différents types de réseaux physiques disponibles (RTC, IP, ATM, …), et qui a pour rôle :
    - ✓ La conversion du trafic TDM en trafic paquets IP
    - ✓ Transmettre selon les instructions du Media Gateway Controller (MGC) le flux media reçu.

- **Signaling Gateway (SG)** : Cet équipement a pour rôle de convertir la signalisation échangée entre le réseau NGN et les réseaux interconnectés. Cette fonction est souvent la plus implémentée physiquement dans le media Gateway

- **Couche de transport :** La couche transport est constituée elle-même d'un système de transmission et d'un système de communication. Le niveau de transmission correspond au réseau physique de liens entre les nœuds, le réseau de commutation ou de routage correspond aux nœuds qui permettent d'acheminer une communication à travers le réseau de transmission en fonction de sa destination contrairement au réseau conventionnel ou l'opérateur de télécommunications possède différents réseaux de commutation dédiés (voix, données,….)

- **Couche de contrôle :** qui gère l'ensemble des fonctions de contrôle des services en général, et de contrôle d'appel en particulier pour le service voix. L'équipement important à ce niveau dans une architecture NGN est le serveur d'appel, plus communément appelé « softswitch », qui fournit, dans le cas de services vocaux, l'équivalent de la fonction de commutation dans un réseau NGN.

- **Couche d'exécution des services :** qui regroupe l'ensemble des fonctions permettant la fourniture de services dans un réseau NGN. En termes d'équipements, Cette couche regroupe deux types d'équipement : les serveurs d'application (ou application servers) et les « enablers », qui sont des fonctionnalités, comme la gestion de l'information de présence de l'utilisateur, susceptibles d'être utilisées par plusieurs applications. Cette couche inclut généralement des serveurs d'application SIP, car SIP (Session Initiation Protocol) est utilisé dans une architecture NGN pour gérer des sessions multimédias en général, et des services de voix sur IP en particulier.

- **la couche applications :** pour les différents services et applications susceptibles d'être offerts dans une architecture NGN. Il peut naturellement s'agir de services IP, mais les opérateurs s'attacheront aussi à supporter les services vocaux existants de réseau intelligent (renvoi d'appel, etc.) dans le cadre d'une migration vers une architecture NGN. Cette couche applications regroupe aussi l'environnement de création de services, qui peut

être ouvert à des fournisseurs de services tiers. Le développement d'applications s'appuie sur les serveurs d'application et les enablers de la couche d'exécution des services.

Ces couches sont indépendantes et communiquent entre elles via des interfaces ouvertes. Cette structure en couches est sensée garantir une meilleure flexibilité et une implémentation de nouveaux services plus efficace. La mise en place d'interfaces ouvertes facilite l'intégration de nouveaux services développés sur un réseau d'opérateur mais peut aussi s'avérer essentielle pour assurer l'interconnexion d'un réseau NGN avec d'autres réseaux qu'ils soient NGN ou traditionnels.

II.2.2. Rôle d'un softswitch dans une architecture NGN [4]

Dans une infrastructure NGN, un Softswitch n'est autre qu'un serveur informatique, doté d'un logiciel de traitement des appels vocaux. Le trafic voix est en général pactisé par le media gateway, et pris en charge par les routeurs de paquets du réseau de l'opérateur. Un softswitch va identifier les paquets voix, analyser leur contenu pour détecter le numéro vers lequel ils sont destinés, confronter ces numéros avec une table de routage (qui indique ce que le softswitch doit faire en fonction de chaque numéro), puis exécuter une tâche (par exemple transmettre ou terminer).

Physiquement, un softswitch peut être implanté sur un serveur dédié ou bien être installé directement sur un équipement différent comme un media gateway ou même un commutateur traditionnel TDM. Dans ce cas, on parlera d'architecture complètement distribuée.

II.2.3. Rôle des media gateways dans une architecture NGN [4]

Les Media Gateway constituent le deuxième élément essentiel déployé dans un réseau NGN. Un media gateway peut par exemple se positionner entre le réseau de commutation circuit et le réseau de commutation de paquets. Dans ce cas, les media gateways transforment le trafic circuit TDM en paquets, la plupart du temps IP, pour que ce trafic puisse ensuite être géré par le réseau NGN.

II.3. Les protocoles utilisés dans NGN [5]

L'architecture de NGN est caractérisée par des couches qui sont interconnectées par des interfaces utilisant des protocoles standards. Le réseau TDM est interconnecté avec NGN grâce à des interfaces basées sur des protocoles. La figure (II.2) en décrit quelques-uns des protocoles standards utilisés dans l'architecture NGN.

Un protocole est une description formelle de règles et de conventions à suivre dans un échange d'informations que se soit pour acheminer les données jusqu'au destinataire ou pour que ce dernier comprenne comment doit il utiliser les données reçues.

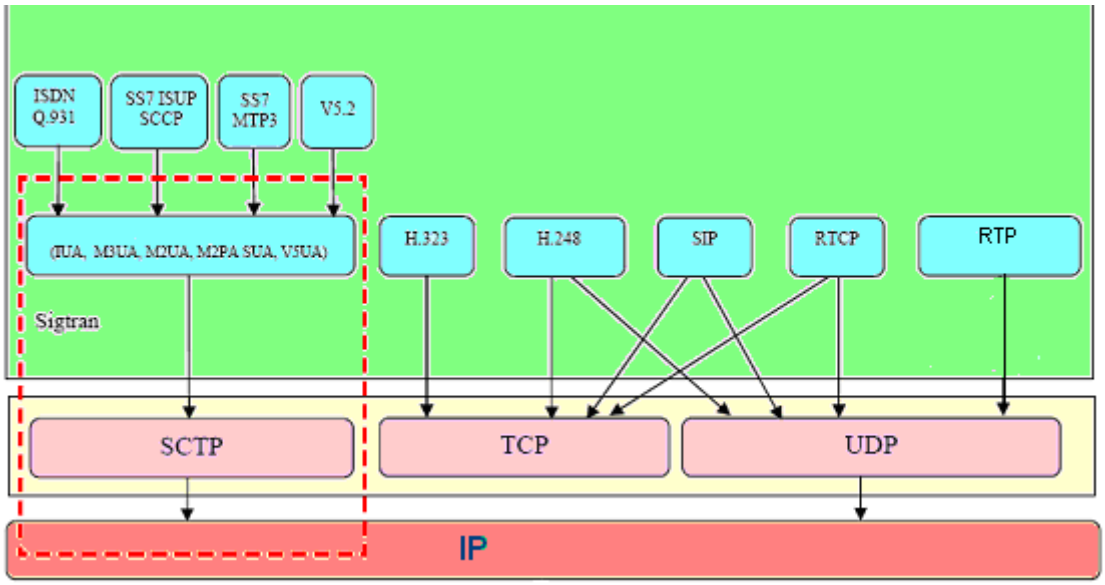


Figure. II.2. Protocoles utilisés dans NGN.

La figure (II.3) montre comment les protocoles illustrés dans la figure(II.2) sont utilisés pour la signalisation dans l'environnement NGN

Les messages de contrôle de signalisation sont transportés en utilisant les protocoles : SIGTRAN, H.248, SIP, H.323 etc.

Les flux media (audio, vidéo ou données….) sont transportés à travers RTP (Real-time Transport Protocol) .RTCP (Real-time Transport Control Protocol) contrôle la transmission des flux à travers RTP.

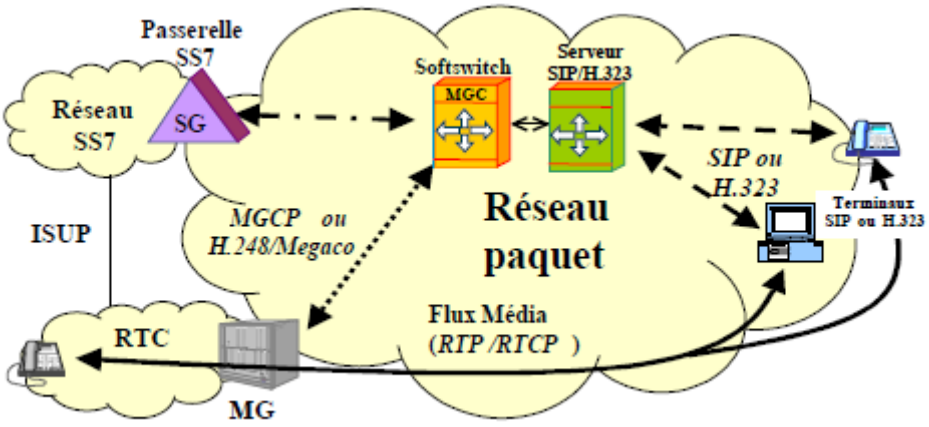


Figure. II.3. Protocoles dans NGN.

II.3.1. Protocole MGCP [6]

MGCP (Media Gateway Control Protocol), décrit par la RFC 3435, et définit par son architecture CLIENT / SERVEUR ou plus précisément Maître /esclave. Ainsi la gestion des services d'appels est centralisée et assuré coté maître tandis que les terminaux coté clients ne gèrent que les fonctionnalités basiques d'appels et vont recevoir les instructions du maître.

Le MGCP assure le contrôle et l'échange des messages de signalisation entre ses passerelles, réparties dans un réseau IP.

II.3.1.1. Architecture du protocole MGCP

L'architecture du protocole MGCP repose donc sur deux entités :

- **Terminaux MGCP** : situés coté client sont des passerelles chargé de recevoir et rapporter les instructions du contrôleur central (call agent).elles accomplissent les taches suivantes :
  - conversion du signal
  - adaptation au support
  - Compression des données
  - conversion de la signalisation
  - Multiplexage
  - Mise en paquets

- **Call agent :** est le « chef d'orchestre » du réseau MGCP, il va se charger de piloter et d'administrer les passerelles de manière centralisée. Il est spécifiquement responsable de l'établissement, de la maintenance et de la terminaison des appels établis entre des terminaux appartenants à des réseaux de nature différente.

Le call agent et les terminaux vont communiquer via des échanges de transactions en utilisant le port UDP 2727 (call agent) et 2427 (terminaux). Les flux voix sont gérés également par le protocole RTP/RTCP comme en SIP et H.323.Voir la figure (II.4).

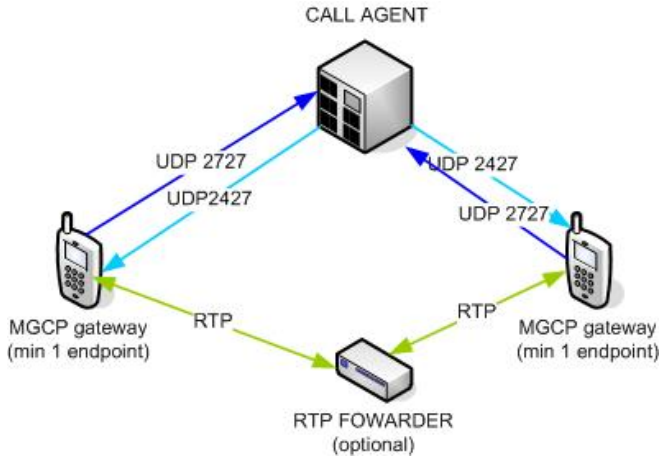


Figure .II.4. Mise en relation entre deux endpoints.

Il est important de préciser que MGCP est un protocole dédié a l'interconnexion des terminaux IP et PSTN, ainsi au sein du cœur de réseau il est tout a fait possible d'utiliser les protocoles H.323 ou SIP pour les interconnexions, MGCP n'intervenant que sur la bordure du cœur de réseau. Voir la figure (II.5).

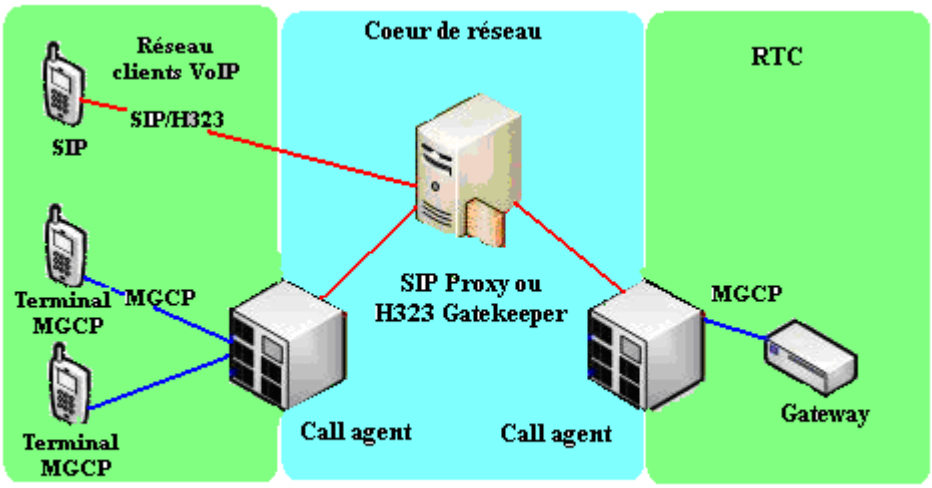


Figure II.5. Positionnement du protocole MGCP dans le réseau NGN.

II.3.1.2.Requêtes

Le protocole MGCP définit neuf requêtes (commande) permettant de spécifier l'action à effectuer. Les commandes sont lancées entre le call agent et les passerelles (MG).Comme MGCP est un protocole de type maître/esclave, on distingue donc deux catégories de commande : celles qui sont lancées par call agent vers une ou plusieurs passerelles et celles qui vont dans l'autre sens

Les neufs requêtes et leurs significations sont récapitulées au tableau(II.1)

Format complet	Format abrégé	Signification
AUDITCONNECTION	AUCX	Elle demande la détection de paramètres consternants une connexion
AUDITENDPOINT	AUEP	Elle demande la détection d'informations consternants un terminal
CREATECONNECTION	CRCX	Elle demande la création d'une connexion
DELETECONNECTION	DLCX	Elle demande la terminaison d'une connexion établie
ENDPOINTCONFIGIRATION	EPC	Elle est utilisée pour la configuration du type de codage des flux qui sont reçus par un terminal téléphonique sur le lien téléphonique

		traditionnel (c.-à-d. le lien circuit, non IP)
MODIFYCONNEXTION	MDCX	Elle permet de modifier les paramètres associés à une connexion déjà établie
NOTIFICATIONREQUET	RQNT	Elle demande à une passerelle de surveiller des événements particuliers concernant un terminal
NOTIFY	NTFY	Elle fait suite à une requête envoyée par le call agent .Elle indique que l'événement pour lequel le call agent avait sollicité une alerte survenue.
RESTARTINPROGRESS	RSIP	La passerelle peut avertir le call agent de l'indisponibilité d'un ou de plusieurs terminaux d'extrémités au moyen de cette commande

Tableau. II.1. Requêtes.

II.3.1.3. Gestion des appels et services de l'abonné

Dans un protocole MGCP, le call agent a la lourde tache de gérer toutes les connexions et services offerts à l'abonné. Ainsi lorsque l'abonné décroche son terminal, l'endpoint de ligne associé va envoyer une commande NOTIFY contenant les informations sur l'événement (décroché du combiné, saisie de digit…).

Le call agent va alors analyser la commande et envoyer au terminal une commande CREATE CONNEXION qui va créer une connexion sur l'endpoint du terminal avec des paramètres comme l'identifiant de l'appel, le codec souhaité, les délais de paquetisation, la bande passante autorisée…

L'abonné compose son appel, les instructions sont envoyées au call agent qui va interroger la base de donnée opérateur classe 5 et relayer l'appel soit sur l'endpoint de ligne associé à un abonné. MGCP faisant partie du même opérateur (présence de son endpoint dans la base abonnée classe 5) ou sur une gateway si l'appel est destiné à un abonné externe situé sur le RTC.

Une fois l'appel terminée, le call agent envoie une commande DELETE CONNEXION, si le raccroché provient de l'appelé, ou le terminal envoie un NOTIFY si cela vient de l'appelant.

La figure(II.6) illustre la gestion des appels et services de l'abonné

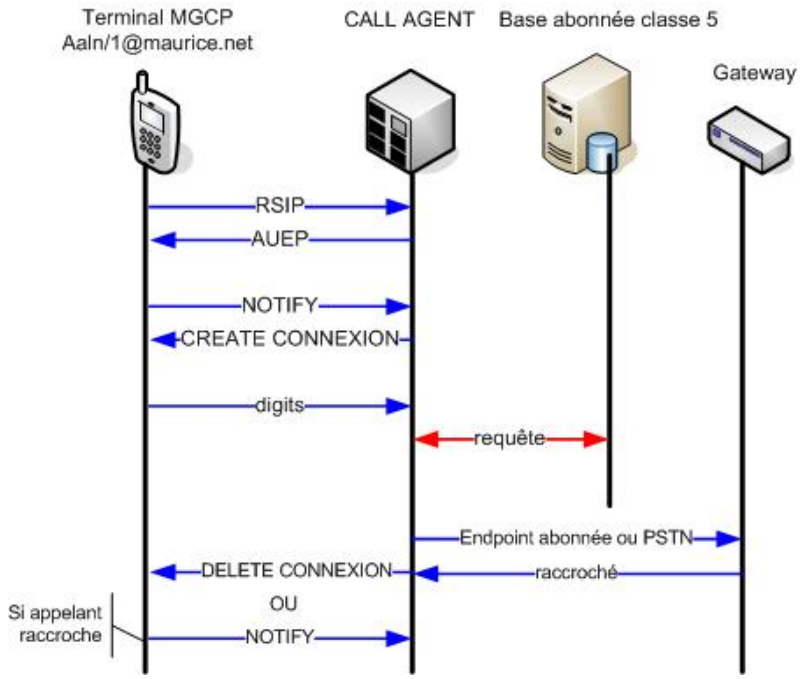


Figure. II.6. Gestion des appels et services de l'abonné.

II.3.2. H.248/Megaco (Media Gateway Control Protocol) [5]

Ce protocole est le résultat de travail commun d'IETF et ITU. H.248 est le nom donné par l'ITU et Megaco par IETF. H.248/MEGACO est conçu pour fournir une architecture centralisée .Il est dérivé du MGCP et possède des améliorations par rapport à celui-ci :

- il supporte les services multimédia et de vidéoconférence
- il utilise des codages en mode texte
- possibilité d'utiliser UDP, TCP et SCTP

II.3.2.1. Positionnement du H248 dans le réseau NGN

H.248/Megaco est un protocole de signalisation entre MG et MGC (appelé aussi Call Agent ou Softswitch).La figure (II.7) représente le positionnement du MGCP et H248/MeGaCo dans le réseau NGN.

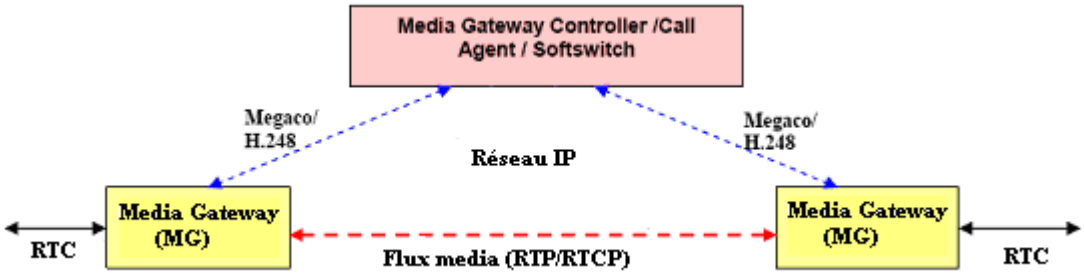


Figure II.7. Positionnement du H248 dans un réseau NGN.

II.3.2.2. Modèle de connexion MEGACO

Le modèle de connexion du protocole MEGACO est un modèle orienté objet. Il décrit les entités logiques ou objets au sein du MG (Media Gateway) qui peuvent être contrôlés par le MGC (Media Gateway Controller). Les MSC-Server et GMSC-Server correspondent à des MGCs. Le CS-MGW équivaut à un MGW. Les principales abstractions utilisées dans ce modèle de connexion sont les terminaisons et les contextes. Une terminaison est une entité logique dans le MG qui commence ou termine un ou plusieurs flux. Une terminaison est un objet abstrait qui représente des ports connectés au MG.

II.3.2.2.1. Terminaison

La terminaison est une entité logique dans une MG, représentant des ports connectés à celui-ci, capable d'envoyer ou/et de recevoir un ou plusieurs flux media. Elle est décrite par un ensemble de caractéristiques qui sont regroupés dans un ensemble de descripteurs inclus dans les commandes.

Chaque terminaison définit un seul contexte et désignée par un identificateur de terminaison unique (termination ID) choisi par le MG.

Il y a deux types de terminaison

-une terminaison qui représente une entité physique et dite semi-permanente, exemple : un circuit de parole raccordé à un MG

-Une terminaison représentant des flux temporaires tels que les flux RTP n'existe que pendant la durée de l'appel correspondant.

II.3.2.2.2. Contexte

Le contexte est une association entre les terminaisons.il existe un type spécial de contexte, le contexte "null" qui contient toutes les terminaisons semi-permanentes non

associées à une autre terminaison.par exemple, dans un MG, tous les circuits de parole au repos sont représentés par des terminaisons dont le contexte « null ».

Contexte ID est l'identifiant du contexte.

La figure (II.8) décrit les concepts de contexte et de terminaison. L'astérisque encadré de chaque contexte représente l'association logique des terminaisons appartenant au contexte.

Le premier contexte actif dans le MGW représente un appel avec trois participants. Le second contexte est le contexte « null ». Le troisième contexte correspond à un appel classique entre deux participants.

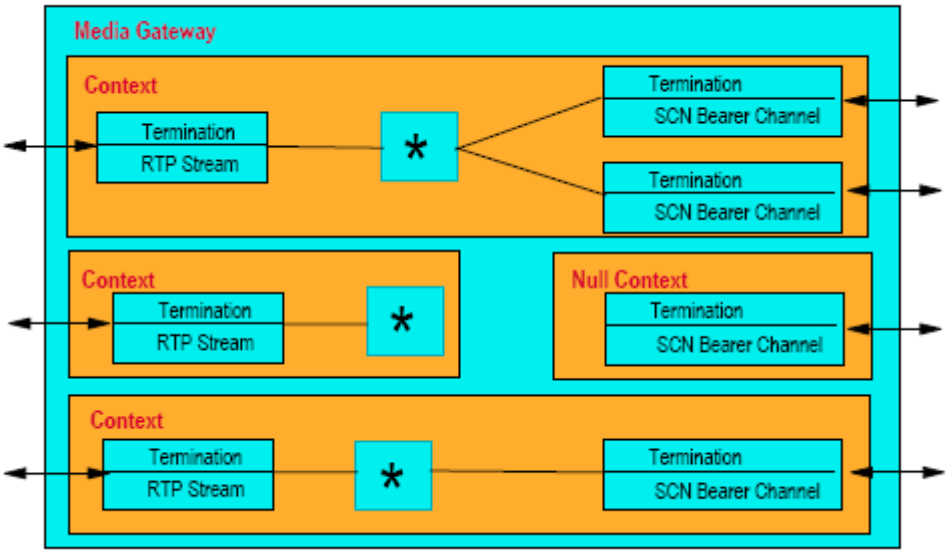


Figure II.8. Contextes et terminaisons MEGACO.

II.3.2.3.Commandes MEGACO

Le protocole MEGACO/H.248 définit huit commandes permettant la manipulation des entités logiques du modèle de connexion, à savoir les contextes et les terminaisons.

La majorité des commandes est émise par un MGC à un MG. Il s'agit des commandes : Add, Modify, Subtract, Move, AuditValue et AuditCapabilitie, Notify et ServiceChange. Deux commandes peuvent être émises d'un MG à un MGC: Notify et ServiceChange

- **Add** : La commande Add ajoute une terminaison à un contexte. Si la commande ne spécifie pas le contexte dans lequel ajouter la terminaison, un nouveau contexte est alors créé. Si la commande ne spécifie pas un identificateur de terminaison (TerminationID) mais le caractère spécial ($), le MG crée une terminaison

temporaire, lui associe un identificateur et l'ajoute au contexte, par contre, une terminaison semi-permanente est connue du MGC et une commande Add sur ce type de terminaison précise l'identifiant de la terminaison.

- **Modify** : La commande Modify permet de modifier les valeurs des propriétés d'une terminaison.

- **Subtract :** La commande Subtract soustrait une terminaison d'un contexte et retourne des statistiques relatives à l'activité de la terminaison dans ce contexte. La commande Subtract appliquée à la dernière terminaison dans un contexte supprime le contexte. Une commande Subtract appliquée à une terminaison semi-permanente déplace cette terminaison dans le contexte « null ». Cette même commande appliquée à une terminaison temporaire supprime la terminaison.

- **Move :** La commande Move déplace une terminaison de son contexte à un autre contexte. Move ne peut pas être utilisée afin de déplacer une terminaison du ou au contexte « null » ; en effet, ce sont les commandes Add et Subtract respectivement qui réalisent ces opérations.

- **AuditValue** : La commande AuditValue retourne la valeur courante des propriétés, événements, signaux et statistiques d'une ou plusieurs terminaisons.

- **AuditCapabilities :** La commande AuditCapabilities retourne les valeurs des propriétés, des signaux et événements associés à une ou plusieurs terminaisons. A la différence de la commande AuditValue, AuditCapabilities retourne l'ensemble des valeurs possibles.

- **Notify :** La commande Notify permet à un MG d'informer un MGC de l'occurrence d'événements sur une terminaison du MG. Les événements à rapporter ont été spécifiés par le MGC dans les commandes Add ou Modify.

- **ServiceChange :** Le MG utilise la commande ServiceChange afin d'informer un MGC qu'une terminaison ou un groupe de terminaisons est sur le point d'être mis hors service ou vient d'être remis en service. Cette commande est aussi émise par un MGC pour

informer un MG que ce dernier doit passer sous le contrôle d'un autre MGC. A la réception de ce message, le MG émet une commande ServiceChange vers le nouveau MGC pour formaliser l'établissement d'une association. Le MGC peut également utiliser cette commande pour demander à un MGW de mettre en service ou hors service une terminaison ou un groupe de terminaisons. Enfin, le MG mis sous tension notifie sa présence à son MGC en utilisant la commande ServiceChange.

II.3.2.4.Transactions

Les commandes et leurs réponses sont passées entre le MGC et le MGW dans des transactions, identifiées par un identificateur de transaction (transactionID). Une transaction consiste en une ou plusieurs actions. Une action est un ensemble de commandes s'appliquant à un contexte donné. Chaque action spécifie donc un identificateur de contexte (contextID) et des commandes à appliquer au contexte.

Il existe trois types de transaction :

- TransactionRequest
- TransactionReply
- TransactionReply

II.3.2.4.1. TransactionRequest

Une transactionRequest est invoquée par l'émetteur. Une requête contient une ou plusieurs actions, chacune identifiant le contexte considéré et les commandes à exécuter sur ce contexte.

II.3.2.4.2. TransactionReply

Après avoir exécuté l'ensemble des commandes, le récepteur retourne une transactionReply. Cette dernière contient une ou plusieurs actions, chacune identifiant le contexte considéré et une ou plusieurs réponses par contexte.

II.3.2.4.3. TransactionPending

Une transactionPending est une réponse intermédiaire permettant d'indiquer à l'émetteur que sa transactionRequest a bien été reçue et qu'elle est en cours de traitement.

II.3.2.5. Relation entre commande, transaction et action

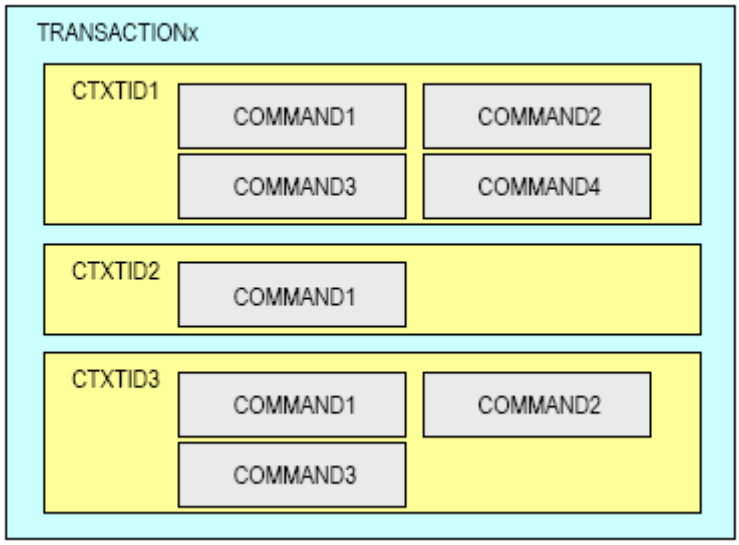


Figure II.9. Relation entre commande, transaction et action.

II.3.3. SIGTRAN (Signaling Transport)

Sigtran a été défini par IETF (Internet Engineering Task Force) qui est un protocole de signalisation du réseau NGN base sur le protocole IP.

Sigtran fait l'adaptation et le transport des différentes signalisations telles que SS7, ISDN, V5, UMTS... etc., à travers un réseau IP.

II.3.3.1. Pile SIGTRAN [5]

La pile de ce protocole est composée de trois couches : IP, SCTP et UA, elle est représentée dans la figure (II.10) :

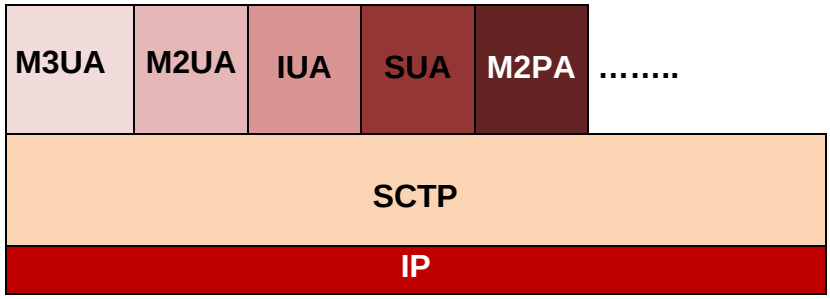


Figure .II.10. Pile du protocole SIGTRAN.

- **La couche IP :** La fonction d'IP est de délivrer des paquets IP là où ils sont supposés aller, l'IP est considéré comme le protocole le plus convenable pour transporter les messages, il fournit un chemin effectif pour le transport des données de l'utilisateur. .

- **Le protocole SCTP (Stream Control Transmission Protocol):** ce protocole est désigné par l'IETF pour le transport des messages de signalisation à travers le réseau IP. Il a les caractéristiques suivantes :
  - ✓ fonctionne pour la plus parts des applications internet.
  - ✓ fournit plusieurs fonctions de signalisation.
  - ✓ peut être utilisé pour les applications exigeant du monitoring et de la détection de perte.
  - ✓ protocol unicast, oriente message.
  - ✓ supporte le multi-streaming (partitionnement des données dans plusieurs flux).
  - ✓ supporte le multi-homing (support d'adresse IP multiple pour la redondance)

- **Les couches UA (User Adaptation) :** ce sont les couches utilisatrices supérieures du SCTP, elles représentent les modules d'adaptation de la signalisation du réseau de commutation par circuit SCN (Switched Circuit Network) par exemple : le M2UA, M3UA, IUA, M2PA et SUA.

  - **Couche M2UA (SS7 MTP2-User Adaptation Layer Protocol):** M2UA est un protocole pour le transport de messages de signalisation MTP3 à travers IP en utilisant les services de SCTP. Ce protocole fournit le service **MTP2** dans une relation « peer to peer » (égal à égal) telle que la communication entre SG et MGC, voir la figure (II.11)

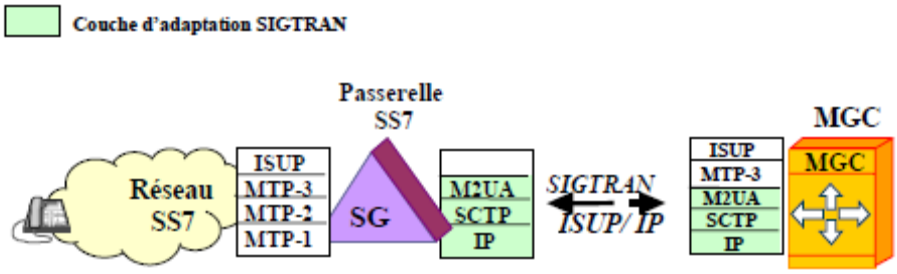


Figure .II.11. La couche d'adaptation M2UA fournit par SIGTRAN

- **M2PA (MTP2 peer-to-peer Adaptation Layer Protocol):** Le protocole M2PA est la couche entre le SCTP et le MTP3 , il a plusieurs objectifs:

  - ✓ il fournit un mécanisme pour le transport de signalisation MTP3 en utilisant SCTP
  - ✓ il permit la communication sans coupure entre les pairs de l'utilisateur MTP2 dans le réseau SS7 et réseau IP.

- **M3UA (MTP3 User Adaptation Layer Protocol) :** M3UA est la couche d'adaptation de l'utilisateur SS7 MTP3, comme le montre la figure (II.12), il fournit le service fondamental de communication pour les utilisateurs MTP3 à travers le réseau IP, afin d'effectuer l'interfonctionnement entre TDM SS7 et IP.

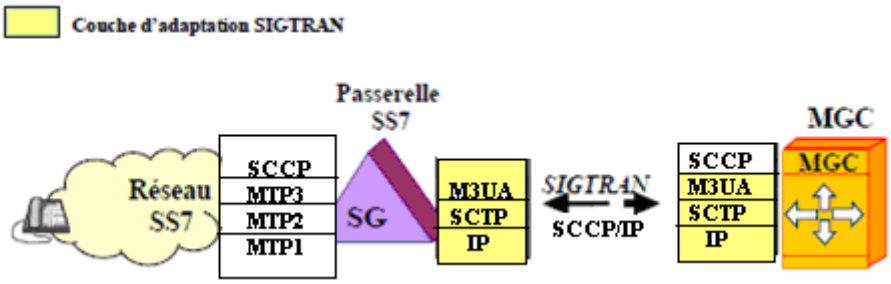


Figure .II.12. La couche d'adaptation M3UA fournit par SIGTRAN.

Le protocole de la couche M3UA qui remplace MTP3 sur la pile SS7 a deux buts :

- ✓ fournir un mécanisme pour le transport de la signalisation d'utilisateur SS7 MTP3 (ISUP, SCCP) en utilisant SCTP.
- ✓ permettre la communication sans coupure entre les pairs utilisateurs MTP3 de SS7et du domaine IP

- **SUA (Signalling Connection Control Part User Adaptation Layer Protocol) :** SUA est optimisé pour le transport des applications de la couche TCAP. En s'associant avec le protocole SCTP, SUA remplace des composants de la pile SS7 y compris SCCP.SUA agit en tant que porteur pour SCCP et le TCAP tout en maintenant toutes les caractéristiques du réseau SS7.Bien que SUA soit un excellent accès aux services à valeurs

ajoutées, l'établissement d'un appel basé sur ISUP exige toujours les services de MTP3

- **IUA (ISDN User Adaptation Layer Protocol) :** IUA définit un protocole pour le transport des messages d'utilisateurs RNIS Q.921 à travers IP en utilisant le protocole SCTP.

II.3.3.2. Positionnement du protocole SIGTRAN dans un réseau NGN

SIGTRAN est utilise dans les connexions du MGC avec SG pour le transfert de la signalisation d'un réseau SCN à travers un réseau IP. La figure (II.13) représente la position du protocole dans le NGN.

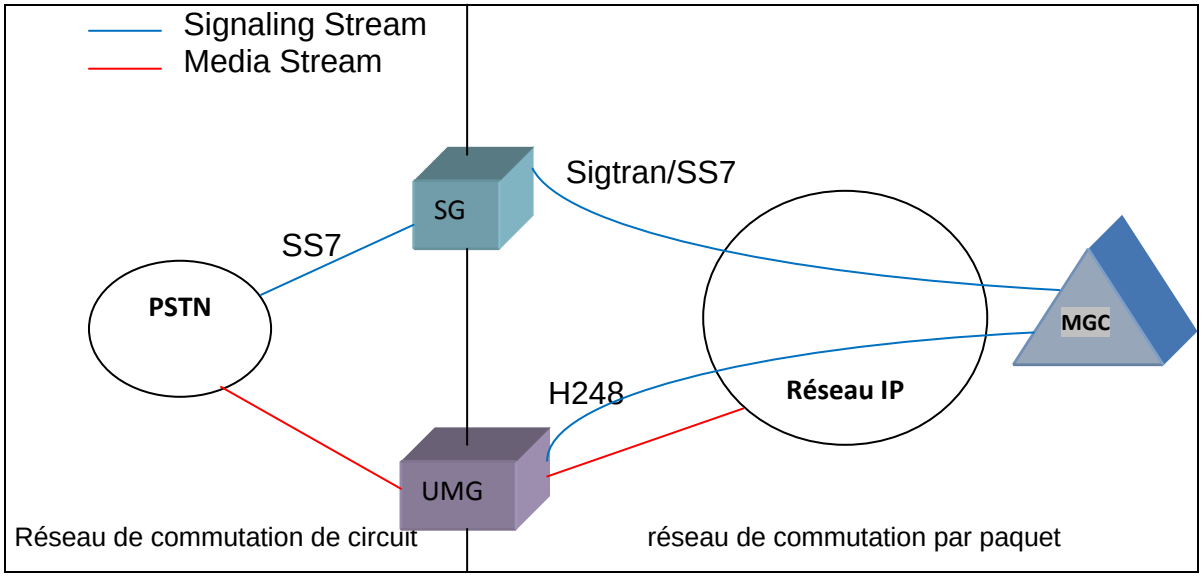


Figure II.13. Positionnement du protocole SIGTRAN dans un réseau NGN.

La signalisation du SCN est accédée par la SG et les flux medias sont accédés par la MG . La SG met en paquet la signalisation et les transmet au MGC.Ce dernier traite la signalisation et contrôle son transport vers la MG via le protocole H248 ,réalisant de ce fait l'interfonctionnement entre le réseau de commutation par circuit et le réseau de commutation par paquet.

II.3.4. Le protocole H323 [7]

Ce protocole est dérivé du protocole H.320 utilisé dans RNIS (RNIS: Réseau Numérique à Intégration de Services), il est très proche du protocole SIP et il en existe cinq

versions, de V1 à V5. Il regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. Très utilisé dans les applications de vidéoconférences, ce protocole est considéré comme plus élaboré que son concurrent SIP.

II.3.4.1.Terminologie

II.3.4.1.1.Terminaux

Un terminal H.323 agit en tant que "end-point" dans une conversation et communique avec un autre terminal H.323.

II.3.4.1.2. Multipoint Control Unit (MCU)

Techniquement, une conférence téléphonique est un appel multipoint, signifiant que les multiples "endpoints" de la conversation participent au même appel. Un point de contrôle multiple (MCU=Multipoint Control Unit) H.323 manipule la signalisation pour ajouter et enlever des participants d'une conférence téléphonique, et le MCU (Multipoint Control Unit) gère également de multiple flux audio et/ou vidéo simultanément. Le processus qui gère les flux audio et vidéo exige une capacité de traitement.

II.3.4.1.3.Codecs

Les codecs jouent un rôle prépondérant dans la numérisation de la voix. En effet, les codecs permettent la compression et la décompression d'un signal audio dans un contexte temps réel. Ces compressions ou décompressions s'effectuent selon des algorithmes de compression permettant de réduire la taille d'un signal (dans notre cas, il s'agit de réduire la taille du signal audio afin de rendre les paquets IP le plus petit possible).

II.3.4.1.4. Gatekeeper

Pour empêcher la saturation, un gatekeeper H.323 peut servir de «policier du trafic», et maintenir la bande passante disponible. Avant d'établir un appel, une passerelle H.323 peut demander la permission du gatekeeper H.323. Si la bande passante est disponible pour un appel, le gatekeeper accorde la demande de connexion, si non le gatekeeper refuse cette demande, protégeant de ce fait les appels vocaux originaux contre une saturation de bande passante qui serait provoquée par un appel supplémentaire.

II.3.4.1.5.Portier

C'est le composant le plus essentiel du système H.323 et expédie les fonctions d'un "directeur". Il agit en tant que point central pour tous les appels dans sa zone et fournit des services aux points finaux enregistrés.

II.3.4.2.La pile du protocole H323

H.323 ressemble davantage à une association de plusieurs protocoles différents représentés dans la figure (II.14) et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

Les messages de signalisation sont ceux que l'on envoie pour demander d'être mis en relation avec une autre personne, qui indiquent que la ligne est occupée, que le téléphone sonne… Cela comprend aussi les messages que l'on envoie pour signaler que tel téléphone est connecté au réseau et peut être joint de telle manière.

En H.323, la signalisation s'appuie sur le protocole RAS (*Registration Admission Status*) pour l'enregistrement et l'authentification, et le protocole Q931 pour l'initialisation et le contrôle d'appel. La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations qu'on va s'échanger. Il est important que les téléphones (ou systèmes) parlent un langage commun s'ils veulent se comprendre. Il serait aussi préférable, s'ils ont plusieurs alternatives de langages qu'ils utilisent le plus adapté. Il peut s'agir du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Le protocole utilisé pour la négociation de codec est le H245 .Le transport de l'information s'appuie sur le protocole RTP qui transporte la voix, la vidéo ou les données numérisées par les codecs. On peut aussi utiliser les messages RTCP pour faire du contrôle de qualité, voire demander de renégocier les codecs si, par exemple, la bande passante diminue.

Pour le contrôle et la signalisation : H.225 H.245 Q.931 RTCP

Pour la voix : G.711 G.722 G.723 G.726 G.728 G.729

Pour la vidéo : H.261 H.263 H.263+ H.264

Pour les données : T.123 T.124 T.125

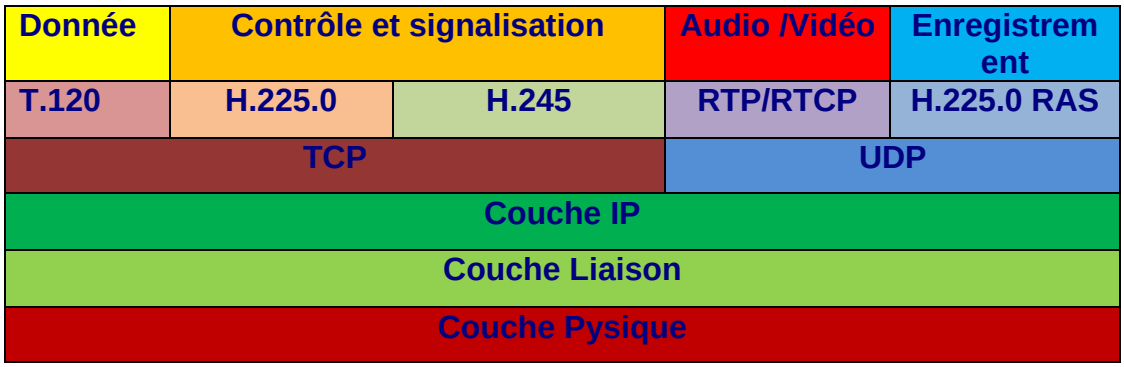


Figure II.14. Pile du protocole H323.

II.3.4.3. Fonctionnement de H.323

Les divers protocoles définissant le standard H.323 servent à établir de la signalisation, négocier des codecs et transporter l'information. Nous allons brièvement décrire l'intérêt de chacun:

- La signalisation est la première étape réalisée lors d'un appel. L'appelant émet une demande de mise en relation avec un destinataire. L'équipement de ce dernier peut alors indiquer que la ligne est libre et que le téléphone peut donc sonner ou au contraire que la ligne est en cours d'utilisation.
- La négociation est le processus permettant de s'accorder mutuellement sur la manière dont les informations échangées vont être codées. Il faut que les équipements parlent le même langage pour se comprendre, à l'image des protocoles qui définissent une "langue" de communication. Il est ainsi décidé quel codec sera utilisé (meilleure qualité de son, meilleure occupation de la bande passante). Le protocole H.245 traite cette négociation de codecs.
- Le protocole RTP (Real-time Transport Protocol) est chargé de transporter les données (la voix dans notre contexte) pour assurer une diffusion quasi temps réel.

Les architectures H.323 peuvent bénéficier de diverses implémentations. Nous allons voir les architectures point à point, multipoint et gatekeeper.

II.3.4.3.1. Architecture point à point

Dans cette architecture, la couche protocolaire est gérée par chaque client et l'ensemble du trafic ne transite qu'entre l'émetteur et le destinataire.

Pour commencer un appel, l'adresse IP du destinataire est appelée. La phase de signalisation s'engage alors et les protocoles associés envoient un message au destinataire en lui proposant d'établir la connexion. L'identifiant H.323 est également envoyé pendant la phase de signalisation. Le destinataire regarde son statu et deux réponses peuvent être envoyées à l'émetteur: libre ou occupé.

Lorsque le destinataire est prêt à recevoir l'appel, la phase de négociation des codecs débute et chaque partie énumère les codecs disponibles afin de s'accorder sur un standard.

Enfin, la communication débute et les flux sont envoyés généralement en RTP. Lorsque les deux parties terminent la communication, tous les sockets se ferment. La Figure (II.15) représente une architecture point à point:

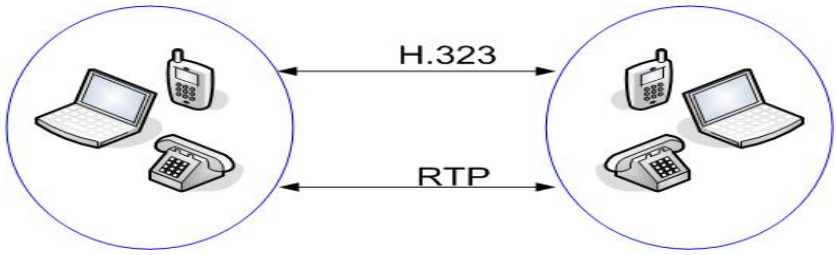


Figure II.15. Architecture point à point.

II.3.4.3.2. Architecture Gatekeeper

Dans cette architecture, un nouvel élément entre en ligne de compte dans le processus de signalisation : le gatekeeper. Il s'agit d'un dispositif assurant une translation *adresse IP / numéro de téléphone* ainsi que toute la partie *autorisation*.

Les clients VoIP sont alors configurés pour s'enregistrer auprès du gatekeeper. Ainsi, lorsqu'ils se connectent au réseau, ces derniers annoncent leur adresse IP et leur identifiant H.323 au gatekeeper.

Pour appeler, le client a besoin d'utiliser l'identifiant H.323 du destinataire et ainsi effectuer une requête auprès du gatekeeper chargé d'autoriser ou non l'émetteur. Si le gatekeeper permet à l'émetteur d'appeler le destinataire, le gatekeeper contacte le destinataire pour connaître son statu. Si le destinataire est prêt à recevoir un appel, son adresse IP est transmise à l'émetteur qui va pouvoir établir la connexion. La communication s'effectue ensuite directement entre les clients et le gatekeeper n'a plus aucun rôle à jouer.

La phase de négociation des codecs débute, à l'image d'une architecture point à point. Le gatekeeper ré intervient lors de la fin de la communication. La Figure(II.16) résume l'architecture gatekeeper:

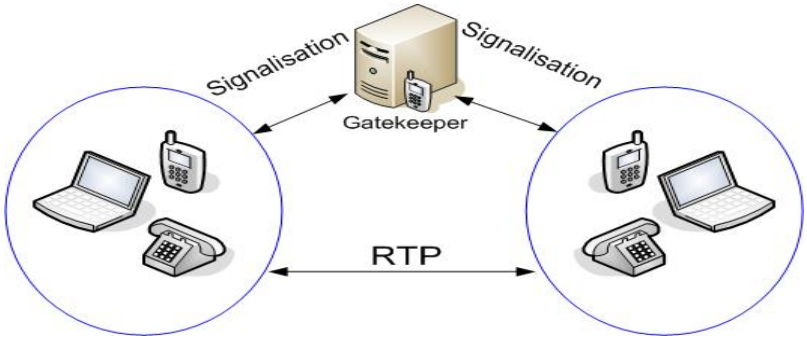


Figure. II.15. Architecture gatekeeper.

II.3.4.3.3. Architecture multipoints

Dans cette architecture, un nouvel élément prend place: le **multipoint control unit** ou **MCU**. Ce dispositif permet de gérer plusieurs communications simultanées, très util pour les conférences téléphonies. Il permet également d'assurer des services comme la diffusion d'une tonalité.

Lors de la mise en service du système VoIP, le multipoint control unit signale sa présence au gatekeeper et lui fournit un certains nombres d'informations (nombre de clients simultanés possibles, les débits possibles ainsi que l'identifiant H.323). Tout se passe ensuite comme dans l'architecture gatekeeper. Les clients VoIP s'enregistrent auprès du gatekeeper.

Cette architecture est la plus recommandée et s'accompagne très souvent de passerelles vers le réseau RTC ou vers d'autres réseaux téléphoniques privés. La figure(II.16)représente une architecture multipoint :

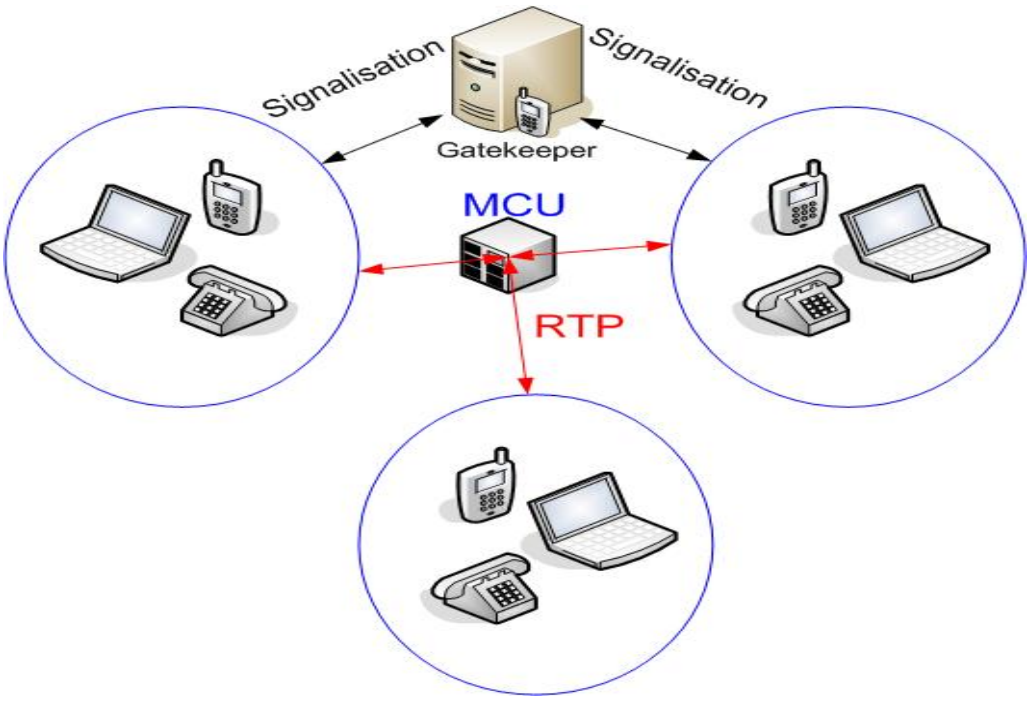


Figure .II.16. L'architecture multipoints.

II.3.4.3.4. Déroulement d'un appel entre deux terminaux en H.323

Il est important de spécifier que la norme H.323 repose sur le principe du peer-to-peer (egal à egal).

Ainsi il est tout à fait possible d'initier un appel direct entre deux correspondants sans passer par un serveur dédié ou une passerelle H.323 dès lors que nous avons connaissances des caractéristiques réseaux du correspondants et que la topologie le permet (NAT, firewall…) comme la figure(II.16) le montre :

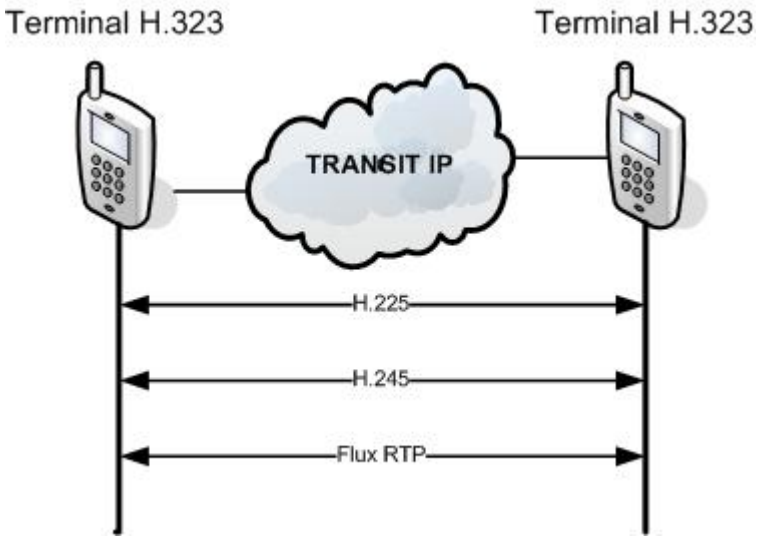


Figure II.16. Déroulement d'appel entre deux terminaux en H323

H323 empruntant la norme Q931, elle fonctionne de la même manière que le protocole ISDN, et supporte donc les messages suivants :

-SETUP

-ALERTING

-CONNECT

-RELEASE COMPLETE

-STATUS FACILITY

Au fil des versions de nouveaux messages ont été introduits (comme le CALL PROCEEDING, STATUS, PROGRESS) afin de répondre aux besoins d'évolutivités.

Exemple d'appel point à point simple

Lorsqu'un correspondant X cherche à joindre Y, plusieurs échanges de messages ont lieu , comme le montre la figure(II.17).

Tout d'abord il lui envoie un message SETUP via le canal de signalisation (H.225 port TCP ou UDP 1720) sur son adresse IP. Dans ce message nous trouvons diverses informations (identifiant source, type de source, adresse de destination, type de destination …)

Ensuite à la réception du setup, le terminal utilisé par Y réponds par un message ALERTING signifiant que le combiné sonne.Si Y décroche alors le terminal envoie le message CONNECT, s'il refuse le terminal envoie RELEASE COMPLETE et l'appel est terminé.

Dès que le message connecté est reçu, une session RTP est alors établie entre les deux terminaux afin d'assurer le transport du flux voix.

A la fin de la communication le message RELEASE COMPLETE est envoyé par celui qui a raccroché pour terminer l'appel.

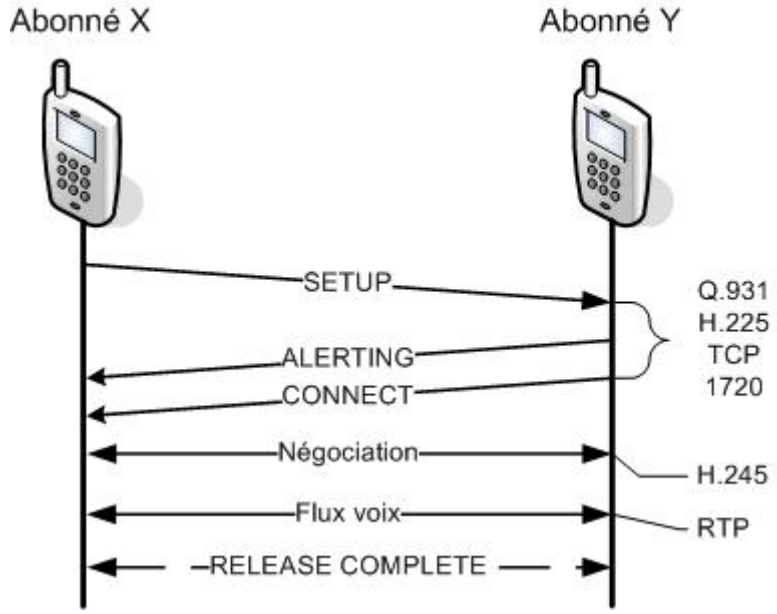


Figure II.17. Déroulement d'appel point à point.

II.3.4.4. L'avenir de H.323

Bien qu'il soit historiquement le protocole le plus utilisé, H.323 souffre aujourd'hui de la concurrence face au nouveau protocole SIP. Malgré que les deux protocoles soient très proches dans leurs architectures de fonctionnement, les manques de souplesse de H3.23, ses caractéristiques trop axée télécom ainsi que l'engouement exponentiel pour le SIP et les possibilités applicatives qu'elle possède font qu'H.323 est de plus en plus remplacé par le protocole SIP dans les nouvelles interconnexions et solutions voIP.

II.3.5. Protocole SIP (Session Initiation Protocol) [7]

Le protocole SIP (Session Initiation Protocol), de l'IETF, est un protocole de signalisation pour l'établissement d'appel et de conférences temps réel sur des réseaux IP. Proposé comme standard à l'IETF en 1999, SIP est rapidement apparu comme une alternative à H.323.

Chaque communication doit pouvoir inclure différents types de données telles que l'audio et la vidéo. SIP est indépendant du protocole de transport utilisé**.** Il s'utilise avec les protocoles TCP et UDP.

Il est décrit comme un protocole de contrôle de la couche application afin d'établir des communications entre deux terminaux. L'application fondamentale de SIP est donc de permettre à deux individus de se contacter, indépendamment de leur localisation et de leur terminal. SIP ressemble en syntaxe à HTTP, car il permet d'établir une session entre 2 interlocuteurs identifiés par des adresses similaires à des adresses email. L'utilisation massive du protocole SIP dans le réseau NGN fait qu'il remplace peu à peu le H323.

II.3.5.1. Adresses SIP

Les adresses SIP se présentent sous la forme suivante:

sip:infos-utilisateur@domaine

Les « Infos-utilisateur » sont sous la forme :

« Nom utilisateur : mot de passe » ou «N° de téléphone »

Le domaine est sous la forme:

« 2 Architecture du protocole SIP »

Exemples : sip :robert_gsm@arcome.fr

sip :robert_home@family.org

sip :0146124200@arcome.fr

II.3.5.2. Architecture de SIP

La figure (II.18) représente l'architecture du protocole SIP :

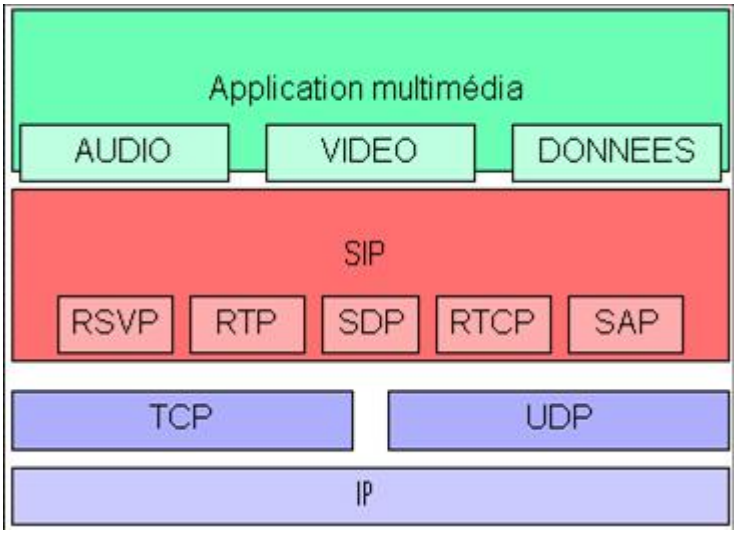


Figure II.18. Architecture de SIP

RSVP : réservation des ressources réseaux sur IP.

RTP : transport des informations en temps réel.

RTCP : assure le contrôle de flux de données multimédia.

SDP (Session Description Protocol) : décrit les sessions multimédia.

II.3.5.3. Comment établir une communication

Pour établir une communication, l'appelant, adressera sa requête à un serveur SIP : l'architecture de SIP est basée sur des relations client/serveur. Les principales composantes sont le terminal (User Agent), le Proxy Server, le Redirect Server et le Registrar (voir la figure (II.19)). Les terminaux sont considérés comme clients lorsqu'ils effectuent une requête, et comme des serveurs lorsqu'ils y répondent. Les terminaux peuvent communiquer directement entre eux ou par l'intermédiaire d'autres serveurs. Les serveurs SIP intermédiaires peuvent se comporter comme proxy serveur ou serveur de redirection (redirect server).

- **Users Agents (UA):** Il y a deux users agents : UAC: l'agent de la partie appelante et UAS: l'agent de la partie appelée il reçoit les requêtes.
- **Proxy Server (PS):** Auquel est relié un terminal agit à la fois comme client et serveur.Il peut transmettre une requête, sans changement, à la destination finale ou éventuellement modifier certains paramètres. Le proxy server renseigne le champ « via » à chaque fois qu'une requête passe par lui afin que la réponse puisse prendre le même chemin au retour.

- **Redirect Server (RS) :** Un redirect server répond à une requête SIP « Invite ». Il établit la correspondance entre l'adresse SIP du terminal appelé et la ou les adresses où il pourra effectivement être joignable**.** Il n'est pas chargé d'accepter les appels ni d'émettre des requêtes et ne fait que répondre aux requêtes émises par des terminaux SIP appelants.

- **Location Server (LS):** Fournit la position courante des utilisateurs dont la communication traverse les RS et PS auxquels ils sont rattachés.
- **Registrar Server** : Accepte les requêtes REGISTER et offre également un service de localisation comme le LS.

Chaque PS ou LS est généralement relié à un Registrar.

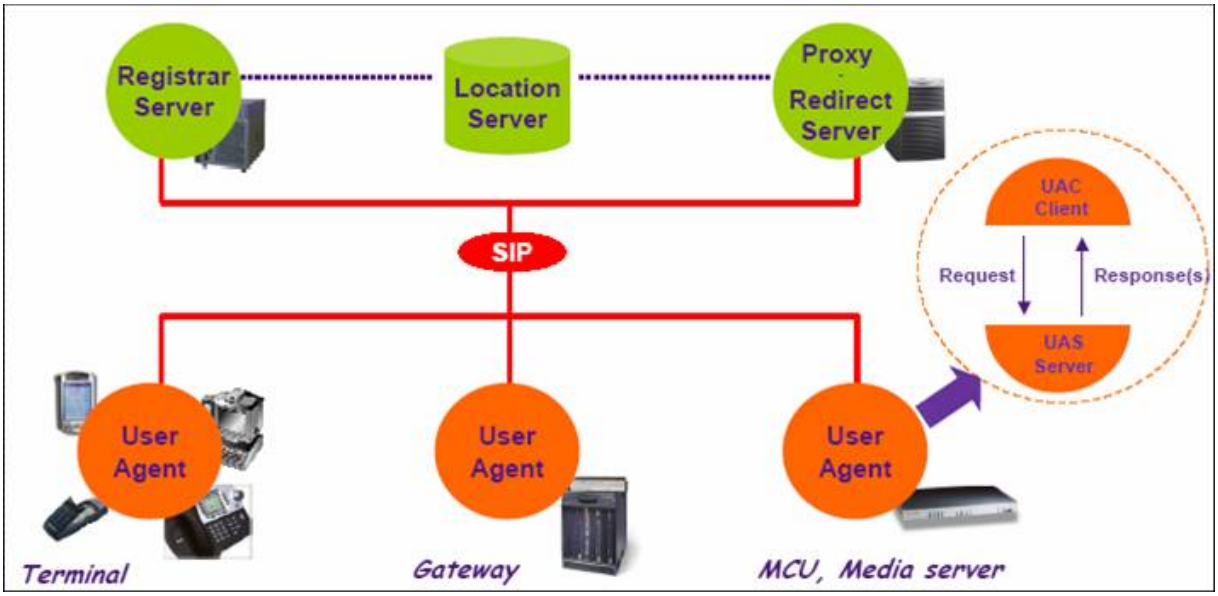


Figure II.19. Etablissement d'une communication avec SIP.

II.3.5.4. Requête

Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes,ces dernieres sont représentées dans le tableau(II.2).

Message	Descripion
INVITE	Indique qu'une entité(utilisateur ou serveur)est Invitée à participer à une session
ACK	Sert à confirmer qu'un client a reçu la réponse Finale d'un message INVITE particulier
OPTIONS	Permet d'interroger l'ensemble des capacités d'un Demandé
BYE	Transmis par un agent d'utilisateur(demandeur ou demandé)pour signaler qu'il souhaite liberer l'appel.
CANCEL	Permet d'annuler une requete en cours.N'annule pas une session déja établie.
REGISTER	Permet de mettre à jour les coordonnées(ce message est associé à l'entité d'enregistrement).

Tableau II.2. Requêtes.

II.3.5.5. Réponses

De nombreuses autres réponses, représentées dans le tableau(II.3), peuvent être générées pour chacune des requêtes «code d'état».

Type de réponse	Description
1xx	Information. La requête est reçue et est en cours de traitement (Exemple :« 180 Ringing »(sonnerie)ou « 100 Taying »(tentative d'accès)).
2xx	Succés.La requête a été traitée correctement.(Exemple :200 OK).
3xx	Réacheminement. Indique qu'une autre intervention est nécessaire pour effectuer l'appel.
4xx	Erreur du client. Le message comporte une erreur et le serveur l'a rejeté.(Exemple : structure de message erronée).
5xx	Erreur du serveur. Le serveur n'a pas réussi à traiter la

	requête. (Exemple : ressource en panne).
6xx	Echec général. La requête ne peut être traitée sur aucun serveur.(Exemple :aucune ressource disponible à l'échelle du réseau).

Tableau II.3. Réponses.

Exemples : Entre deux User Agents :

Cas le plus simple: les deux UAs connaissent l'adresse IP de leur interlocuteur c'est pourquoi ils peuvent se joindre directement.

Pour joindre un autre utilisateur, il est nécessaire de connaître son adresse. La figure (II.20) représente l'établissement d'une session SIP entre deux abonnés.

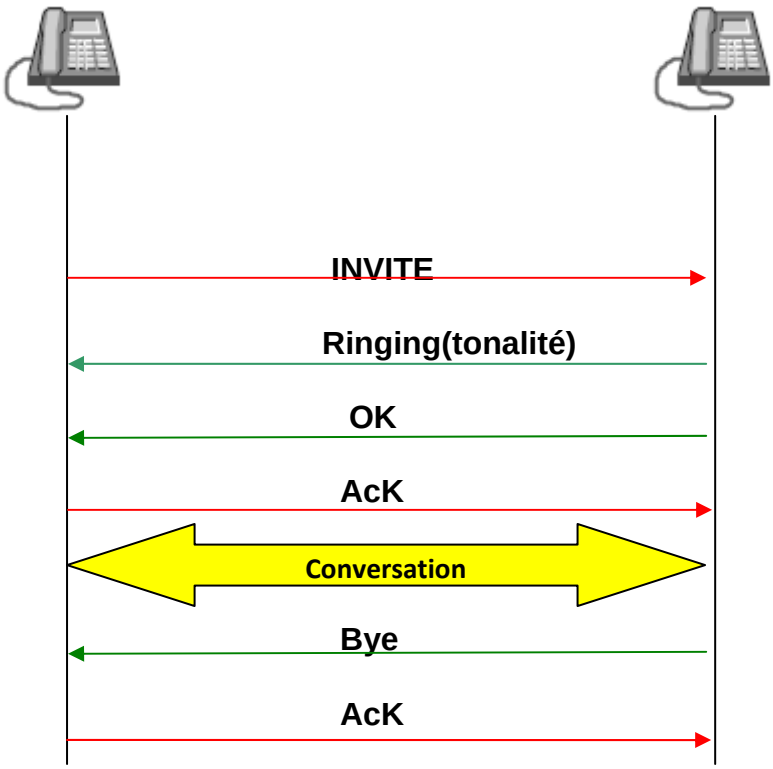


Figure II.20. Etablissement d'une session SIP entre deux abonnés.

II.3.6. Le protocole RTP [8]

Le protocole RTP (Real-Time Transport Protocol) sert au transport de l'information à proprement parler. Il assure le synchronisme des paquets lors de l'entrée sur le réseau ainsi qu'au moment de la sortie. Ce protocole se situe au niveau transport du modèle de référence afin de lutter contre les gènes du réseau.

RTP possède plusieurs fonctions et fournit des mécanismes de contrôle élaboré. Il permet tout d'abord de réaliser un séquencement des paquets par le biais d'un système de numérotation. Grâce à des paquets numérotés, il devient très facile d'identifier ceux qui ont été perdus lors de la transmission (si un numéro est manquant dans la séquence, on sait alors qu'il y a eu perte). Cette séquence de paquets est déterminante dans la reconstitution de la voix. L'avantage de détecter la perte d'un paquet permet dans certains cas de reconstituer le paquet manquant en réalisant une synthèse des paquets qui précèdent et succèdent.

RTP effectue également une identification du corps des paquets, afin de savoir ce que chaque paquet transporte. Ici aussi, en cas de perte, on peut envisager une recomposition du message perdu. Identifier la source de la transmission est également une fonction assurée par RTP.

Cependant, pour assurer ses fonctions, RTP se base sur un autre protocole, RTCP (Real-Time Control Protocol), afin de transporter des informations complémentaires et nécessaires à la gestion d'une session.

II.3.7. Protocole RTCP [8]

RTCP (Real-Time Control Protocol) permet de gérer les rapports de qualité de service (QoS) renvoyés par le destinataire d'une communication à l'émetteur afin de connaître le nombre de paquets perdus ainsi que d'autres informations comme le temps nécessaire pour effectuer un aller-retour. En consultant ces rapports, l'émetteur est alors capable de répondre à une contrainte de temps obligatoire, notamment en termes de réduction de temps aller-retour, par le biais d'une meilleure compression afin de garantir la qualité de service.

RTCP fournit également une meilleure synchronisation des médias, un mécanisme d'identification (numéro de téléphone, nom d'un destinataire...) et de contrôle de session

(arrivée ou départ d'une personne au sein d'une conférence audio...). Ces informations sont envoyées de manière cyclique par les utilisateurs en communication.

Il faut savoir qu'un protocole, utilisant le même schéma que RTCP, peut être utilisé. Il s'agit de RTSP (Real Time Streaming Protocol) qui gère et contrôle des communications basées entre deux serveurs stockant les données multimédias. Ce protocole est assez intéressant lorsque l'on souhaite par exemple pouvoir réécouter une conversation téléphonique ultérieurement.

II.4. Présentation de l'HONET

HONET, abréviation de Home Network, est la solution U-SYS (Universal System) proposée par la société chinoise Huawei définissant un réseau d'accès NGN, cette solution a été adopté par le réseau téléphonique d'Algérie Telecom en vue d'une migration du réseau RTC vers le réseau NGN.

Le réseau NGN est doté d'équipements caractérisés par leur grande puissance, simplicité à gérer et une grande fiabilité, permettant d'offrir plusieurs méthodes d'aces aux différents nouveaux services.

Le réseau NGN de la wilaya de Tizi-Ouzou (HONET) est constitué essentiellement de trois entités :

- ✓ SoftX3000
- ✓ UMG8900 (Universal Media Gateway 8900)
- ✓ MRS6100 (Media Ressource Server 6100)

La figure (II.21) représente la position des trois entités dans le réseau NGN :

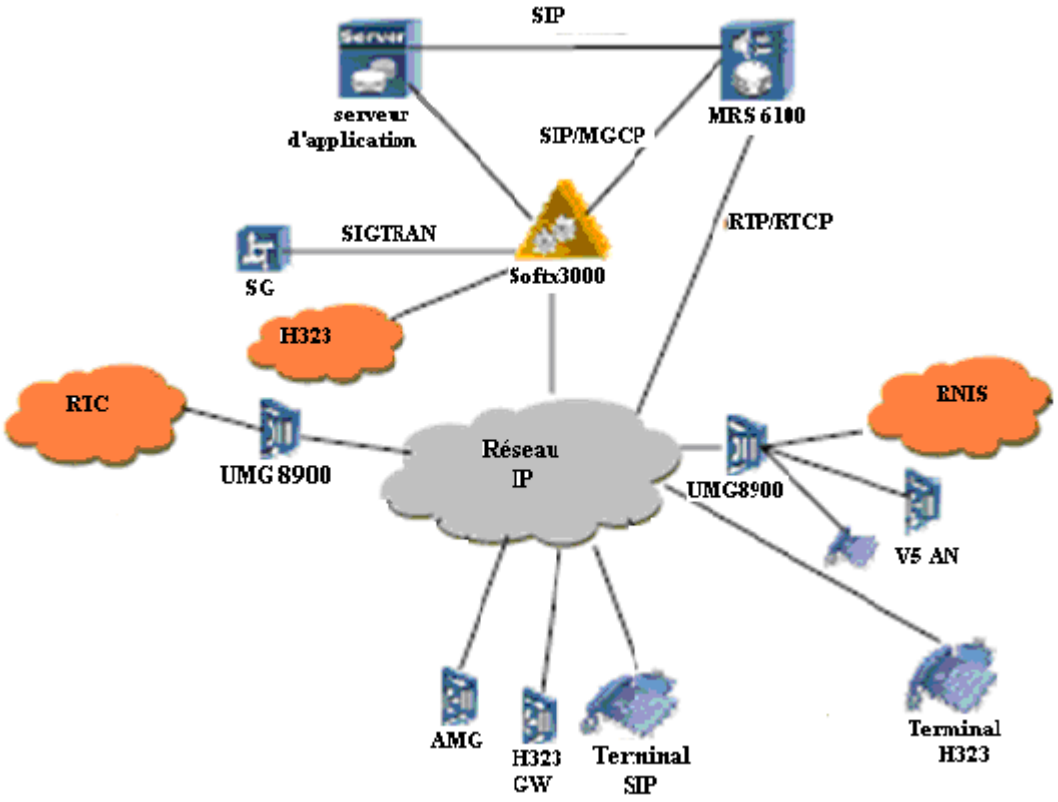


Figure II .21. Position de SoftX3000, UMG8900 et MRS6100 dans le réseau NGN.

II.4.1. SoftX3000

Le SoftX3000 est un softSwitch qui est un équipement de la couche de contrôle dans le réseau NGN. Il est caractérisé par sa grande capacité et d'une haute performance. C'est un équipement de télécommunication qui est employé dans la salle centrale d'équipement du central téléphonique et n'a aucune interface de câble d'abonnée.

Le softX3000 a pour rôle : le contrôle d'appel, la gestion des connexions de voix, données et des services multimédias basés sur le réseau IP.

II.4.2. UMG8900 (Universal Media Gateway 8900)

L'UMG8900 est une Gateway (passerelle), qui est un équipement de la couche d'accès dans un réseau NGN, développé par la société chinoise Huawei. Il fait la conversion et l'adaptation des différents formats des flux media. Il peut fonctionner comme AG (Gateway d'accès), TG (Trunk Gateway) dans le NGN et comme commutateur traditionnel d'un réseau PSTN.

II.4.3.MRS6100 (Media Ressource Server 6100)

MRS6100 est le composant noyau de ressources qui fournit des services à valeurs ajoutée dans un réseau IP, appartenant à la couche de services du réseau NGN. Il est responsable du traitement des services media dans le réseau tel que génération de tonalité, collection d'entrée d'utilisateurs, reconnaissance de la parole, synthèse vocale, enregistrement, fax et vidéo conférence. Il est contrôlé par le SoftX3000 et les serveurs d'application et il fournit les fonctions suivantes pour attribuer différents services dans le réseau IP :

- ✓ Fournir les services.
- ✓ Communication avec d'autres entités.
- ✓ Gestion et maintenance des ressources.

III.1. Menace

Une menace est une personne, un évènement ou une idée qui représente un danger pour un actif (composant, matériel, documentation fourniture, donnée sur le réseau). Les caractéristiques d'une menace peuvent compromettre la confidentialité, l'intégralité ou la disponibilité d'un active en exploitant une faiblesse du système.

III.1.1. Catégorie de menace

Il existe cinq catégories de menace :

a. divulgation : l'information ou les données qui exige une grande confidentialité sont vulnérable à la divulgation. Cette catégorie de menace met ces données en danger par divulgation non autorisée.

b. interruption : elle touche principalement les services en s'attaquant à leur disponibilité (exemple : panne de courant).

c. modification : ce genre de menace comprend essentiellement l'intégrité des renseignements (piratage informatique).

d. destruction : cette catégorie englobe tous se qui contribue à la destruction de l'information.

e. enlèvement : cette catégorie touche à tout se qui concerne le vol de donnée ou de système.

III.2. Risques

Le risque est la disponibilité à une certaine exploitation des points faibles d'un système, malgré les mesures de sécurité.

III.3.Mesures de protection

On peut citer trois :

- protection physique.
- Protection environnementale.
- Protection logique.

III.3.1. Protection physique

Pour établir une communication ente deux entités de réseau, il faut placer une connexion afin d'émettre ou recevoir des informations.

Cette connexion se fait en sur demande préalable de l'émetteur ,la décision est laissée soit pour le récepteur soit pour le gestionnaire de service.

- **mode avec connexion** : il se fait en trois phases : l'établissement de la connexion la transmission des données et la libération de la connexion.
  La transmission de données,dans ce mode, est sécurisée car l'émetteur et le récepteur sont en accord, et le contrôle est effectué au moins au niveau des extrémités. En plus l'émetteur et le récepteur négocie sur la qualité de service (QOS).
- **mode sans connexion** : il n'a pas besoin de présence à la fois et au même temps des entités communicantes, donc il n'ya pas de négociation entre l'émetteur et le récepteur. La connexion est mise en place par une certaine logistique qui assure le transfert des données grâce à la structure en couches.La difficulté de ce mode réside dans l'établissement de contrôle de communication par le gestionnaire de réseau.

III.3.1.1. Sécurité physique des équipements

La sécurité physique des équipements comprend :

- ✓ l'identification de l'emplacement des équipements.
- ✓ La limitation des accès physiques et l'utilisation de surveillance environnementale appropriée.

III.3.1.2. Emplacements physiques

Le choix de l'emplacement physique des ressources vitales du réseau est très importante. Tous les équipements de l'infrastructure de réseau doivent être situés dans des zones à accès non autorisé.

III.3.2. Protection environnementale

Pour garantir la disponibilité des ressources vitales du réseau il faut protéger l'environement en appliquant des moyens de protection dont les plus essentiels sont :

- la prévention, la détection et la protection contre les incendies.

- la prévention, la détection et prise de mesures correctives contre l'inondation.
- la protection de l'alimentation électrique ;

-le contrôle de température

- le contrôle de l'humidité

- la protection contre la poussière et les salissures

III.3.3. Protection logique

La sécurité logique fait référence à la réalisation de mécanismes de sécurité logicielle. Elle repose principalement sur la mise en œuvre adéquate d'un processus de contrôle d'accès logique le quel s'appuie sur un triple service d'identification, d'authentification et d'autorisation**.**

La sécurité logique comprend outre les mécanismes logiciels permettant d'assurer la confidentialité des données par chiffrement, toutes les mesures de protection contre l'infection des fichiers par contamination de virus et d'autres programmes destructifs.

III.3.4. Services de sécurité

Parmi les services de sécurité, on trouve l'ISO (International Standardisation Organisation) qui s'est attachée à prendre toutes les mesures nécessaires à la sécurité des données durant leur transmission, ses travaux ont donné naissance à un standard international, ISO 748-2.

Cette architecture est très utile pour l'implémentation des éléments de sécurité dans un réseau, pour cela trois concepts ont été définis :

- les fonctions de sécurité, qui sont déterminées par les actions, pourront compromettre la sécurité d'un établissement.
- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre.
- les services de sécurité, qui représentent les logiciels et le matériel mettant on œuvre du mécanisme dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin

Cinq types de sécurité ont été définis :

a- La confidentialité : La confidentialité ou le secret, consiste a conserver des informations à l'abri de ceux qui ne sont pas autorisé à la connaitre.

b- l'authentification : elle revient à s'assurer de l'indenté d'un interlocuteur avant de lui révéler des services.

c- l'intégrité : elle permet de s'assurer que les données reçues émanent bien de leur prétendu et non d'un adversaire malintentionné qui les aurait modifiés au cours de leur acheminement.

d- la non- répudiation : elle s'applique aux signatures pour prouver que les données reçues sont réellement envoyées par un émetteur donné.

e- le contrôle d'accès : il à pour rôle de prévenir l'accès à des ressource sous des conditions définies et par des utilisateurs spécifiés.

L'étude des besoins de l'émetteur et du récepteur par ces cinq services de sécurité donne le processus suivant :

- ✓ le message ne doit parvenir qu'au bon destinataire.
- ✓ l'émetteur du message doit pouvoir être connu avec certitude.
- ✓ il doit y avoir identité entre le message reçu et le message émis.
- ✓ le destinataire ne peut contester la réception du message.
- ✓ l'émetteur ne peut contester l'émission du message.
- ✓ l'émetteur ne peut accéder à certaines ressources que s'il en a l'autorisation.

III.4. Cryptographie

C'est la science de transformer les données pour en cacher le sens elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en une succession de chiffres sous forme de bits, puis faire des calcules sur ces chiffres pour :

- o les modifier
- o faire en sorte que le destinataire pourra les décrypter.

Le faite de coder un message de façon à le rendre secret s'appelle le cryptage .la fonction inverse consistant à retrouver le message original, est appelé décryptage.

III.4.1. Chiffrement

On peut assurer la confidentialité des données réseau en recourant au chiffrement de l'information. Ce dernier consiste à convertir les données en une inintelligible pour les personnes non autorisées. Par la suite pour reconvertir l'information dans sa forme original. On doit utilise un processus de déchiffrement.

L'information sensible peut être mise en mémoire sous forme chiffrée. De cette façon, personne n'arrivera à la contourner.

Les mesures de contrôle de l'accès parviennent au fichier. la confidentialité de l'information est protégée car cette information est chiffrée.

III.4.1. 1. Principe général du chiffrement

L'émetteur souhaite envoyer un message M au récepteur à travers un canal de communication susceptible d'être espionné par un tiers à tout instant, donc dans cette situation les personnages ont besoin :

- d'un algorithme de chiffrement qui prend en paramètre un code secret appelé clé de chiffrement Ke.
- d'un algorithme de déchiffrement qui prend en paramètre un code secret appelé clé de déchiffrement Kd.

Une formalisation simple des principes de chiffrement et de déchiffrement peut être donnée par les relations suivantes :

$C=EKe(M)$ et $M=DKd(c)$

Où C représente le message chiffré.

Le principe est modélisé par la figure (III-1).le système tel qu'il est représenté n'est sur que s'il est impossible à un intrus de déduire le texte claire du message chiffré et à fortiori de retrouver la clé de déchiffrement. On distingue en général trois types de chiffrement.

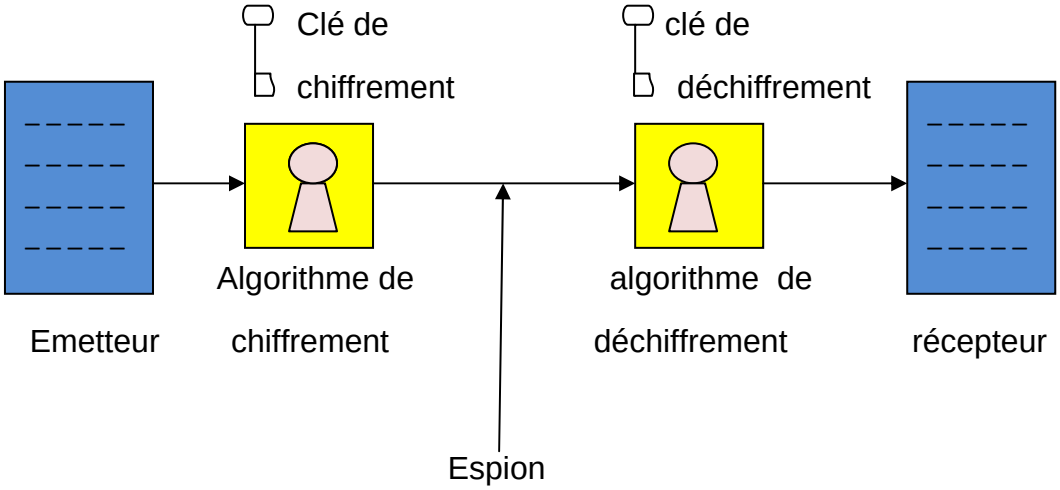


Figure.III.1. Principe de chiffrement et de déchiffre.

III.4.1.1.1.Chiffrement restreint

C'est le type de déchiffrement le plus ancien dans lequel la confidentialité du message chiffré repose sur l'algorithme de chiffrement. Ce type de déchiffrement n'est pas utilisé à grande échelle et a émané pendant très longtemps d'instances diplomatiques ou militaires.

III.4.1.1.2. Chiffrement à clé secrète

Le chiffrement a clé secrète encore appelé chiffrement symétrique ou chiffrement conventionnel est le type de chiffrement le plus répondu .Dans le schéma précédent il correspond à des clés de chiffrement et de déchiffrement identique ou facilement déductibles l'une de l'autre, connues uniquement par l'émetteur et le récepteur. L'algorithme et quant à lui est public et la confidentialité du message échangé repose uniquement sur le secret de la clé partagée, voir la figure (III.2)

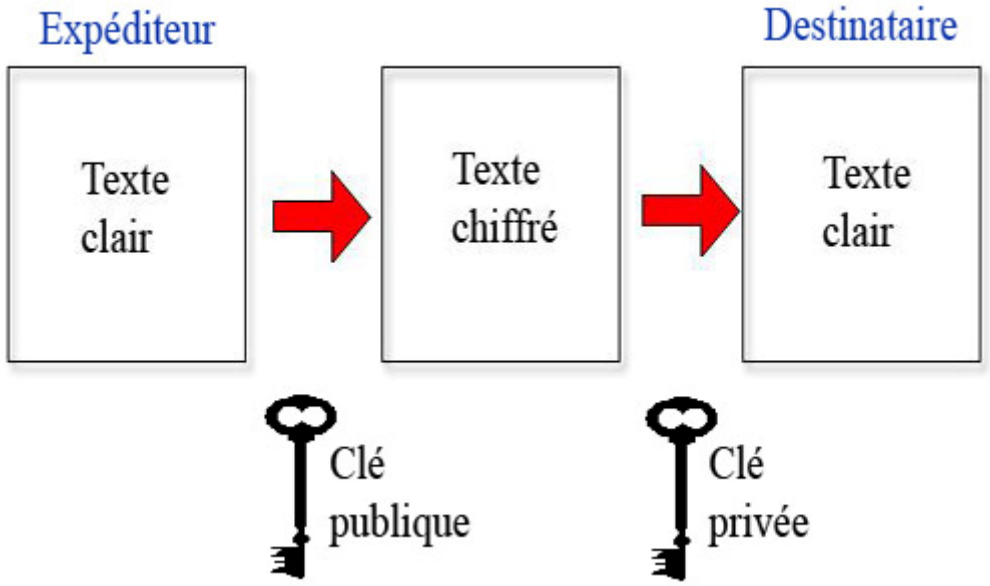


Figure.III.2. Chiffrement à clé secrète.

En supposant alors inévitablement deux questions, d'une part celle de nombre de clés à générer dans un réseau à n points ou chaque personne doit posséder une clé différente pour chacune des communications avec les (n-1) autre personnes (d'où une totale de n (n-1)/2 clés pour le réseau).

Malgré ces inconvénients, ce type de système a l'avantage,pour des raisons algorithmiques, d'être extrêmement rapide (comparativement à sa contre partie à clé publique) avec un moindre coût, permettant d'atteindre des débits de l'ordre de centaines de mégabit par seconde.

III.4.1.1.3. Chiffrement à clé publique

Le chiffrement à clé publique ou chiffrement asymétrique est une découverte bien plus récente (inventée en 1976)

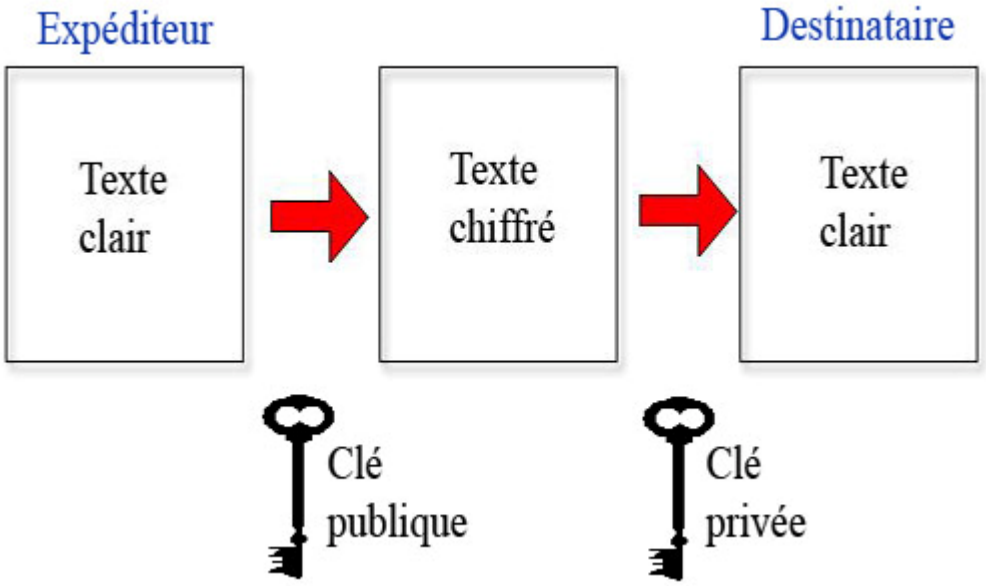


Figure.III.3. Chiffrement à clé publique.

La sécurité du système repose sur le secret de la clé de déchiffrement et sur l'impossibilité de déduire cette dernière à partir de la connaissance de la clé de chiffrement, voir la figure (III.3).

La clé publique étant publiée et la clé privée étant connue que de son propriétaire. Ainsi pour un réseau à n abonnés, le nombre de clés à générer est ainsi réduit à 2n.

Les algorithmes utilisés dans se type de cryptage sont marqués par une grande lenteur. Ce qui donne des débits de l'ordre de centaine de kilobit par seconde, qui les rendent inapte à une utilisation en ligne pour échanger des messages longs.

III.4.1.1.4. Mode opérationnel de chiffrement [9]

III.4.1.1.4.1. Mode ECB (Electronique Code Book)

Ce mode est le plus simple, le message M est découpé en blocs mi de taille fixe et chaque bloc est crypté séparément et codé de la mêmé manière (figure .III.4) ce mode de chiffrement ne présente donc aucune sécurité et n'est jamais utilisé.

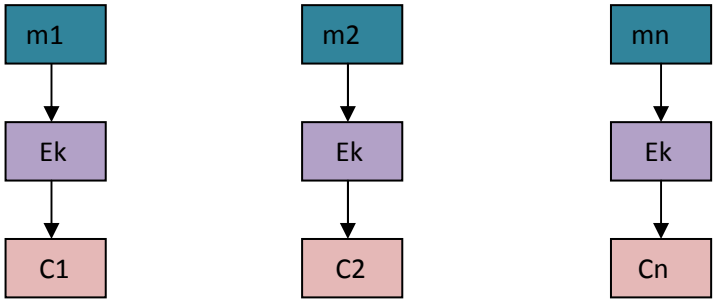


Figure.III.4. Mode ECB.

III.4.1.1.4.2. Mode CBC (Cipher Bloc Chaining)

Le mode CBC à été introduit pour qu'un bloc ne soit pas codé de la même manière s'il est dans deux messages déférents, il faut ajouter une valeur initial C0. Chaque bloc est d'abord modifié par XOR avec le bloc crypté précédent avant d'être lui-même crypté par :

Ci=Ek (mi⊕Ci-1), voir la figure(III.5).

Et pour le déchiffrement il nécessite l'inverse de la fonction de codage :

Dk=Ek^{-1}. Et mi = Ci-1⊕D(Ci).

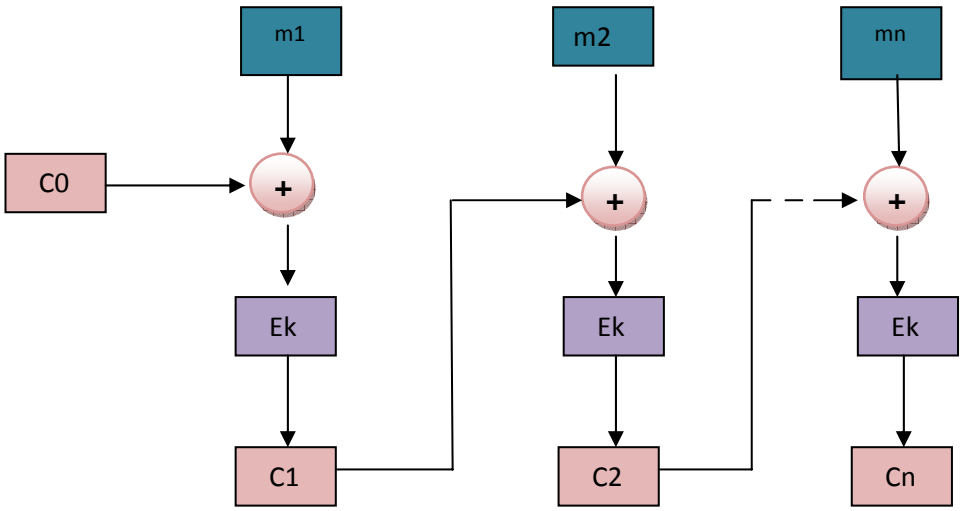


Figure.III.5. Mode CBC.

III.4.1.1.4.3. Mode CFB (cipher feed back)

Pour ne pas avoir besoin de la fonction inverse pour décrypter, il est possible de faire un XOR après le cryptage; c'est le mode CBF:

Ci=mi ⊕Ek (Ci-1) ; voir la figure (III.6).

Et pour déchiffrer on a : mi=Ci⊕Ek(Ci-1)

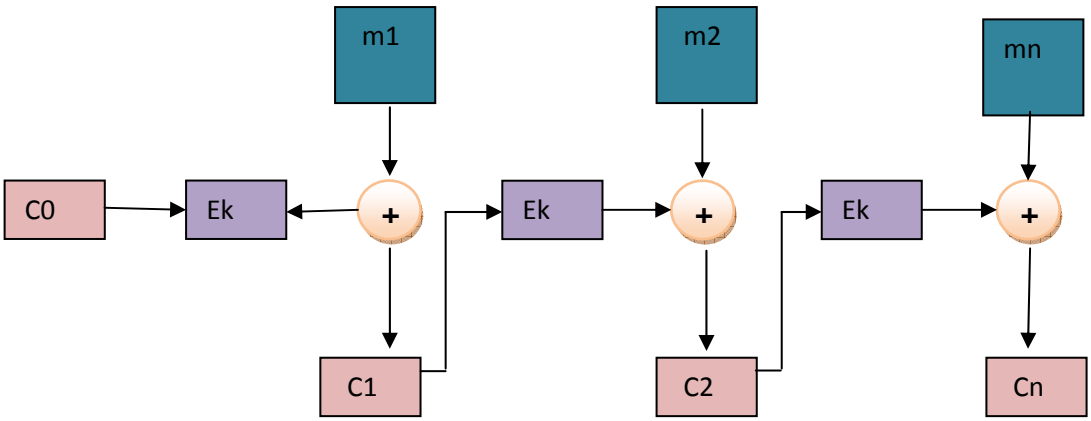


Figure.III.6. Mode CBF.

III.4.2. Clés

Une clé est une valeur qui est utilisée avec un algorithme cryptographique pour produire un texte spécifique, sa taille se mesure en bits.

III.4.3. Signature numérique

Supposant que l'on dispose d'un algorithme de chiffrement à clé publique (C'est la fonction de chiffrement et D la fonction de déchiffrement). Comme nous avons vu dans le paragraphe précédent la fonction C est connu du tous, tendis que D n'est connu que par le propriétaire légitime du couple (C,D).

Lorsque le propriétaire du couple (C,D) souhaite signer un message M ,il calcule S=D(M),donc toute personne disposant de message M et de signature S peut vérifier l'origine de la signature C(S).si cette quantité est bien égale à M, alors on est certain que l'auteur de signature est bien le propriétaire du couple (C,D),car c'est la seule personne qui peut produire D(M).

Pour être un peu précis, ce n'est jamais un message M que le propriétaire de message signe, mais l'empreinte de M par une fonction de hachage, cette empreinte dépond très fortement du message, et sous réserve que la fonction de hachage utilisée soit bonne,cette

méthode est aussi sûre que la signature complète du message. L'intérêt de la fonction de hachage est de permettre de signer une quantité de données beaucoup plus petite que le message entier.

La signature numérique peut également être réalisée en utilisant des certificats électroniques. Ceux-ci sont générés par les autorités de certificat (CA) qui permettent d'identifier de façon unique l'entité possédant le certificat et constituent donc un moyen de signature numérique ; ils peuvent être vue comme la carte d'identité de l'entité possédant le certificat. En plus de ce rôle, les certificats permettre de chiffrer des informations.

On distingue deux types d'algorithme de cryptage : symétrique et asymétrique.

VI.1. Algorithmes symétriques [9]

IV.1.1. Algorithme DES

DES, pour Data Encryption Standard « standard de cryptage des données » est un algorithme très répondu à clé privée crée en 1977.Cet algorithme a été étudié intensivement ces dernières années et est devenu l'algorithme le plus connu dans le monde.

IV.1.1.1. Fonctionnement du DES

Le DES est un algorithme qui reçoit en entrée un bloc de texte claire de 64 bits en utilisant une clé de 56 bits, en effet, la clé compte 64 bits,mais parmi lesquels un bit sur huit est utilisé comme bit de parité. A la sortie, résulte un bloc de 64 bits qui représente le texte chiffré.

Les étapes de chiffrement son :

1) On a un texte clair M,on lui applique une permutation initial IP fixée pour obtenir une chaîne x0, on a donc :

x0=IP(M)=L0.R0

Ou Lo contient les 32 premiers bits de x0 et R0 les 32 restants.

2) seize itérations (ou seize tours) d'une certaine fonction sont effectués. On calcule Li et Ri, $1 \leq i \leq 16$ suivant la règle :

$$\begin{cases} Li=Ri-1 \\ Ri=Li-1+f\ (Ri-1, Ki) \end{cases}$$

3) la permutation inverse IP^{-1} est appliquée à R16 L16 pour obtenir un bloc de texte chiffré $y=IP^{-1}$ (R16 L16) (à noter l'inversement de L16 et de R16)

Le fonctionnement général est illustré dans la figure(IV.1) :

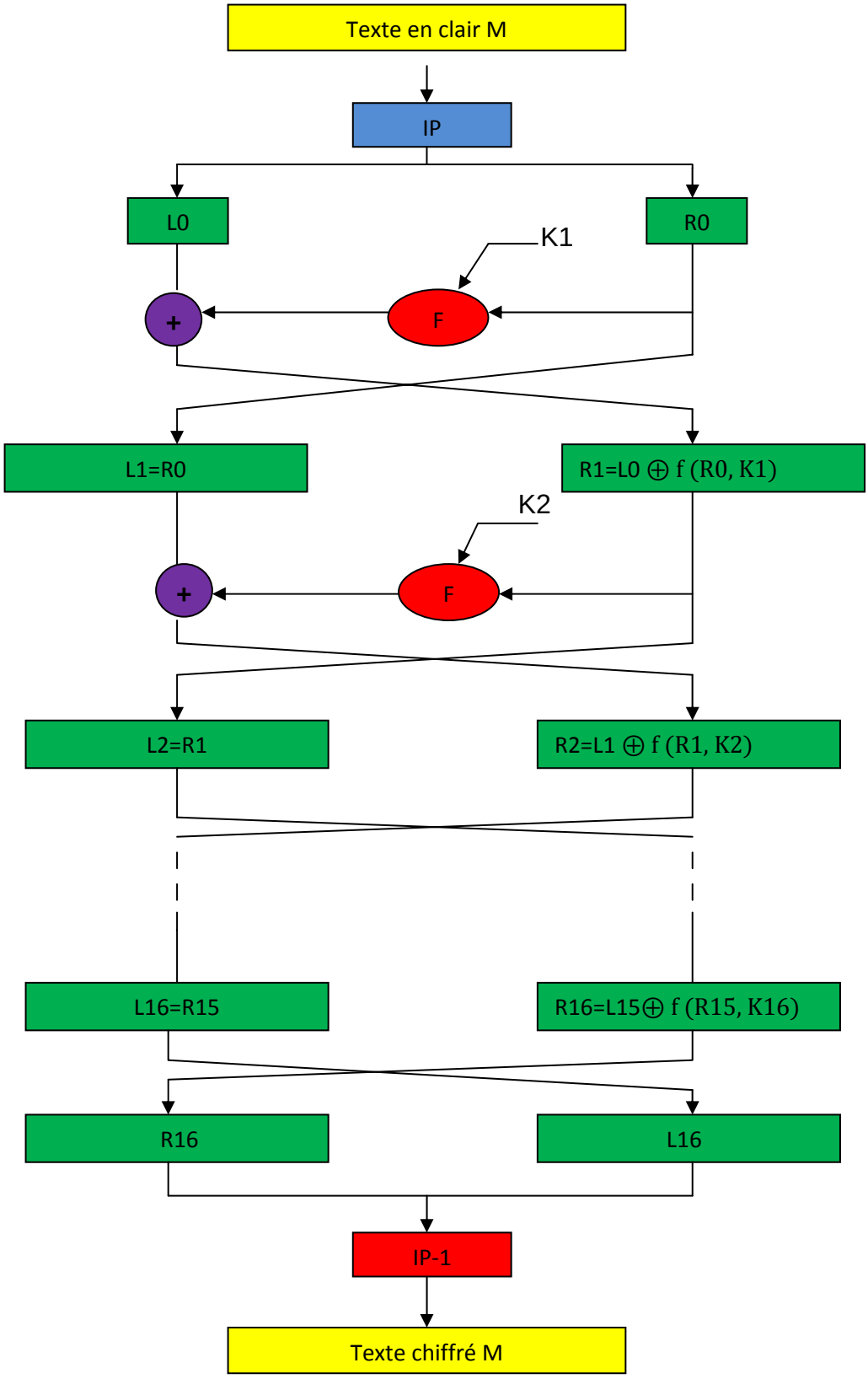


Figure.IV.1. Fonctionnement générale du DES.

Les détails de la permutation initiale IP sont fournis dans le tableau (IV.1) :

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tableau.IV.1. Permutation initial IP.

Cela signifie que dans le calcul de y=IP(x), le 58° bit de x est le premier de y. le 50°bit de x et le seconde de y, ce formalisme sera utilisé dans les tableaux qui suivent, on a aussi la permutation inverse IP^{-1}, représentée dans le tableau (IV.2) :

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tableau.IV.2. Permutation initial inverse IP.

IV.1.1.1.1.Fonction f (R_{i-1}, K_i)

f est une fonction qui prend en entrée les 32 bits R_i et les 48 bits de la clé de tour et fournit une sortie de 32 bits. Elle est définie en utilisant huit permutations appelées S-boxes qui associent à six bits d'entrée quatre bits de sortie. Chaque clé de tour Ki contient un sous-ensemble défirent des 56 bits, enfin, une permutation inverse de la permutation initiale IP^{-1} donne le texte chiffré.

Dans un premier temps R_{i-1} est étendue en un bloc de 48 bits en utilisant une fonction d'étalement E, représenté dans le tableau (IV.3)

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tableau IV.3. Fonction d'expansion E.

En suite,on effectue une opération de ou exclusif entre le résultat de E(Ri-1) et Ki (une clé de 48 bits),puis on scinde le résultat de cette opération en huit blocs de 6 bits $B_1B_2B_3B_4B_5...B_8$.Chaque B_i pour 1=i=8 et ensuite utilisé comme l'entrée d'une fonction de substitution (S-box) ,Sj qui associe un bloc de 6 bits $B_i=B_1B_2B_3B_4B_5B_6$ un bloc de 4 bits de la manière suivante :l'entier représenté par b_1b_6 sélectionne une ligne de Sj et l'entier représenté par $b_2b_3b_4b_5$ une colonne .Enfin,la valeur de Sj (Bi) est la représentation de l'entier inscrit dans la S-box à cette position .

Les huit « boîtes-S» S1, S2…….. , S8 sont représentées dans les tableaux(IV.4) :

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

18

S5

2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9
14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6
4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14
11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

S6

12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

S7

4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6
1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

S8

13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2
7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

Tableau.IV.4. Huit « boîtes-S».

Après la fonction S-box on obtient une chaîne C=C1.C2....C8 ,de longueur 32 bits,est alors réordonnée suivant une permutation fixé P représentée dans le tableau (IV.5)

p

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tableau.IV.5. Permutation P.

IV.1.2. Triple DES

Le Triple DES bien que sécurisé est employé assez peu fréquemment dans les applications communes de par son temps d'exécution relativement élevé. Bien qu'il existe plusieurs versions de Triple DES, celle approuvée en standard effectue un triple passage de l'algorithme DES (C'est bien sûr de la que vient la lenteur d'exécution du cryptage).

D'ailleurs ce n'est pas un triple passage à proprement parler du chiffrage par l'algorithme DES puisque en réalité la clé de 168 bits fournie est découpée en 3 clés de 56 bits

(Algorithme DES), voir la figure (IV.3).

La première est utilisée pour un premier chiffrage,la seconde sert à effectuer une opération de déchiffrage sur les données précédemment chiffrées (cela agit donc comme chiffrage des données sans utiliser le "même" algorithme).
Et enfin la troisième clé est utilisée pour rechiffrer les données.

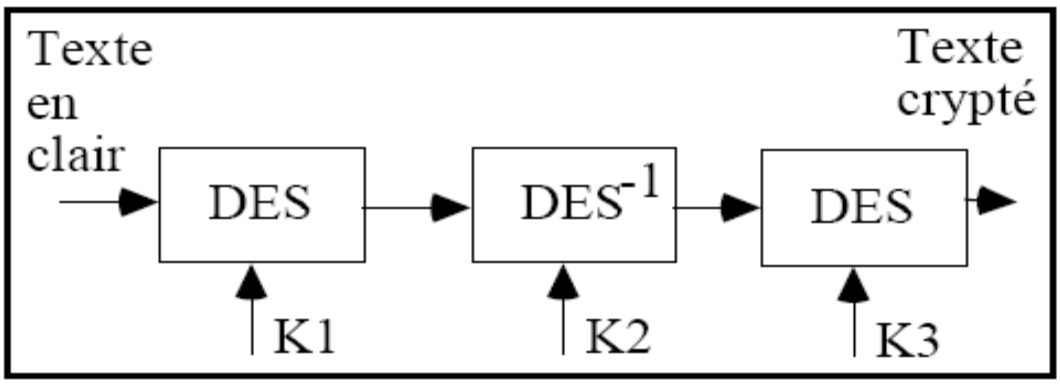


Figure.IV.3. Triple DES.

IV.1.3. Algorithme IDEA

Le système IDEA (Internationnal Data Encryption Algorithm) à été crée par X.Lai et J.Massrey en 1992, renforçant des versions préliminaires : PES (Proposed Encryption Standard), IPES (Improved Proposed Encryption Standard). IDEA, un algorithme de chiffrement de données par blocs, offre d'excéllentes garanties de sécurité. A ce jour, personne n'a encore publié de résultats démontrant des faiblesses de l'algorithme. IDEA constitue ainsi un choix judicieux pour le cryptage de transmission de données.

IV.1.3.1.Chiffrement

IDEA est un système de chiffrement n'utilise que trois opérations simples :

- le XOR bit à bit.
- l'addition modulo 2^16.
- la multiplication modulo 2^16+1.

Pour le produit, on remplace un facteur égale à zéro par 2^16.

IV.1.3.1.1. Génération des sous-clés

La clé K est de 128 bits ; on effectue une rotation de 25 vers la gauche et l'on juxtapose à droite, puis devisée en 8 blocs de 16 bits qui représentent les sous-clés, on recommence jusqu'à avoir nos 52 sous-clés. Ces clés formeront 8 groupes de 6 sous-clés (un groupe par ronde) : K1, K2, K3, K4, K5, K6, et un groupe de 4 clés pour la ronde finale : K1, K2, K3, K4.

IV.1.3.1.2. Description d'une ronde

Le texte est découpé en blocs de 64 bits, redivisés en quatre blocs de 16 bits : X1, X2, X3, X4,et l'on fait les quatorze calculs suivants pour trouver la sortie qui va être l'entrée de la ronde suivante :

- Etape1 = X1 * K1
- Etape2 = X2 + K2
- Etape3 = X3 + K3
- Etape4 = X4 * K4
- Etape5 = Etape1 XOR Etape3
- Etape6 = Etape2 XOR Etape4
- Etape7 = Etape5 * K5
- Etape8 = Etape6 + Etape7
- Etape9 = Etape8 * K6
- Etape10 = Etape7 + Etape9
- Etape11 = Etape1 XOR Etape9 => X1 de la ronde suivante
- Etape12 = Etape3 XOR Etape9 => X3 de la ronde suivante
- Etape13 = Etape2 XOR Etape10 => X2 de la ronde suivante
- Etape14 = Etape4 XOR Etape10 => X4 de la ronde suivante

Pour finir, on applique une étape supplémentaire après la huitième ronde :

- C1 = X1 * K1
- C2 = X2 + K2
- C3 = X3 + K3
- C4 = X4 * K4

Les 4 blocs C1, C2, C3, C4, forment alors le message chiffré.

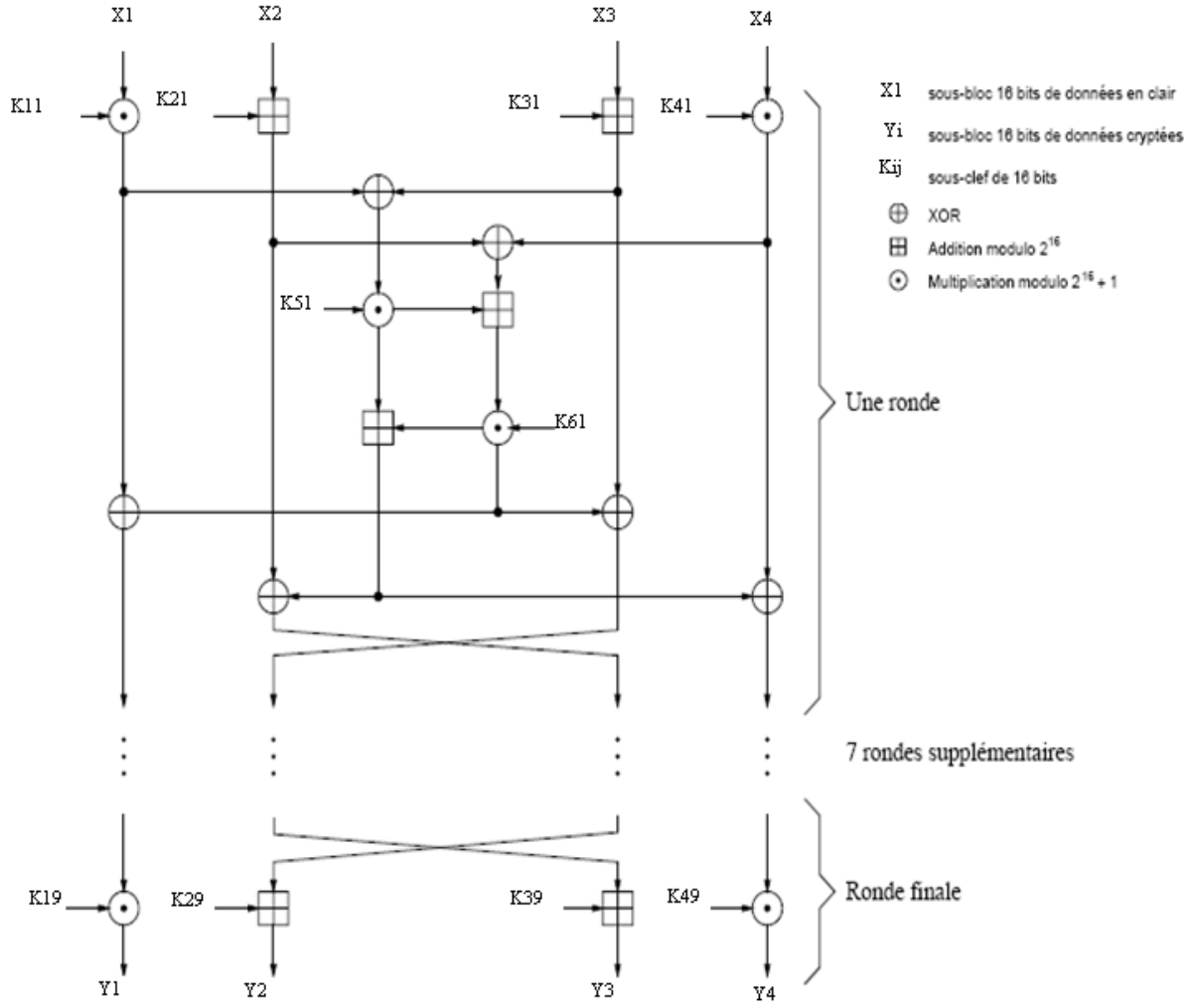


Figure.III.10. Diagramme d'IDEA.

IV.1.3.2. Déchiffrement

Pour déchiffrer le texte, il faut d'abord inverser la dernière opération :

- C1 = C1 * $K1^{-1}$
- C2 = C2 - K2
- C3 = C3 - K3
- C4 = C4 * $K4^{-1}$

On applique alors les opérations suivantes selon 8 rondes, en utilisant les groupes de 6 clés en partant de la dernière à la première :

- Etape1 = C1 XOR C3 (Etape5 lors du cryptage)
- Etape2 = C2 XOR C4 (Etape6 lors du cryptage)
- Etape3 = Etape1 * K5 (Etape7 lors du cryptage)
- Etape4 = Etape2 + Etape3 (Etape8 lors du cryptage)
- Etape5 = Etape4 * K6 (Etape9 lors du cryptage)
- Etape6 = Etape3 + Etape5 (Etape10 lors du cryptage)
- Etape7 = C1 XOR Etape5 (Etape1 lors du cryptage)
- Etape8 = C3 XOR Etape5 (Etape3 lors du cryptage)
- Etape9 = C2 XOR Etape6 (Etape2 lors du cryptage)
- Etape10 = C4 XOR Etape6 (Etape4 lors du cryptage)
- Etape11 = Etape7 * $K1^{-1}$ => C1 de la ronde suivante
- Etape12 = Etape8 - K3 => C3 de la ronde suivante
- Etape13 = Etape9 - K2 => C2 de la ronde suivante
- Etape14 = Etape10 * $K4^{-1}$ => C4 de la ronde suivante

Les 4 blocs C1, C2, C3, C4 obtenus après la dernière ronde forment alors le message en clair.

IV.1.4.Algorithme AES [9]

Avec le temps, et les progrès de l'informatique, les 2^{56} clés possibles du DES n'ont plus représenté une barrière infranchissable. Il est désormais possible, même avec des moyens modestes, de percer les messages chiffrés par DES en un temps raisonnable. En janvier 1997, le NIST (*National Institute of Standards and Technologies*) des Etats-Unis lance un appel d'offres pour élaborer l'AES, *Advanced Encryptions System*. Le cahier des charges comportait les points suivants :

- évidemment, une grande sécurité.

- une large portabilité : l'algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs 8 bits peu puissants, que dans des processeurs spécialisés pour chiffrer des milliers de télécommunications à la volée.
- la rapidité.
- une lecture facile de l'algorithme, puisqu'il est destiné à être rendu public.
- techniquement, le chiffrement doit se faire par blocs de 128 bits, les clés comportant 128,192 ou 256 bits.

Au 15 juin 1998, date de la fin des candidatures, 21 projets ont été déposés. Certains sont l'œuvre d'entreprises (IBM), d'autres regroupent des universitaires (CNRS), les derniers sont écrits par à peine quelques personnes. Pendant deux ans, les algorithmes ont été évalués par des experts, avec forum de discussion sur Internet, et organisation de conférences. Le 2 octobre 2000, le NIST donne sa réponse : c'est le Ri[22]jndael qui est choisi un algorithme mis au point par 2 belges, Joan Daemen et Vincent Rijmen.

Le Rijndael procède par blocs de 128 bits, avec une clé de 128 bit également. Chaque bloc subit une séquence de 5 transformations répétées 10 fois :

1. Addition de la clé secrète (par un ou exclusif).
2. Transformation non linéaire d'octets : les 128 bits sont répartis en 16 blocs de 8 bits (8 bits=un octet), eux-mêmes dispatchés dans un tableau 4×4. Chaque octet est transformé par une fonction non linéaire S.
3. Décalage de lignes : les 3 dernières lignes sont décalées cycliquement vers la gauche : la 2ème ligne est décalée d'une colonne, la 3ème ligne de 2 colonnes, et la 4ème ligne de 3 colonnes.
4. Brouillage des colonnes : Chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre matrice 4×4). Les calculs sur les octets de 8 bits sont réalisés dans le corps à 2^8 éléments.
5. Addition de la clé de tour : A chaque tour, une clé de tour est générée à partir de la clé secrète par un sous-algorithme (dit de cadencement). Cette clé de tour est ajoutée par un ou exclusif au dernier bloc obtenu.

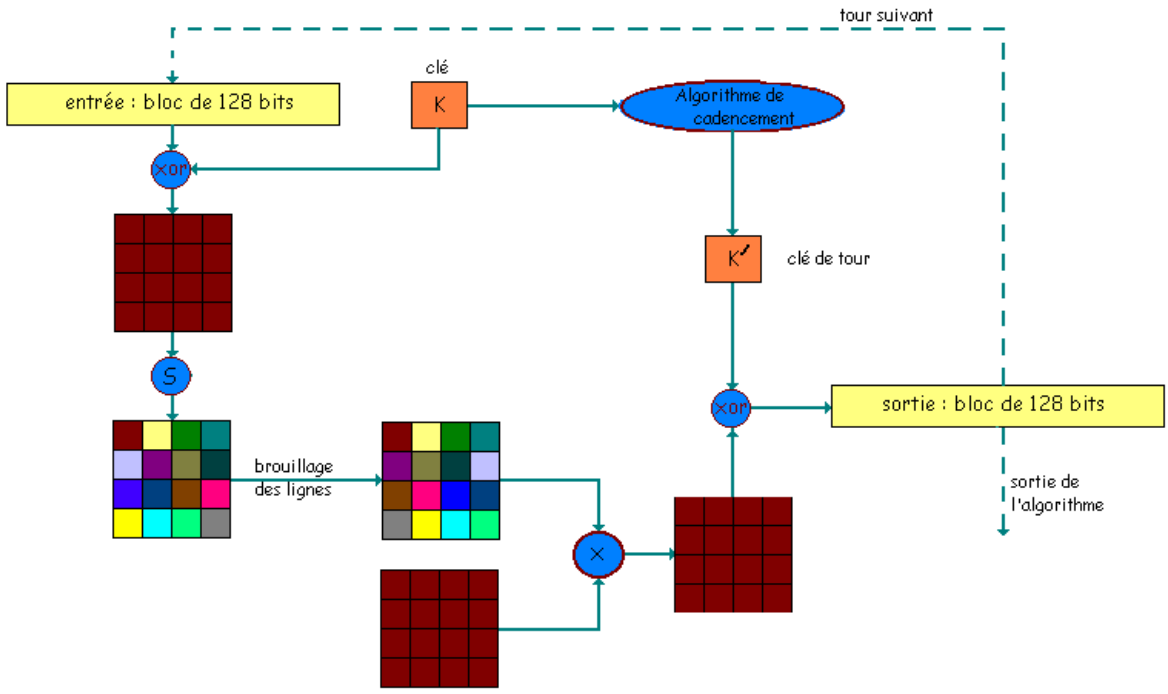


Figure.III.12. Algorithme AES.

IV.2.Algorithmes asymétriques

IV.2.1. Algorithme RSA [10]

Cette méthode a été inventée en 1977 par, Ron Rivest, Adi Shamir et Len Ademan (RSA signifie Rivest-Shamir Adelman).

RSA est un algorithme à clé publique qui sert aussi bien à la cryptographie de documents, qu'à l'authentification. Grace au faite qu'il été à clé publique, au faite qu'il était très sûr..

IV.2.1.1. Génération des clés privées et publique

Dans le système RSA, un utilisateur crée son couple (clé publique, clé privée) en utilisant la procédure suivante :

1) Choisir au hasard deux grands nombres premiers p et q.il faut que p et q contiennent au moins 100 chiffres décimaux chacun.
2) Calculer n=p q
3) Choisir un petit entier « e » qui est premier avec Ø(n)= (p-1) (q-1) ;

4) Calculer d, l'inverse par la multiplication de e modulo Ø(n) ;
5) Publier la paire Ke=(e, n) qui est la clé publique RSA .
6) Garder secret la paire Kd=(d, n) qui est la clé privée RSA.

On a alors :

- Chiffrement RSA : Eke (M)=M^e mod n,
- déchiffrement RSA : Dke (M)=M^d mod n,

Exemples :

1. Prenons p=47, q=59 (ces valeurs sont faibles et ne correspondent évidement pas à des clés réelles

- on calcule n=p*q=47*59=2773.
- On choisit « e» premier par rapport à$\emptyset(n)$. Prenant par exemple e=17
- On calcule alors, par l'algorithme d'Euclide étendu 13, « d» telle que d*e=1mod (p-1) (q-1), soit d=157.
- On a alors un couple clé publique (17,2773), clé privée (157,2773).

Pour chiffrer B, c'est la valeur 01000010=66 ; on calculera donc (66^{17})(mod 2773) c'est-à-dire 872. Pour retrouver le message d'origine, on calculera (1553^{157})(mod 872)qui donne bien 66

2. une personne A. possédant la clé publique (e, n) et qui veut envoyer le message top secret M: « pouvoir c'est vouloir » à la personne B procède comme suit :

a) Convertir le message en une suite de nombres, en prenant par exemple : a=01, b=02, c=03,……, z=26.
b) il résulte : M=16152122150918030519202215211215091 8
c) Découper le message obtenu en parties de taille égale et inferieure à celle de n, on aura donc 10 parties de trois chiffres.
   M=180 514 040 526 221 521 191 221 140 409
   M=m1 m2 m3 m4 m5 m6 m7 m8 m9 m10
d) Crypter chaque partie mi à l'aide de la formule suivante : $Ci = m_i^e mod n$

On a d'abord $p = 59, q = 73, \emptyset(n) = (p-1)(q-1) = 4176$

Prenons e=5 ; on calcule d comme suit :

$$ed \ mod \ \emptyset(n) = 1$$

Une autre méthode plus simple pour calculer d ; est de chercher un entier m tel que :

$(m * \emptyset) + 1$ sera divisible par e=5

donc : $ed = m * \emptyset(n) + 1 \Rightarrow 5d = (m * 4176) + 1$

$$\Rightarrow d = 3341 \ pour \ m = 4$$

Donc on a :$cim_i^e \ modn$

Ce qui donne : $c1 = m_1^5 \ mod 4307 = 1264$

:

$c10 = m_{10}^5 \ mod 4307 = 3165$

Le message crypté A peut l'envoyé à B.

B reçoit le message et utilise sa clé privée pour le décrypter, en appliquant la formule inverse :

$mi = c_i^d \ modn$

Ce qui donne :

M=180 514 040 526 221 521 191 221 140 409.

B prend son tableau de correspondance alphabétique et répond le message envoyé : rendez-vous lundi

IV.3. PGP (pretty good privacy) [9]

Le PGP est un algorithme utilisé pour la protection du courrier électronique, il a été mis au point par l'informaticien américain Philipe Zemmerman.

Le PGP combine à la fois le meilleur de la cryptographie symétrique (rapidité du chiffrement) et de la cryptographie symétrique (sécurité de l'échange de clés).

IV.3.1.Principe de fonctionnement du PGP

Il fonctionne suivant le principe suivant :

a) Compression : le texte à envoyer est compressé, cette étape permet de réduire le temps de transmission de données, et améliore également la sécurité. En effet, la compression détruit les modèles de texte (fréquence des lettres, mots répétés) et on sait que ces modèles sont souvent utilisés dans des analyses de cryptographie.
b) Chiffrement du message : une clé secrète IDEA est crée de manière aléatoire, et les données sont cryptées avec cette clé.
c) Chiffrement de la clé de session : la clé de session est chiffrée en utilisant la clé publique du destinataire (et l'algorithme RSA).
d) Envoi et réception du message : l'expéditeur envoie le couple message chiffré/clé de session chiffrée au destinataire. Celui-ci récupère d'abord la clé de session, en utilisant sa clé privée puis déchiffre le message grâce à la clé de session.

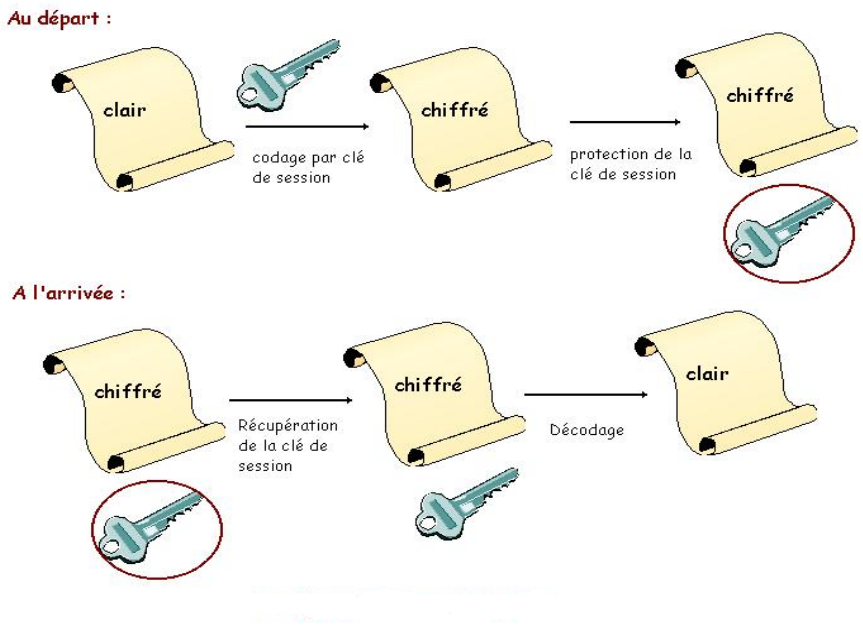


Figure.III.11. Principe de fonctionnement du PGP.

IV.3.2. Sécurité du PGP

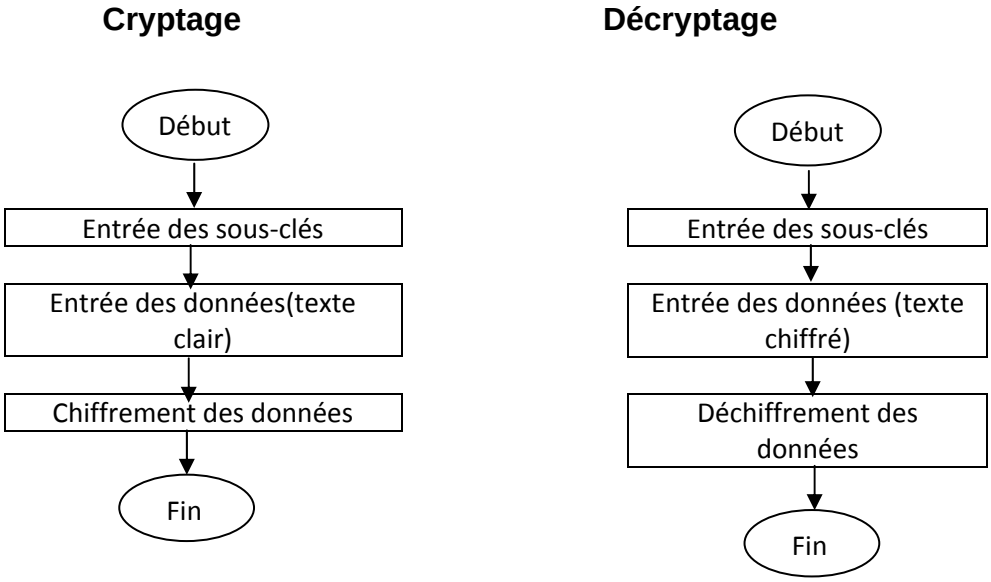
C'est la combinaison algorithme symétrique (IDEA pour crypter les données), et l'algorithme (RSA pour crypter la clé IDEA) qui confère à PGP sa vitesse et sa grande sécurité.

PGP est un système de chiffrement le plus proche de la classe militaire.

Pour la programmation de l'algorithme IDEA, on a utilisé le langage de programmation MATLAB version 6.5 dont voici les différents organigrammes :

V.1.Organigramme général

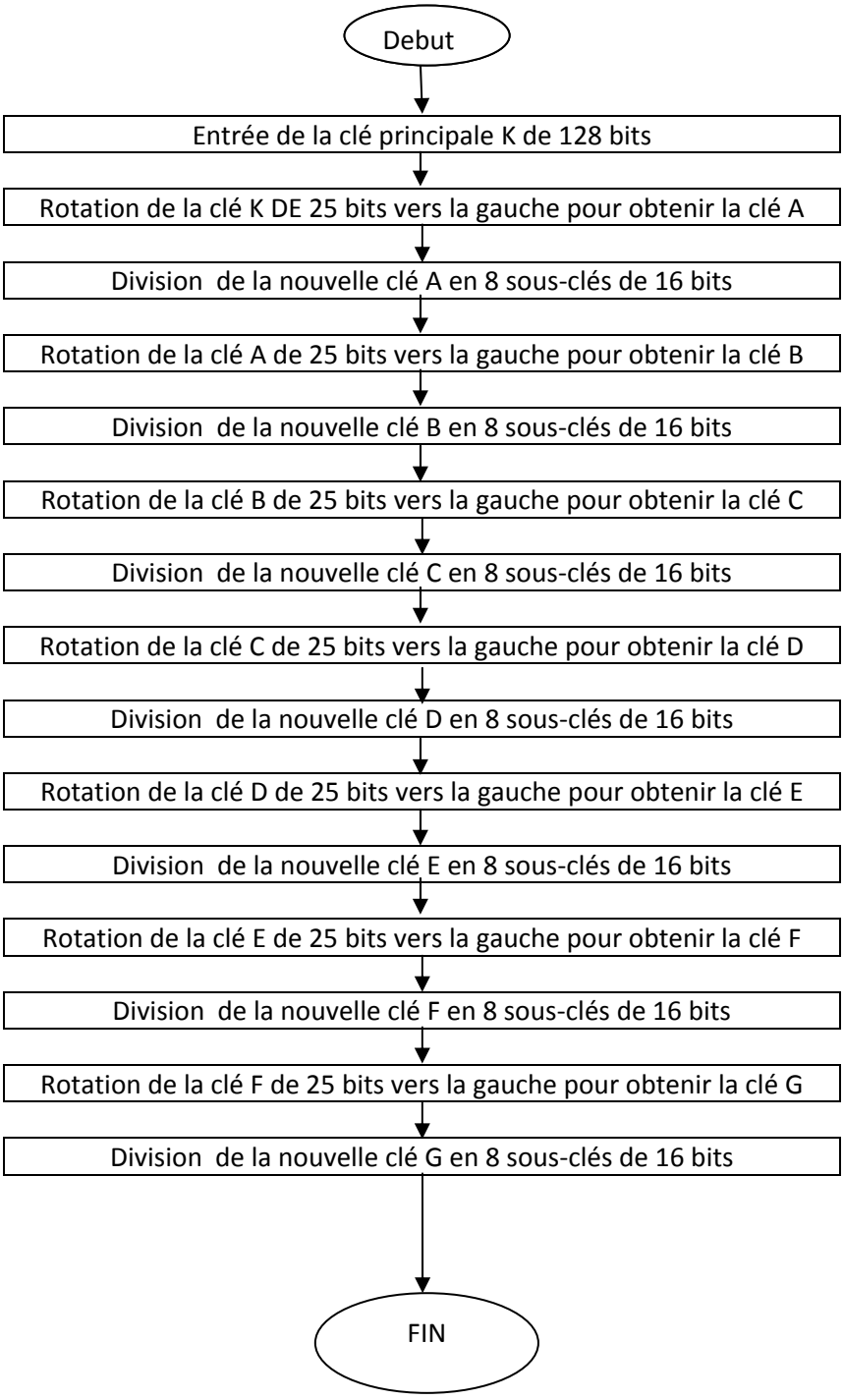
Voici les organigrammes de cryptage et de décryptage représentés dans l'organigramme (V.1) :



L'organigramme. V.1. Cryptage et décryptage.

V.2.Génération des sous-clés

On part de la clé de 128 bits ; on effectue une rotation de 25 vers la gauche et l'on juxtapose à droite, on obtient une nouvelle clé qu'on divise en huit bloc de 16 bits ; on recommence jusqu'à avoir nos 52 sous-clés



Organigramme .V.2. Génération des sous-clés.

V.3.Chiffrement

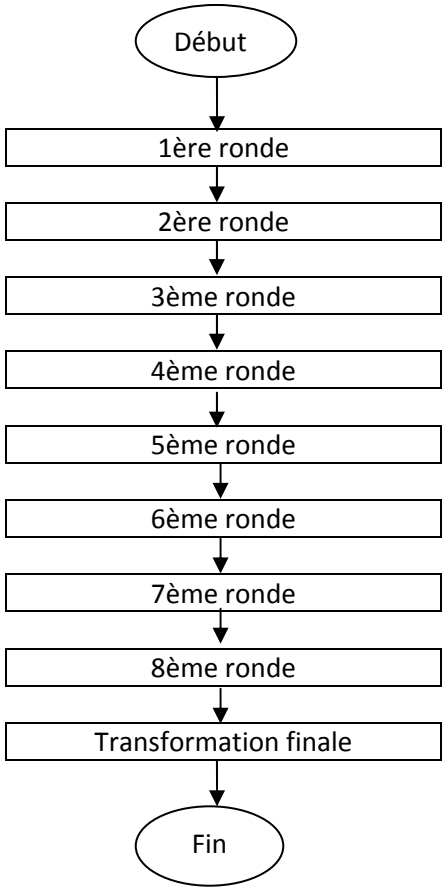
Le chiffrement est constitué de huit rondes plus une transformation finale, chaque ronde utilise le résultat de la ronde précédente.

Pour la programmation on utilise trois opérations :

+ : addition modulo 2^16.

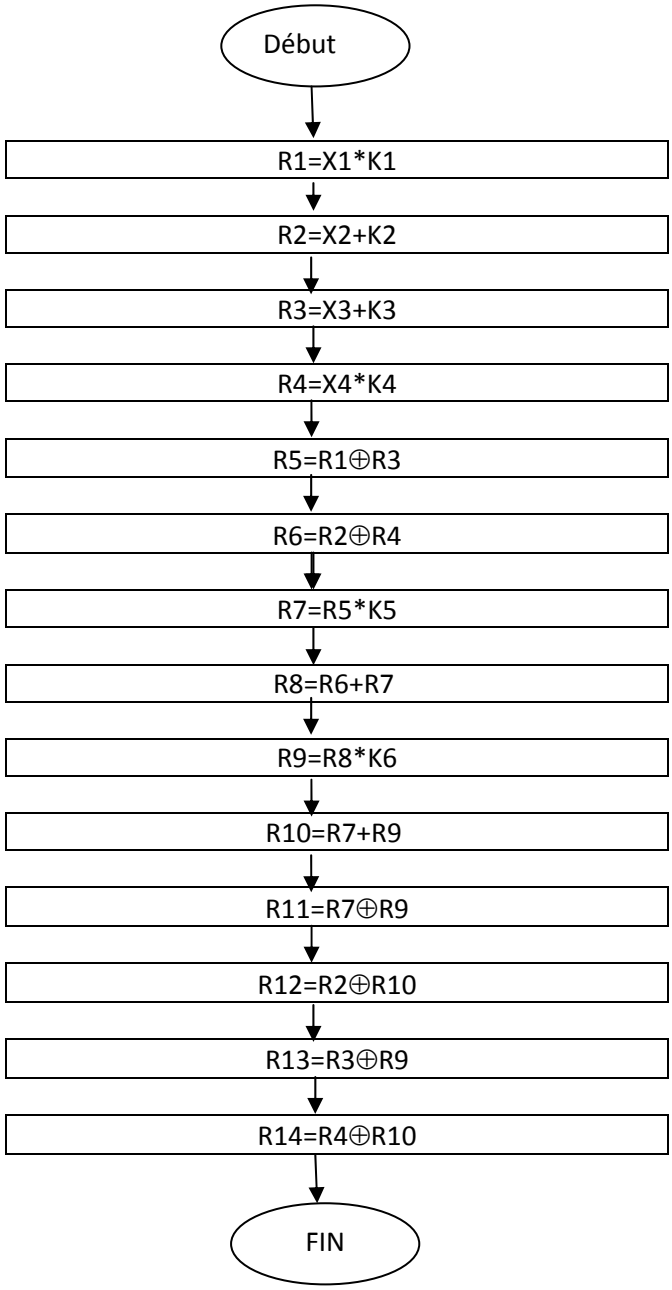
* : multiplication 2^16+1.

⊕ : ou exclusif bit par bit.



Organigramme. V.3. Chiffrement.

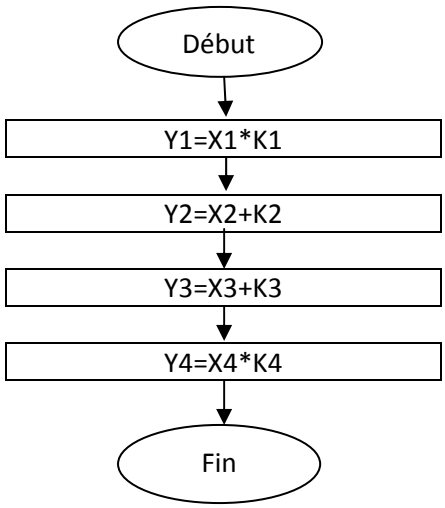
V.3.1. Description d'une ronde



Organigramme. V.4. Ronde de chiffrement.

V.3.2.Transformation finale

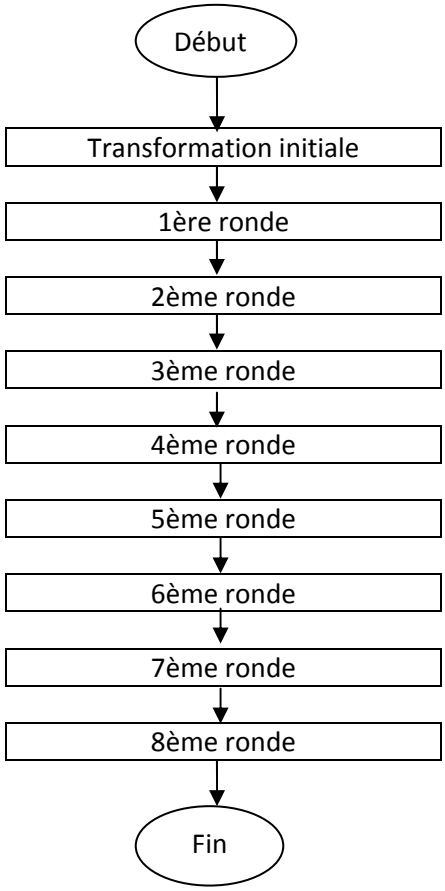
La transformation finale utilise le résultat de la huitième ronde.



Organigramme. V.5. Transformation finale.

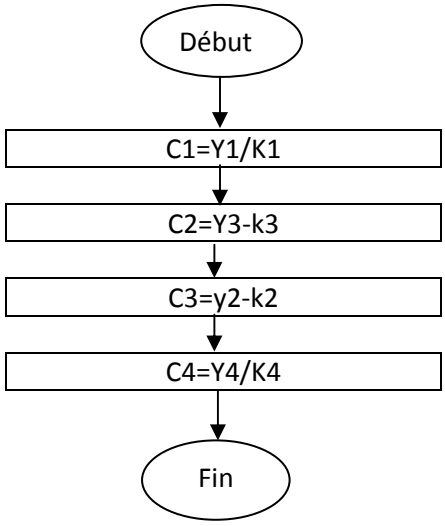
V.4. Déchiffrement

Le déchiffrement est constitué d'une transformation initiale plus huit rondes, chaque ronde utilise le résultat de la ronde précédente



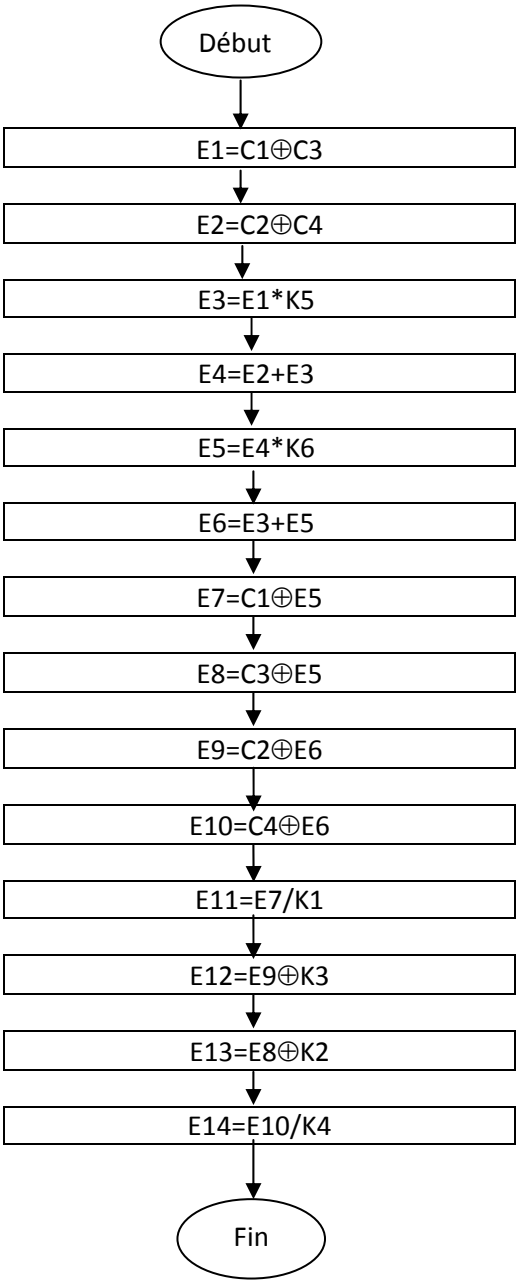
Organigramme. V.6. Déchiffrement.

V.4.1.Description de la transformation initiale



Organigramme. V.7. Transformation initiale.

V.4.2.Description d'une ronde



Organigramme. V.4. Ronde de décryptage.

CONCLUSION GENERALE

Dans ce travail, nous avons étudié le réseau de télécommunication de nouvelle génération d'Algérie Télécom et les différents protocoles de transmission utilisés dans ce type de réseau et le réseau RTC. Par ailleurs, nous avons étudié les différents techniques et algorithmes de cryptage utilisés pour sécuriser la transmission des données dans un réseau, en particulier, l'algorithme IDEA qui est très adapté aux types de données circulant dans un réseau NGN. En effet, cet algorithme s'apprête bien à l'exécution en temps réel, c'est le cas de la transmission de la parole et de la vidéo sur un réseau NGN. L'IDEA comporte plusieurs opérations qui le rendent difficile à décrypter par les personnes non autorisées, avec sa clé de 128 bits, IDEA est considéré comme pratiquement sûr.

Dans notre travail, nous avons réussi à implémenter l'algorithme IDEA sous Matlab. Les essais effectués sur cet algorithme ont donné des résultats très satisfaisants. Néanmoins, avec la collaboration de l'équipe technique de HONET de Tizi-Ouzou, ce travail peut trouver application réelle en implémentant cet algorithme au niveau de couche application dans le réseau NGN d'Algérie Télécom.

Enfin, nous souhaitons que notre travail puisse être d'un apport pour les promotions à venir et de leur servir comme support de documentation.

[1] S.AMRANE, M.CHERIFI, 2007 « Etude de l'architecture du centrale téléphonique de nouvelle génération des réseaux NGN de la wilaya de Tizi-Ouzou. » thèse ingénieur, UMMTO.

[2] R. LACEB, M. DAHMANE et O. TAMGOUT, 2006 :«étude pour la mise en œuvre d'un réseau de nouvelle génération (NGN) et migration du Réseau Téléphonique Commuté (RTC) de la wilaya de Tizi-Ouzou », thèse d'ingénieur, UMMTO.

[3] CLAUD SERVIN « Réseau & Télécom » Edition DUNOD Paris 2003.

[4] Etude réalisée pour le cabinet Acrome pour le compte de l'autorité de Régulation des télécommunications, Septembre 2007 « Etude technique, économique et règlementaire de l'évolution vers les réseaux de nouvelle génération NGN ».

[5] Technical Manual Signaling & Protocols, U-SYS SoftX3000 Softswitch System.

[6] Huawei Technologies proprietary Technical Manuel system Description U-SYS Softx3000.

[7]. Huawei Technologies proprietary Technical Manual U-SYSMRS6100.

[8] Huawei Technologie Interconnexte protocol Data configuration.

[9] T.EBRAHIMI, F.LEPREVOS, B.WARUSFEL « Cryptographie et sécurité des systèmes et réseaux » Lavoisier, 2006.

[10] « Sécurité dans les réseaux sans fils », Ingénieur en éléctronique, promotion 2005.

[11] S.Belal,T.Toubal , 2006 «Sécurité dans les réseau mobiles de 3ème génération Algorithme KASUMI »Thèse ingénieur,UMMTO.

Chapitre I

Le réseau téléphonique RTC et la signalisation SS7

Chapitre II

Le réseau de nouvelle génération NGN

Chapitre III

Généralités sur la sécurité des réseaux

Chapitre IV

Algorithmes de cryptage

Conclusion générale

Introduction générale

Abréviations

Bibliographie

Annexes

Chapitre V

Application

AES : Advenced Encryption Standard
ATM: Asynchronous Transfert Mode.
CODEC : COder DECoder.
DES : Data Encryption Standard
DSL: Digital Subscriber Line.
DTMF: Dual Tone Multi Frequency.
IDEA: International Data Encryption Algorithm.
IETF: Internet Engineering Task Force.
IP : Internet Protocol
ISDN: I ntegrated Services Digital Network.
ISO: International Standardization Organisation.
ISUP:ISDN Subscriber Part.
ITU-T : International Télécommunication Union –Télécommunication standardization sector.
IUA ISDN-Subscriber Adaptation Layer.
LAN : Local Area Network.
M2PA :MTP2-Subscriber Peer –to-Peer Adaptation Layer.
M2UA :Message Transfer Part 2(MTP2)-Subscriber Adaptation Layer.
M3UA: Message Transfer Part 3(MTP3)-Subscriber Adaptation Layer.
MAC: Media Access Control.
MG: Media Gateway.
MGC: Media Gateway Controller.
MGCP: Media Gatway Control Protocol.
MPLS: Multi-Protocol Label Switching.
MRS: Media Ressource Server.
MTP:Message Transfer Part.
NGN: Next Génération Network.
OSI: open system inteconnection.
PSTN: Public Switched Telephone Network.
QoS: Quality of Service.
RAS: registration admission status.
RSA: Rivest Shamir Adalman.
RTC: Réseau Téléphonique Commuté.
RTCP : Real Time Control Protocol.
RTP: Real Time Protocol.
RNIS : Réseau Numérique à Intégration de Services (ISDN).
SCCP: Signaling Connection Control Part.
SCN: Switched Circuit Network.
SCTP: Stream Control Transmission Protocol
SDP: Session Description Protocol.
SG: Signaling Gateway.
SIP: Session Initiation Protocol.
SS7: Signalling System 7.
TCP/IP: Transmission Control Protocol/Internet Protocol.
UDP : User Datagram Protocol.