11/621.821

République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de fin d'étude
pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**
Filière : **Télécommunications**
Spécialité : **Système de Télécommunications**

SECURITE DES DONNEES DANS LES RESEAUX DE TELECOMMUNICATIONS RADIO-MOBILE

Présenté par :

CISSE Fatou Seck

TALL Madina

Sous la direction de :

Dr. TABA Med Tahar

Mai 2014

Remerciement

En préambule à ce mémoire nous remercions ALLAH qui nous aide et nous a donné la patience et le courage durant ces longue années d'études.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Ces remerciements vont tout d'abord au corps professoral et administratif de la faculté **08 Mai 1945 de GUELMA** des Sciences de Technologie, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

Nous tenons à remercier sincèrement **M. Med Taba Tahar** qui en étant notre encadreur sait toujours montrer à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacrer et sans qui le mémoire n'aurait jamais vu le jour. Nous tenons également à remercier **M. khebizi Ali** Adjoint du chef de département de l'informatique à l'université 08 Mai 1945 de Guelma et **M. Meguellatni Djamel** Informaticien, pour leur aide et leur soutien.

On n'oublie pas nos parents pour leur contribution, leurs soutiens et leur patience.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et ami(e)s, qui nous ont toujours encouragés au cours de la réalisation de ce mémoire.

Merci à tous et à toutes !!!

Dédicace

A mes très chers parents ***M. CISSE Amadou Boubacar*** *et* ***Mme. CISSE Fatoumata Boncano Touré****, je ne saurais comment vous remercier pour la très bonne éducation que vous nous avez donnée à mes frères et à moi. Vous m'avez appris le sens de l'honneur, le respect de soi et de son prochain, à ne jamais baissé les bras, à toujours rester forte quelle que soit la situation dans laquelle je me trouve, d'être fière de qui je suis et de ne jamais oublier d'où je suis afin de réussir au mieux ma vie. Merci pour le soutien moral et financier que vous m'avez apporté et que vous continuez de m'apporter à chaque instant de ma vie. Merci à vous, de m'avoir inculqué les vraies valeurs de la vie et InSha Allah vos efforts ne seront pas vains ;*

Qu'Allah vous gratifie de sa miséricorde et vous accorde son paradis (Amin).

A mes frères et sœurs : ***Malick, Gogo, Abba et Aissata*** *vos encouragements, soutien, réconfort, présence et amour me sont précieux et indispensables ;*

A mes tantes, oncles, cousins et cousines ;

A ***M. DIALLO Mamadou Kolon****, merci pour tes bons conseils et surtout pour tous ses moments passés à mes côtés. Ta présence m'a permis de faire face à plein d'épreuves de la vie. Fern Bork a dit : « Il y a des personnes qui marquent nos vies, même si cela ne dure qu'un moment. Et nous ne sommes plus les mêmes. Le temps n'a pas d'importance mais certains moments en ont pour toujours », merci de me soutenir et surtout d'être présent pour me relever à chacune de mes chutes ;*

A ***M. LITIMBA Alberto Di Gladi*** *et à* ***M. GUISSO Moustapha Amadou****, merci mille fois à vous d'être si près de moi tout en étant à des milliers de kilomètres. Votre amitié est sans condition, vous m'avez appris que les liens du cœur sont plus forts que ceux du sang, vous êtes et resterez dans mon cœur InSha Allah;*

A mon amie et binôme ***Mlle. TALL Madina,*** *merci pour toute la patience dont tu fais preuve envers moi, le travail en équipe n'est pas facile et tu as su le rendre agréable ;*

A mes ami(e)s qui me sont resté(e)s fidèles et qui m'ont soutenu(e)s dans les situations difficiles et tout comme les moments de joie.

A toute la communauté étrangère de Guelma et plus précisément à la ***Promotion Malienne de 2009*** *;*

Ce travail vous est dédié !

CISSE Fatou Seck

Dédicace

Je tiens tout d'abord a remercié le tout puissant et le très miséricordieux, de m'avoir donné la capacité d'écrire et de réfléchir, la force d'y croire, la patience d'aller jusqu'au bout de mes rêve et le bonheur de lever mes mains vers le ciel et te dire « YA QAYYUM »

Je dédie ce modeste travail à mon très cher **Père Saidou Cheick Tall** et ma très chère et douce **MèreOumouBaouro Cissé**, eux qui m'ont donné la vie, le symbole de tendresse qui se sont sacrifiés pour mon bonheur et ma réussite; école de mon enfance, qui ont été mon ombre durant toutes ces années d'études, et qui ont veillé sur moi tout au long de ma vie à m'encourager, à me donner l'aide et à me protéger. Que Dieu vous gardes et vous protèges.je vous remercie pour l'éducation que vous nous avez prodigué à mes frères et moi avec tous les moyens et au prix de toutes les sacrifices qu'ils ont consentis à notre égard. Merci pour le sens du devoir que vous m'avez enseigné depuis mon enfance.

A mon **frère Amadou Saidou** et mes**sœurs Aminata Saidou et Kadidia Saidou** que j'aime tant, qui n'ont cessé de me soutenir pendant tout mon parcours. Les mots ne peuvent résumer ma reconnaissance et mon amour à votre égard je vous aime tant.

A mes **Tantes Oncles Cousins et Cousines** de la famille **Tall et Cissé**pour leur encouragement et leur soutien.

A Mr **Sankaré El Hadj Amadou** pour son soutien moral et son encouragement à la réalisation de ce travail.

A mon chère amie, binôme **Fatou Seck Cissé** qui m'a supporté durant ces quelque mois de travail ensemble et chez qui j'ai trouvé l'attente dont j'avais besoin.

A mes **ami(e)s** avec lesquels j'ai partagé mes moments de joie et de bonheur. Que toute personne ayant m'aider de près ou de loin trouve ici l'expression de ma reconnaissante.

A toute la communauté étrangère de **Guelma** et plus précisément la promotion malienne de **2009.**

Madina Tall

Table des Matières

TABLES DES MATIERES

Chapitre III : Algorithmes de Chiffrement

Chapitre IV : Simulation

Introduction Générale

Introduction générale

L'évolution des technologies de l'information et de la communication et le besoin croissant de mobilité ont donné naissance aux réseaux sans fil qui utilisent comme support de transmission les ondes hertziennes suivant la technologie cellulaire.

Les réseaux de communication sans fil sont en plein développement du fait de leur interface radio qui offre la mobilité aux utilisateurs et sont souvent utilisés comme extension d'un réseau filaire déjà existant. Ce sont des réseaux faciles et rapides à déployer et qui permettent, en plus de la transmission de données, d'autres applications telles que la voix, la vidéo et l'Internet. Ces réseaux comportent cependant des failles, ils sont moins sécurisés que les réseaux filaires et les informations transmises à travers l'espace peuvent être captés par d'autres individus malveillants.

Sécuriser un réseau consiste donc à prendre en compte tous les risques possibles, tels que les attaques volontaires, les accidents, les défauts logiciels ou matériels ou encore les erreurs humaines et à les réduire autant que possible.

La cryptographie étant l'art de cacher des messages, c'est de là que vient l'idée de sécurisation des données afin qu'elles ne puissent pas être interceptées par d'autres individus. Ce pendant l'histoire de la cryptographie débuta depuis l'Antiquité. Parmi, les méthodes de cryptographie nous avons : la Cryptographie Classique, la Cryptographie Moderne et la Cryptographie Future et cette dernière étant en voie de développement. Ces méthodes cryptographiques seront étudiées tout au long de notre travail afin de savoir laquelle offre une meilleure sécurité.

Notre travail consiste à étudier les différentes méthodes utilisées dans la cryptographie des messages, des images et sons et d'essayer de faire leurs implémentations sous matlab.

Pour mener à bien notre projet nous avons d'abord procédé, dans le premier chapitre à une brève présentation et architectures du réseau GSM et du réseau Wifi.

Le deuxième chapitre est consacré à la sécurité des données dans les réseaux de télécommunications. On y décrit également la cryptographie et les différents types de cryptages utilisés en GSM et WIFI.

Le troisième chapitre présente les différents types d'algorithmes cryptographiques utilisés pour faire le cryptage leur historique et leur principe de fonctionnement, leurs avantages et leurs inconvénients.

Quant au dernier chapitre, il est réservé à l'implémentation de ces algorithmes sur Matlab. Et nous terminons notre travail par une conclusion et perspectives.

Chapitre I

Présentation des réseaux GSM et Wifi

Présentation des réseaux GSM et Wifi

Introduction

La téléphonie mobile est un système de communication basé sur la radiotéléphonie, qui est la transmission de la voix sous forme d'une onde radio.

Le GSM est une norme de seconde génération pour la téléphonie mobile s'appuyant sur les transmissions numériques permettant une sécurisation des données (avec **cryptage**). La protection est assurée par les algorithmes de chiffrement A5/1 et A5/2. Le réseau GSM est idéal pour les communications de type « voix »

Les réseaux sans fils s'appuient sur les ondes hertziennes comme support de transmission suivant la technologie cellulaire. Ce sont des réseaux faciles et rapides à déployer et qui permettent, en plus de la transmission de données, d'autres applications telles que la voix, la vidéo et l'Internet. Ces réseaux comportent cependant des failles, ils sont **moins sécurisés** que les réseaux filaires et la qualité de service laisse parfois à désirer.

Ce premier chapitre est basé sur le principe et fonctionnement des réseaux GSM et Wifi.

I.1. Présentation du GSM (Global System for Mobile communications)

I.1.1. Evolution de la téléphonie mobile

L'histoire de la téléphonie mobile (numérique) débute réellement en 1982. En effet, à cette date, le Groupe Système Mobile, appelé GSM, est créé par la Conférence Européenne des administrations des Postes et Télécommunications (CEPT) afin d'élaborer les normes de communications mobiles pour l'Europe dans la bande de fréquences de 890 à 915 [*MHz*] pour l'émission à partir des stations mobiles et 935 à 960 [*MHZ*] pour l'émission à partir de stations fixées. Il y eut bien des systèmes de mobilophonie analogique (MOB1 et MOB2, arrêté en 1999), mais le succès de ce réseau ne fut pas au rendez-vous.

Les années 80 voient le développement du numérique tant au niveau de la transmission qu'au niveau du traitement des signaux, avec pour dérivés des techniques de transmission fiables, grâce à un encodage particulier des signaux préalablement à l'envoi dans un canal, et l'obtention de débits de transmission raisonnables pour les signaux (par exemple 9, 6 kilobits par seconde, noté [*kb/s*], pour un signal de parole).

Ainsi, en 1987, le groupe GSM fixe les choix technologiques relatifs à l'usage des télécommunications mobiles: transmission numérique, multiplexage temporel des canaux radio, **chiffrement des informations** ainsi qu'un nouveau codage de la parole. Il faut attendre 1991 pour que la première communication expérimentale par GSM ait lieu. Au passage, le sigle GSM change de signification et devient Global System for Mobile communications et les spécifications sont adaptées pour des systèmes fonctionnant dans la bande des 1800 [*MHz*]. [1]

I.1.2. Architecture du réseau GSM (Global System for Mobile) :

L'architecture du réseau GSM est représentée par la figure ci-dessous :

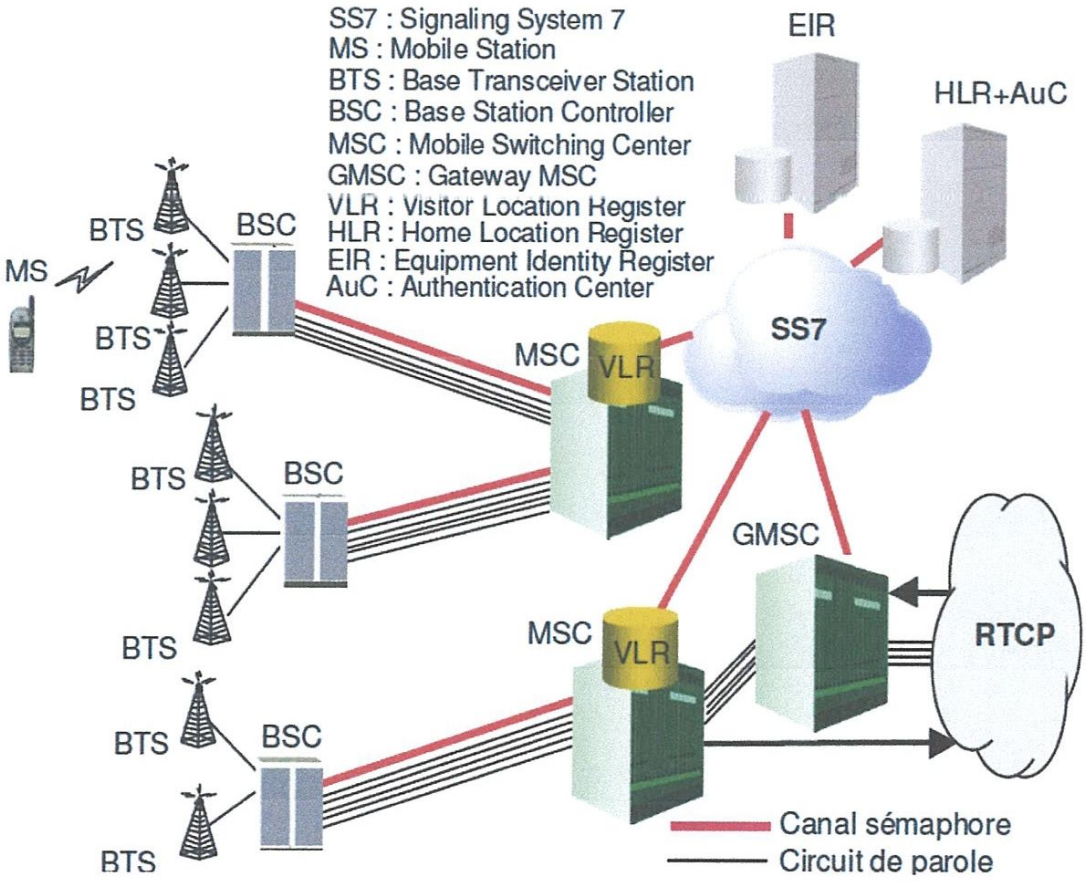

Figure I.1. : Architecture du réseau GSM

➢ **Station Mobile (MS, Mobile Station)**

Le but d'un réseau GSM/DCS est d'offrir des services de télécommunication à des abonnés, quels que soient leurs déplacements à l'intérieur d'une zone de service, desservie par un opérateur ou éventuellement par plusieurs opérateurs ayant passé des accords mutuels. Pour ce faire, l'abonné mobile utilise une station mobile (MS, Mobile Station) qui est constituée de deux éléments séparables :

• Un équipement mobile qui fournit les capacités radio et logicielles nécessaires au dialogue avec le réseau et demeure indépendant de l'abonné utilisateur.

• Une carte SIM (Subscriber Identification Module) qui contient les caractéristiques de l'abonné et de ses droits. Lorsque la carte n'est pas présente dans le terminal, le seul service que peut accepter le réseau de la part de l'abonné mobile est le service d'urgence.

Sous-système Radio (BSS, Base Station Subsystem)

➢ **Base Transceiver Station (BTS)**

La BTS (Base Transceiver Station) relie les stations mobiles à l'infrastructure fixe du réseau. La BTS est composée d'un ensemble d'émetteur / récepteurs. Elle assure : La gestion du multiplexage temporel (une porteuse est divisée en 8 slots dont 7 sont alloués aux utilisateurs), et la gestion des sauts de fréquence. Des opérations de **chiffrement**. Des mesures radio permettant de vérifier la qualité de service; ces mesures sont transmises directement au BSC. La gestion de la liaison de données (données de trafic et de signalisation) entre les mobiles et la BTS.

La gestion de la liaison de trafic et de signalisation avec le BSC.

La capacité maximale typique d'une BTS est de 16 porteuses, soit 112 communications simultanées. En zone urbaine où le diamètre de couverture d'une BTS est réduit, cette capacité peut descendre à 4 porteuses soit 28 communications.

➢ **Base Station Controller (BSC)**

Un BSC gère un ou plusieurs BTS et n'est relié qu'à un seul MSC. Pour le trafic abonné venant des BTS, le BSC joue le rôle de concentrateur. Pour le trafic venant du commutateur, il joue le rôle d'aiguilleur vers la BTS dont dépend le destinataire.
Un BSC utilise les mesures radio des BTS pour gérer la signalisation des "Handover" entre les cellules dont il a la responsabilité.

Sous-système réseau (NSS, Network Subsystem)

➢ **Mobile Switching Center (MSC)**

Un MSC (Mobile Switching Center) est un commutateur qui réalise les fonctions de connexion et de signalisation pour les mobiles localisés dans une zone géographique appelée zone de localisation du MSC. La différence principale entre un MSC et un commutateur d'un réseau fixe est qu'un MSC doit prendre en compte l'impact de l'allocation des ressources radio aux mobiles et la mobilité des mobiles. Il doit posséder des ressources suffisantes pour réaliser au moins les procédures suivantes :
• Procédures pour l'enregistrement des localisations.
• Procédures requises pour les handovers.
Un MSC constitue l'interface entre le système radio et les réseaux fixes. Il réalise toutes les fonctions nécessaires à la mise en œuvre des appels de et vers les mobiles.

Dans la pratique, un MSC intègre les fonctionnalités d'un VLR.

➢ **Gateway MSC (GMSC)**

Si le Réseau Téléphonique Commuté (RTC) doit router un appel vers un abonné mobile, 'appel est routé vers un MSC. Ce MSC interroge le HLR concerné, puis route l'appel vers le MSC sous lequel le mobile est localisé (il peut s'agir du même MSC). Un MSC qui reçoit un appel d'un autre réseau et qui assure le routage de cet appel vers la position de localisation d'un mobile est appelé Gateway MSC (GMSC).

➢ Home Location Register (HLR)

Le HLR (Home Location Register) contient les informations relatives aux abonnés du réseau. Un réseau peut posséder plusieurs bases pour mettre en œuvre le HLR en fonction des capacités de ces bases de données. Dans un HLR, chaque abonné est décrit par un enregistrement contenant le détail des options d'abonnement et des services complémentaires accessibles à l'abonné. A ces informations statiques se rajoutent des informations dynamiques telles que la dernière localisation connue du mobile (localisation permettant la taxation et le routage des appels vers le MSC sous lequel le mobile est localisé) et son état. Le HLR contient par ailleurs la clé secrète de l'abonné qui permet au service d'authentifier l'abonné. Cette clé est inscrite sous un format codé que seul l'AUC (Authentication Center) peut décrypter.

➢ Visitor Location Register (VLR)

Le VLR (Visitor Location Register) est une base de données généralement associée à un commutateur MSC. Il est aussi possible de considérer un VLR partagé par plusieurs MSCs. Sa mission est d'enregistrer des informations dynamiques relativess aux abonnés actuellement connectés. Le réseau doit connaître à chaque instant la localisation des abonnés présents. Dans le VLR, chaque abonné est décrit en particulier par un identifiant et une localisation. Grâce à ces informations, le réseau est apte à acheminer un appel vers un abonné mobile. A chaque changement de zone de localisation d'un abonné, le VLR du MSC auquel est rattaché le mobile doit être mis à jour ainsi que l'enregistrement de cet abonné dans le HLR. Lorsqu'un appel doit être délivré, c'est le HLR qui est le premier interrogé afin de connaître la dernière localisation connue de l'abonné.

➢ Authentication Center (AUC)

L'AUC (Authentication Center) est associé à un HLR et sauvegarde une clé d'identification pour chaque abonné mobile enregistré dans ce HLR. Cette clé est utilisée pour fabriquer :

• Les données nécessaires pour authentifier l'abonné dans le réseau GSM.

• Une clé de chiffrement de la parole (Kc) sur le canal radio entre le mobile et la partie fixe du réseau GSM. L'AuC est une fonctionnalité généralement intégrée dans le HLR.

➢ **Equipment Identity Register (EIR)**

Un EIR sauvegarde toutes les identités des équipements mobiles utilisés dans un réseau GSM. Cette fonctionnalité peut être intégrée dans le HLR.
Chaque poste mobile est enregistré dans l'EIR dans une liste :
• Liste "blanche" : poste utilisable sans restriction.
• Liste "grise" : poste sous surveillance (traçage d'appels).
• Liste "noire" : poste volé ou dont les caractéristiques techniques sont incompatibles, avec la qualité requise dans un réseau GSM (localisation non autorisée).

➢ **Réseau Sémaphore Numéro 7 appliqué au GSM**

Le mode associé est utilisé entre les BSCs et les MSCs. Le protocole de signalisation utilisé est BSSAP (Base Station Subsystem Application Part).
Le mode quasi-associé s'applique au sous-système réseau (NSS, Network Subsystem). Les MSCs, GMSCs, HLR et EIR sont considérés comme des SPs (Signaling Point) rattachés à des STPs (Signaling Transfer Point). Les protocoles de signalisation considérés sont ISUP, MAP (Mobile Application Part), INAP (Intelligent Network Application Part) et CAP (CAMEL Application Part). [5]

I.1.3. Bande de fréquence du GSM

La norme GSM a connu une évolution. La première génération utilise la bande de fréquence des 900 MHz, alors que la 2ième génération utilise la bande des 1800 MHz.

Chaque canal radio comprend un couple de deux canaux (ou bandes de fréquences), l'un pour la transmission des signaux de la station de base vers les stations mobiles, le canal descendant, l'autre pour la transmission des signaux des stations mobiles vers la station de base, le canal montant. Le GSM exploite à la fois les techniques SDMA (Space Division

Multiple Access), FDMA (Frequency Division Multiple Access) et TDMA (Time Division Multiple Access) , (espace, fréquence, temps).

Les caractéristiques de chaque génération sont données au tableau suivant:

	GSM-900	GSM-1800
Bande spectrale- Canaux descendants	935 à 960 MHz	1805 à 1880 MHz
Bande spectrale- Canaux montant	890 à 915 MHz	1710 à 1785 MHz
Espacement entre les canaux d'un couple	45 MHz	95 MHz
Nombre de canaux (multiplexage FDMA)	124	374
Largeur des canaux	200 KHz	200 KHz
Multiplexage TDMA	8	8
Nombre de canaux logiques	992	2992

Tableau I.1. : Bandes de fréquences GSM et leurs caractéristiques.

Il est à noter que ce ne sont pas tous les pays qui peuvent utiliser toutes les bandes spectrales en raison d'applications militaires et d'une utilisation déjà réservée pour les systèmes cellulaires analogiques. De plus, si dans un pays donné plusieurs compagnies exploitent un réseau numérique, alors chacun aura une bande de fréquences différentes afin de prévenir les chevauchements. [7]

Présentation du réseau Wifi (Wireless Fidelity)

I.2.1. Evolution du réseau d'accès sans fil wifi

Le Wi-Fi est un ensemble de protocoles de communication sans fil régi par les normes du groupe IEEE 802.11. Dans la pratique, le réseau Wi-Fi permet de relier des ordinateurs portables, des agendas électroniques, des téléphones portables, des machines de bureau, des assistants personnels (PDA), etc. au sein d'un réseau informatique afin de permettre la transmission de données entre eux. Malheureusement un aspect de la configuration est souvent négligé et méconnu : « **la sécurité** ». Nous allons voir le niveau de sécurité des différents systèmes de chiffrement pouvant être utilisés dans les implémentations modernes du Wifi. [2]

La norme IEEE 802.11 a été définie par le consortium IEEE (Institue of Electrical and Electronics Engineers) en 1999. Le nom « Wifi » est une marque déposée par le WECA (Wireless Ethernet Compatibily Alliance). **[3]**

I.2.1.a. Les normes wifi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbit/s. Des révisions ont été apportées à la norme originale afin d'améliorer le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11n, appelées normes 802.11 physiques) ou de spécifier des détails de sécurité ou d'interopérabilité. Voici un récapitulatif des différentes révisions de la norme 802.11 et leur signification :

- ✓ **La norme 802.11a :** Wifi 5

La norme 802.11a (baptisée Wi-Fi 5) permet d'obtenir un haut débit (dans un rayon de 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels). La norme 802.11a spécifie 52 canaux de sous-porteuses radio dans la bande de fréquences des 5 GHz (bande U-NII = Unlicensed - National Information Infrastructure), huit combinaisons, non superposées, sont utilisables pour le canal principal. La modulation utilisée est, au choix : 16-QAM, 64-QAM, QPSK ou BPSK.

✓ **La norme 802.11b**

La norme 802.11b est la norme la plus répandue en base installée actuellement. Elle propose un débit théorique de 11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu'à 300 mètres (en théorie) dans un environnement dégagé. La plage de fréquences utilisée est la bande des 2,4 GHz (Bande ISM = Industrial Scientific Medical) avec, en France, 13 canaux radio disponibles dont 3 au maximum non superposés (1 - 6 - 11, 2 - 7 - 12, ...). La modulation utilisable est, au choix : DBPSK ou DQPSK.

✓ **La norme 802.11c :** pontage 802.11 vers 802.11d

La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.11d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).

✓ **La norme 802.11d :** internationalisation

La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d'origine du matériel.

✓ **La norme 802.11e :** amélioration de la qualité de service

La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche « liaison de données ». Ainsi, cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo.

✓ **La norme 802.11f :** itinérance (en roaming)

La norme 802.11f est une recommandation à l'intention des vendeurs de points d'accès pour une meilleure interopérabilité des produits.

Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement quelles que

soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (en roaming).

✓ **La norme 802.11g**

La norme 802.11g offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) sur la bande de fréquences des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. Cette aptitude permet aux nouveaux équipements de proposer le 802.11g tout en restant compatibles avec les réseaux existants qui sont souvent encore en 802.11b. Le principe est le même que celui de la norme 802.11a puisqu'on utilise ici 52 canaux de sous-porteuses radio mais cette fois dans la bande de fréquences des 2,4 GHz. Ces sous-porteuses permettent une modulation OFDM autorisant de plus hauts débits que les modulations classiques BPSK, QPSK ou QAM utilisés par la norme 802.11a.

Cette modulation OFDM étant interne à l'une des 14 bandes 20 MHz possibles, il est donc toujours possible d'utiliser au maximum 3 de ces canaux non superposés (1-6-11, 2-7-12, ...) et ce, par exemple, pour des réseaux différents.

✓ **La norme 802.11h**

La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (Hiperlan 2, d'où le « h » de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie.

✓ **La norme 802.11i**

La norme 802.11i a pour but d'améliorer la sécurité des transmissions (**gestion et distribution des clés, chiffrement et authentification**). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les standards 802.11a, 802.11b et 802.11g.

✓ **La norme 802.11IR**

La norme 802.11IR a été élaborée de manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.

✓ **La norme 802.11j**

La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne

✓ **La norme 802.11n : WWiSE (World-Wide Spectrum Efficiency)**

La norme 802.11n est disponible depuis le 11 septembre 2009. Le débit théorique atteint les 300 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 100 mètres) grâce aux technologies MIMO (Multiple-Input Multiple-Output) et OFDM (Orthogonal Frequency Division Multiplexing). En avril 2006, des périphériques à la norme 802.11n commencent à apparaître basés sur le Draft 1.0 (brouillon 1.0) ; le Draft 2.0 est sorti en mars 2007, les périphériques basés sur ce brouillon seraient compatibles avec la version finale du standard. Des équipements qualifiés de « pré-N » sont disponibles depuis 2006 : ce sont des équipements qui mettent en œuvre une technique MIMO d'une façon propriétaire, sans rapport avec la norme 802.11n.

Le 802.11n a été conçu pour pouvoir utiliser les fréquences 2,4 GHz ou 5 GHz. Les premiers adaptateurs 802.11n actuellement disponibles sont généralement simple-bande à 2,4 GHz, mais des adaptateurs double-bande (2,4 GHz ou 5 GHz, au choix) ou même double-radio (2,4 GHz et 5 GHz simultanément) sont également disponibles. Le 802.11n saura combiner jusqu'à 8 canaux non superposés, ce qui permettra en théorie d'atteindre une capacité totale effective de presque un gigabit par seconde

✓ **La norme 802.11s : Réseau Mesh**

La norme 802.11s est actuellement en cours d'élaboration. Le débit théorique atteint aujourd'hui 10 à 20 Mbit/s. Elle vise à implémenter la mobilité sur les réseaux de type Ad-Hoc. Tout point qui reçoit le signal est capable de le retransmettre. Elle constitue ainsi une

toile au-dessus du réseau existant. Un des protocoles utilisé pour mettre en œuvre son routage est OLSR.

- ✓ **La norme 802.11v**

La norme 802.11v a été adoptée le 2 février 2011. Elle décrit des normes de gestion des terminaux en réseau: reportings, gestion des canaux, gestion des conflits et interférence, service de filtrage du trafic...

- ✓ **La norme 802.11a :** amélioration du débit et de la couverture

IEEE 802.11ac est un standard de transmission sans fil en cours de développement qui permettra une connexion sans fil haut débit en dessous de 6 GHz (ce qui est communément connu comme la bande des 5 GHz). Les canaux attendus offriraient 500Mbps chacun, soit jusqu'à 8Gbps de débit pour un flux grâce au multiplexage. La ratification est attendue pour fin 2012 à fin 2013.

Linksys, la division grand public de **Cisco Systems**, a développé la technologie **SRX** pour « Speed and Range Expansion » (« Vitesse et Portée Étendue »). Celle-ci superpose le signal de deux signaux 802.11g pour doubler le taux de transfert des données. Le taux maximum de transfert des données via un réseau sans fil SRX400 dépasse donc les capacités d'un réseau filaire Ethernet 10/100 que l'on trouve dans la plupart des réseaux. [4]

I.2.2. Architecture du réseau sans fil wifi

Les réseaux Wifi possèdent une architecture basée sur un système cellulaire. Les stations 802.11 peuvent s'organiser suivant deux modes de fonctionnement : Le mode Infrastructure et le mode ad-hoc. [3]

I.2.2.1. Le mode Infrastructure

Le mode Infrastructure est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (PA) qui agissent comme des concentrateurs (exemple : répéteur ou commutateur en réseau Ethernet). Autrefois ce mode était essentiellement utilisé en entreprise. Dans ce cas, la mise en place d'un tel réseau oblige de poser à intervalles réguliers des bornes « Point d'accès » (PA) dans

la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID = Service Set IDentifier) afin de pouvoir communiquer. L'avantage de ce mode, en entreprise, est de garantir un passage obligé par le Point d'accès: il est donc possible de vérifier qui accède au réseau. Actuellement les FAI, les boutiques spécialisées et les grandes surfaces fournissent aux particuliers des routeurs sans fil qui fonctionnent en mode Infrastructure, tout en étant très facile à configurer. [6]

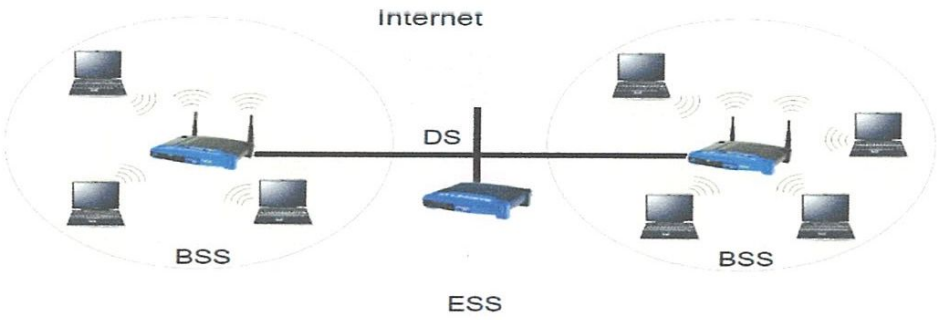

Figure I.2. : Mode infrastructure ESS (Extented Service Set)

I.2.2.2. Le mode « ad hoc »

Le mode « Ad-Hoc » est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès (en anglais : Access Point [AP]). Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire (exemple : échange de fichiers entre portables dans un train, dans la rue, au café…). La mise en place d'un tel réseau se borne à configurer les machines en mode ad hoc (au lieu du mode Infrastructure), la sélection d'un canal (fréquence), d'un nom de réseau (SSID) communs à tous et si nécessaire d'une clé de chiffrement. L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de point d'accès. Des protocoles de routage dynamique (exemples : OLSR, AODV…) rendent envisageable l'utilisation de réseaux maillés autonomes dans lesquels la portée ne se limite pas à ses voisins (tous les participants jouent le rôle du routeur). [6]

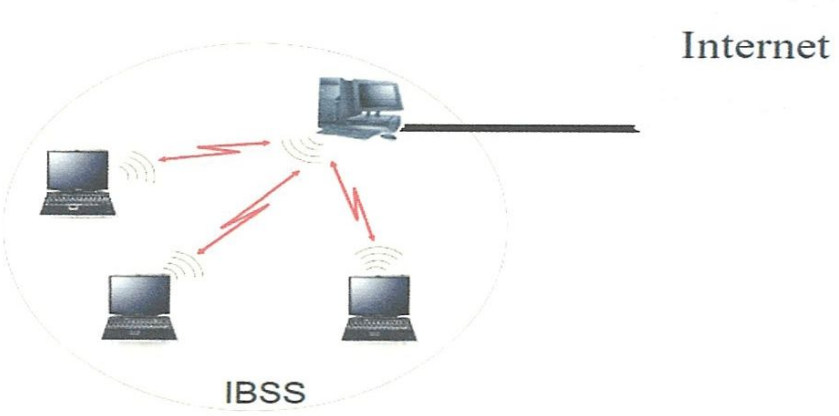

Figure I.3. : Mode ad-hoc avec accès internet IBSS (Independent Basic Service Set).

Voici les principaux avantages et inconvénients à déployer un réseau sans fil WiFi :

Avantages

- Mobilité : les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.
- Facilité et souplesse : un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- Coût : si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.
- Évolutivité : les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins.

Inconvénients

- Qualité et continuité du signal : ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- Sécurité : la sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice.

I.2.3. Bandes de fréquence du réseau Wifi

Les technologies utilisées pour les réseaux WPAN et les WLAN, fonctionnent sur deux bandes : les bandes ISM (Industrial Scientific Medical) (de 2400 à 2500 MHz) et la bande U-NII (Ulicensed-National Information Infrastructure) (de 5150 à 5720 MHz)

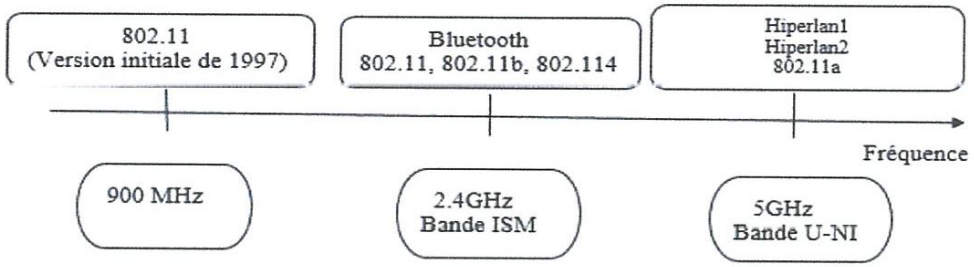

Figure I.4 : Bande de fréquence et canaux Wifi. [8]

I.2.3.1. Bande ISM

La bande ISM correspond à trois sous bandes (902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz) seule la bande de 2.400-2.4835 GHz avec une bande passante de 83.5 MHZ est utilisée par la norme 802.11. La largeur de bande ISM (le maximum est de 83.5 MHz) est suivant les pays, de même que la puissance utilisable (en France, elle est de l'ordre 10mW en intérieur et 2.5 mW en extérieur). Par ailleurs cette bande, plus précisément la sous bande 2.400-2.4835 GHz, est fortement utilisée par différents standards et perturbée par des appareils (four en microonde, clavier et souris sans fil, …) fonctionnant dans ces fréquences. Le tableau ci-dessous résume les canaux et fréquences utilisés dans cette bande ;

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2..432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

Tableau I.2 : Répartition des canaux de la bande ISM

Les canaux emploient réellement 22 MHz de largeur de bande de signal, ainsi des canaux adjacents devront être séparés par au moins cinq canaux pour éviter tout risque de chevauchement. Par exemple, les canaux 1,6 et 11 non aucun chevauchement.

On peut utiliser seulement trois canaux pour couvrir un domaine infiniment grand, sans chevauchement entre canaux.

I.2.3.2. Bande U-NII

La bande U-NII (5.15- 5.35 GHz, 5.725-5.825 GHz) offre une bande passante totale de 300 MHz, chacune utilisant une puissance de signal différente. Le tableau ci-dessous illustre les fréquences centrales des canaux utilisés.

Fréquence	Numéro du canal	Fréquence transmise (GHz)	Puissance maximale transmise (mW)
U-NII bande base	36	5.18	40
40		5.200	
44		5.220	
48		5.240	
U-NII bande moyenne	52	5.260	200
56		5.280	
60		5.300	
64		5.320	
U-NII bande haute	149	5.725	800
153		5.765	
157		5.785	
161		5.805	

Tableau I.3 : Canaux utilisés dans la bande U-NII.

Un des avantages de cette bande consiste à remédier aux problèmes d'interférence rencontrés dans la bande ISM, en utilisant une bande de fréquence moins utilisée par d'autres appareils. [8]

Conclusion

Ce premier chapitre se base surtout sur la présentation, l'évolution des réseaux GSM et Wifi, les normes et ainsi que l'architecture bien détaillée de chacune de ses deux technologies. Il entame le second chapitre qui parlera de la question de sécurité des données en insistant sur les failles et les insécurités liées au piratage informatique survenant lors de la transmission des données.

Chapitre II

Sécurité des données

Introduction

La première fonction d'un système d'information est de stocker et de permettre l'échange de données. La sécurisation d'un système d'information consiste donc à réduire le risque que les données soient compromises ou qu'elles ne puissent plus être échangées. En outre ; si un système informatique contrôle, par exemple, des équipements industriels ou le trafic aérien, alors on peut imaginer toutes sortes de catastrophes bien pires que quelques données compromises.

La question de la sécurité est sans doute la première que se pose une société lorsqu'elle se penche sur le Wifi. Si l'on communique à travers les ondes, tout le monde peut capter les communications. Face à cette crainte, de nombreux dirigeants d'entreprise ont eu un réflexe de prudence : attendre quelque mois ou quelques années pour bénéficier du retour d'expérience d'autres entreprises. Cependant il existe des solutions très robustes pour rendre un réseau sans fil tout aussi sécurisé qu'un réseau filaire.

Quant au système GSM, il est pleinement numérique et est maintenant opérationnel et largement utilisé. On remarque une importante croissance du marché de la communication mobile et de la nécessité de sécuriser le système.

La confidentialité et la sécurité sont fragilisées par l'utilisation du canal radio pour transporter les informations. Les abonnés mobiles sont particulièrement vulnérable à la possibilité d'utilisation frauduleuse de leur compte par des personnes ayant substituées l'identité d'abonnés autorisés et à la possibilité d'avoir leurs communications écoutées lors de l'appel.

Dans ce chapitre nous commencerons par définir ce qu'est la sécurité, la généralité sur la cryptographie et nous donnerons les différentes solutions de sécurité existantes.

Sécurité

Sécuriser un réseau consiste donc à prendre en compte tous les risques possibles, tels que les attaques volontaires, les accidents, les défauts logiciels ou matériels ou encore les erreurs humaines et à les réduire autant que possible. [8]

Cependant, sécuriser un message revient à le **crypter** (ou **chiffrer)** afin de le rendre compréhensible qu'à ceux qui connaissent le code.

II.1. Généralités sur la Cryptographie et le Chiffrement

II.1.1. Définition de la Cryptographie

La **cryptographie** est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu.

Alors que la cryptographie est la science de la sécurisation des données, la *cryptanalyse* est la science de l'analyse et du cassage des communications sécurisées. La cryptanalyse classique mêle une intéressante combinaison de raisonnement analytique, d'application d'outils mathématiques, de découverte de redondances, de patience, de détermination, et de chance. Les cryptanalystes sont aussi appelés attaquants.

La cryptologie embrasse à la fois la cryptographie et la cryptanalyse.

II.1.2. Objectifs visés par la Cryptographie

La cryptographie apporte un certain nombre de fonctionnalités permettant de renforcer le niveau de sécurité d'un S.I en palliant à certains types de menaces. En effet, elle consolide les objectifs de sécurité décrits dans le chapitre précédent (Intégrité, confidentialité, Authentification et non –répudiation). Donc, la cryptographie est inévitable pour la sécurité de tout S.I.

- ✓ **Pour assurer la confidentialité** : l'utilisation d'un algorithme de chiffrement permet d'empêcher l'accès aux messages transmis par les non autorisés. Ils peuvent lire les messages transmis sur le canal mais ne peuvent pas le déchiffrer. Donc, il permet de s'assurer que les données concernées ne peuvent être dévoilées qu'aux personnes concernées.
- ✓ **Contre l'usurpation d'identité** : utilisation d'algorithme d'authentification. Il s'agit que **A** s'identifier à **B** en prouvant qu'elle connaît un secret **S**, comme par exemple un mot de passe. Elle permet de prouver l'origine ou l'identité d'une entité (personne).
- ✓ **Contre l'altération de données** (préserve l'intégrité): Utilisation d'algorithme de contrôle d'intégrité. De tels algorithmes permettent de vérifier que le message n'a pas subi d'altération lors de son parcours. Donc elle garantit que les données ne peuvent êtres altérées (intentionnellement ou non) durant leur transmission ou leur stockage.
- ✓ **Contre la répudiation (Signature proprement dite)**: utilisation d'algorithmes de signatures. Permet à une personne de prendre part à un contrat avec impossibilité de renier par la suite ses engagements.

II.1.3. Principes de la Cryptographie

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

La cryptologie est essentiellement basée sur l'arithmétique : Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour :

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé **cryptogramme** (en anglais ***ciphertext***) par opposition au message initial, appelé message en **clair** (en anglais ***plaintext***) ;
- faire en sorte que le destinataire saura les déchiffrer.

Le fait de coder un message de telle façon à le rendre secret s'appelle ***chiffrement***. La méthode inverse, consistant à retrouver le message original, est appelée ***déchiffrement***.

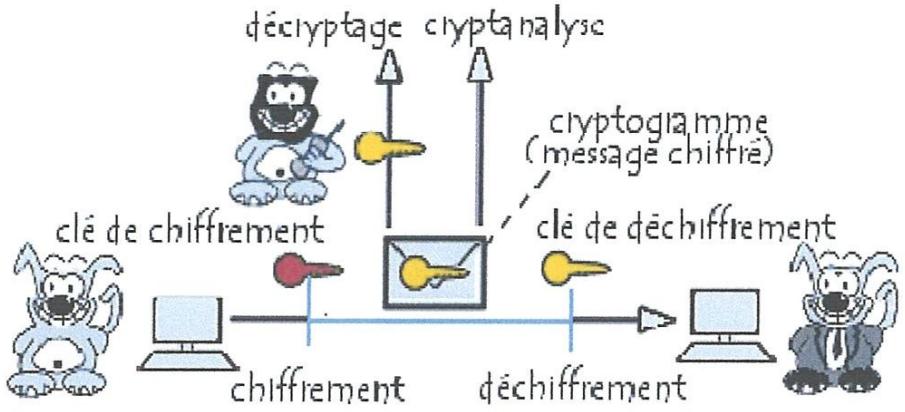

Figure II.1: principe de la Cryptographie

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs :

- **Les clés symétriques**: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.

- **Les clés asymétriques**: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

On appelle décryptement (le terme de décryptage peut éventuellement être utilisé également) le fait d'essayer de déchiffrer illégitimement le message (que la clé de déchiffrement soit connue ou non de l'attaquant). Lorsque la clef de déchiffrement n'est pas connue de l'attaquant on parle alors de **cryptanalyse** ou **cryptoanalyse** (on entend souvent aussi le terme plus familier de ***cassage***).

La **cryptologie** est la science qui étudie les aspects scientifiques de ces techniques, c'est-à-dire qu'elle englobe la cryptographie et la cryptanalyse.

II.1.4. Cryptanalyse

On appelle **cryptanalyse** la reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques. Ainsi, tout cryptosystème doit nécessairement être résistant aux méthodes de cryptanalyse. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un cryptosystème, on dit alors que l'algorithme de chiffrement a été « cassé ».

On distingue habituellement quatre méthodes de cryptanalyse :

- Une **attaque sur texte chiffré seulement :** Le cryptanalyste n'a, à sa disposition, pour retrouver la clef de déchiffrement, qu'un nombre fini de textes chiffrés. Cette attaque consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés.
- Une **attaque sur texte clair connu :** Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant. Le cryptanalyste s'efforce de reconstituer la clef à partir de couples (clairs, chiffrés) correspondants.
- Une **attaque sur texte clair choisi**: Le cryptanalyste est capable de produire le cryptogramme correspondant au texte clair de son choix.
- Une **attaque sur texte chiffré choisi:** Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés. Le cryptanalyste est capable de produire le texte clair correspondant au texte chiffré de son choix.

II.1.5. Domaines d'application de la Cryptographie

On constate que depuis ces dix dernières années, la cryptographie entre dans nos vies de tous les jours par l'intermédiaire du courrier électronique (pour protéger ses informations les plus personnelles), payement électronique (par carte de crédit), et de l'Internet en général (jeux

virtuels, commerce électronique, et de plus en plus de nouvelles applications (Services Web) liées aux nouvelles technologies numériques et au traitement automatisé massif de l'information...). Voici une liste non exhaustive des principaux domaines d'utilisation des moyens de chiffrement témoignant des enjeux importants du chiffrement dans le monde :

- Liaisons satellites,
- Réseaux ATM et GSM,
- Protection contre le piratage et l'espionnage,
- Paiement par carte bancaire,
- Commerce électronique,
- Certification (preuve) de documents électroniques (GED, EDI),
- Sécurisation d'échanges confidentiels (secret médical, secret juridique, ...),
- Authentification lors d'accès à des ordinateurs sensibles (centrale nucléaire, ...).

Protéger les informations importantes d'une entreprise devient de plus en plus essentiel pour maintenir un niveau de compétitivité suffisant. Le vol ou la destruction/endommagement de données confidentielles ou importantes (**hacking, espionnage industriel**), entraîne pour une entreprise des dommages financiers très coûteux, c'est pourquoi elles se doivent de se protéger, et utiliser des méthodes de chiffrement efficaces qui ne pourront pas être trop facilement brisés par des esprits malveillants. Cette idée peut être illustrée par les exemples suivants :

- **Industrie** : La copie de fichiers qui a permis à une entreprise de connaître des informations confidentielles à propos des principaux fournisseurs de son principal concurrent, et de ses stratégies marketing (prix de ventes, coûts...), de façon à lui permettre de suggérer des offres plus intéressantes que tous ses concurrents : estimation de la perte à 1,5 million de francs.
- **Banque de France** : destruction logique de quelques fichiers importants. Estimation de la perte à 100 millions de francs.
- **Services** : une modification d'un programme a permis de falsifier un report et de réaliser des opérations frauduleuses. Estimation de la perte : 20 millions de francs

II.1.6. Différents types de cryptage

On peut regrouper les systèmes de chiffrement en deux catégories:

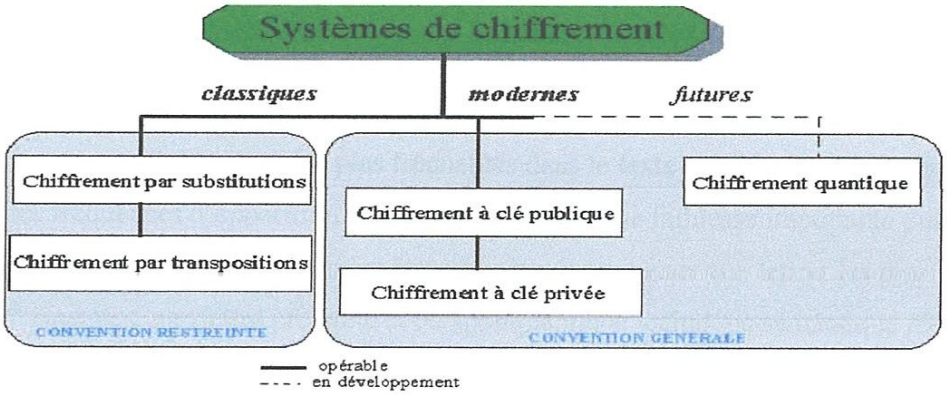

Figure II.2 : Système de chiffrement

II.1.6.1. Le chiffrement classique

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

II.1.6.1.a. Substitution

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

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer,

- le nombre d'alphabets utilisés dans le cryptogramme,

- la manière spécifique dont ils sont utilisés.

On distingue couramment quatre types de substitutions différentes :

- **Substitution homophonique** : comme pour le principe précédent, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré. Par exemple, " A " peut correspondre à 5, 13, 25 ou 56 ; " B " 7, 19, 31, ou 42 ; etc. Ce procédé est plus sûr , mais aussi craqué par les cryptanalystes ou des espions expérimentés.

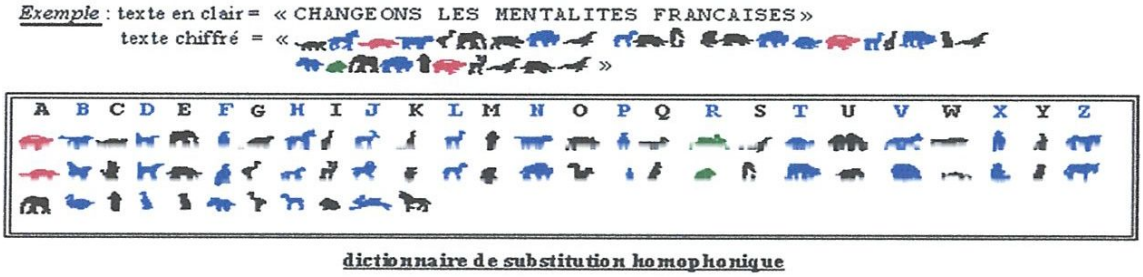

Figure II.6 : Un Exemple de Substitution Homophonique

- **Substitution polyalphabétique** : le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions monoalphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille polyalphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille polyalphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de départ). L'exemple le plus célèbre est l'algorithme de **VIGENERE** et de BEAUFORT. L'illustration la plus simple qui corresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

Exemple

Texte clair : j'adore écouter la radio toute la journée

Clé : MUSIQUE (à répéter autant de fois pour atteindre la taille du texte clair)

Texte en clair : j'adore ecouter la radio toute la journee

Clé répétée : M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU

Le texte chiffré est alors :

V'UVWHY IOIMBUL PM LSLYI XAOLM BU NAOJVUY

Clé Utilisée \ Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Lettre chiffrée

Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tableau II.1: Table de chiffrement de Vigenere

Exemple : texte en clair = « ABCBACCBA ACBB »
clé = « DBBCBAACD »

K \ C	ABCD
A	CBDA
B	DCAB
C	CABD
D	BDAC

texte chiffré = « BCAAD DDABB ACA »

Tableau II.2 : Table de Chiffrement Poly-Alphabétique Aléatoire

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

On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. La variante anglaise consiste à garder le W et à fusionner I et J.

Tableau II.3. : Chiffrement Playfair

Méthode de chiffrement

On chiffre le texte par groupes de deux lettres (des **bigrammes**) en appliquant les règles suivantes:

1. Si les deux lettres sont sur les coins d'un rectangle, alors les lettres chiffrées sont sur les deux autres coins. Exemple **OK** devient **VA**, **BI** devient **DC**, **GO** devient **YV**. La première des deux lettres chiffrées est sur la même ligne que la première lettre claire.

2. Si deux lettres sont sur la même ligne, on prend les deux lettres qui les suivent immédiatement à leur droite: **FJ** sera remplacé par **US**, **VE** par **EC**.

3. Si deux lettres sont sur la même colonne, on prend les deux lettres qui les suivent immédiatement en dessous: **BJ** sera remplacé par **JL**, **RM** par **ID**.

II.1.6.1.b. Cryptage par transposition

Les méthodes de chiffrement par transposition consistent à réarranger les données à chiffrer de façon à les rendre incompréhensibles. Les lettres se retrouvent mélangées (elles conservent leur identité, un E reste un E, mais changent de position)

Une illustration simple (de ce qu'on appelle d'ailleurs la **transposition simple à tableau**, procédé le plus utilisé) consisterait à écrire un texte ligne par ligne dans un tableau à 10 colonnes puis à transmettre le message par colonne. Prenons comme exemple le message :

"CE MESSAGE EST UNE ILLUSTRATION SIMPLE DU PROCEDE DE TRANSPOSITION"

Ecrivons ce message dans le tableau à 10 colonnes, en supprimant les espaces et la ponctuation (ici inexistante) :

C	E	M	E	S	S	A	G	E	E
S	T	U	N	E	I	L	L	U	S
T	R	A	T	I	O	N	S	I	M
P	L	E	D	U	P	R	O	C	E
D	E	D	E	T	R	A	N	S	P
O	S	I	T	I	O	N			

Tableau II.4. : Cryptage par transposition.

L'émetteur émet le message par colonne; cela donne la suite de caractère suivante:

CSTPDOETRLESMUAEDIENTDETSEIUTISIOPROALNRANGLSONEUICSESMEP

Il ne reste plus au destinataire qu'à déchiffrer.

Il sait que le tableau à 10 colonnes. Il va donc reconstituer le tableau mais pour cela il faut d'abord qu'il trouve le nombre de lignes. Cela ne présente guère de difficulté à celui qui sait qu'il s'agit d'un tableau de 10 colonnes; il lui suffit de diviser le nombre de caractères par 10 : comme il a reçu 57 caractères, il en déduit qu'il y a 5 lignes de 10 caractères et 1 ligne incomplète de 7 caractères. Il va donc considérer 7 groupes de 6 caractères puis 3 groupes de 5 qu'il va ranger dans son tableau.

La connaissance de la langue lui permettra simplement ensuite de replacer les espaces et la ponctuation.

D'un point de vue pratique, il conviendrait d'ajouter le "conditionnement" du message permettant par exemple d'identifier l'émetteur ou d'identifier la ou les clefs de transposition car, fréquemment, plusieurs grilles sont en service en même temps.

On peut augmenter la sécurité des messages en "améliorant" (par exemple en insérant des "nulles" dans le message - lettres inutiles - suivant une convention connue du déchiffreur …) la transposition simple ou en réalisant des transpositions successives (avec le même tableau ou un autre tableau).

Il s'agit par exemple de réordonner géométriquement les données pour les rendre visuellement inexploitables. Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des **permutations**. Plusieurs types différents de transpositions existent.

- **Transposition simple par colonnes**

On écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement. Le destinataire légal pour décrypter le message réalise le procédé inverse. L'algorithme allemand ADFGFX est fondé sur ce principe et fut utilisé pendant la première guerre mondiale. Il fut cassé par une jeune étudiante française.

Exemple : texte à chiffer = «I LOVE MY ENGLISH TEACHER»
utilise une matrice [6;4].

I	L	O	V
E	M	Y	E
N	G	L	I
S	H	T	E
A	C	H	E
R			

texte chiffré = « IENSA RLHGH COYLT HVEIE E »

Tableau II.5. : Transposition simple par colonnes

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

Exemple : texte en clair = «I LOVE MY ENGLISH TEACHER»
utilise le mot clé **SERGIO.**

Clé : S E R G I O
6 1 5 2 3 4

I	L	O	V	E	M
Y	E	N	G	L	I
S	H	T	E	A	C
H	E	R			

texte chiffré = « LEHEV GEELA MICON TRIYS H »

Tableau II.6. : Transposition complexe par colonnes

Exemple : texte clair= « FATOU MADINA ETUDIANTES »

Clé : **GUELMA**

Clé : G U E L M A
3 6 2 4 5 1

F	A	T	O	U	M
A	D	I	N	A	E
T	U	D	I	A	N
T	E	S			

Tableau II.7. : Transposition complexe par colonnes

Texte chiffré : « MEN TIDS FATT ONI UAA ADUE »

- **Transposition par carré polybique** : Fait à partir d'un carré de Polybe (Historien grec du II ème siècle av. J.C.), contenant toutes les lettres dans un ordre précis et pouvant être repérées

chacune par deux coordonnées (on peut utiliser un mot clé précis pour faire ce carré, l'écrire dans la première ligne puis compléter le tableau avec les lettres manquantes dans l'ordre alphabétique). On écrit d'abord la première coordonnée de chaque lettre du message puis après à la suite la deuxième coordonnée de chaque lettre, et enfin on réunit par paire chaque coordonnée pour les transposer en une lettre grâce au tableau. (Par exemple la première lettre du message codé se trouve être la lettre ayant pour première coordonnée, la première coordonnée de la première lettre et pour deuxième coordonnée, la première coordonnée de la deuxième lettre). Un mot clé secret est utilisé pour construire un alphabet dans un tableau. Les coordonnées des lignes et des colonnes correspondant aux lettres du texte à chiffrer sont utilisées pour transcrire le message en chiffres. Avec ce procédé chaque lettre du texte en clair est représentée par deux chiffres écrits verticalement. Ces deux coordonnées sont ensuite transposées en les recombinants par deux sur la ligne ainsi obtenue.

Exemple détaillé

	1	2	3	4	5
1	**S**	**T**	**E**	**P**	**H**
2	A	B	C	D	F
3	G	I	J	K	L
4	M	N	O	Q	R
5	U	V	W	X	Y
6	Z	.	;	,	!

	M	**A**	**T**	**H**	**E**	**M**	**A**	**T**	**I**	**Q**	**U**	**E**	**S**
1 ère coordonnée	4	2	1	1	1	4	2	1	3	4	5	1	1
2 ème coordonnée	1	1	2	5	3	1	1	2	2	4	1	3	1

Ce qui nous donne : 42 11 14 21 34 51 11 12 53 11 22 41 31

1 ère coordonnée	4	1	1	2	3	5	1	1	5	1	2	4	3
2 ème coordonnée	2	1	4	1	4	1	1	2	3	1	2	1	1
	N	S	P	A	K	U	S	T	W	S	B	M	G

On obtient au final : NSPAKUSTWSBMG

Tableau II.8. : Transposition par carré polybique

Il est important de faire remarquer que les transpositions sont plus contraignantes que les substitutions, car elles ont besoin de plus de mémoire et ne fonctionnent que sur des messages à chiffrer d'une longueur limitée ; c'est pourquoi elles sont moins utilisées dans les algorithmes bien que pourtant un peu plus sûres que les substitutions.

II.1.6.2. La Cryptographie Moderne

Avec le développement de l'informatique et l'accroissement de la puissance des ordinateurs, les méthodes de cryptanalyse sont devenues de plus en plus praticables et les messages sont devenus vulnérable au déchiffrement. Les masses d'informations échangées et leurs importances (Données stratégiques, informations opérationnelles, guides et procédés industriels et militaires…etc.) ont donné naissance à de nouvelles techniques pour dissimuler (cacher) les informations. Une transition qualitative en matière de sécurité a été faite sur la base du principe de KERCKHOFFS qui stipule que ***pour qu'une méthode de chiffrement soit efficace, il faut que son algorithme soit divulgué à tout le monde***. Des méthodes de chiffrement à clé public sont, alors apparues.

- **Les limites de la Cryptologie Classique**

Il faut constater que la première limite des algorithmes cryptographique classiques est la **distribution *sécurisé de la clé elle-même***. On parle de système à clé secrète.

Les problèmes de cette technologie sont les suivants :

- si la clé secrète est compromise (volée, extorquée, piratée, ...) par un opposant, alors ce dernier pourra déchiffrer tous les messages encodés avec celle-ci. Un pirate peut même se faire passer pour un émetteur légitime (usurpation d'identité de la victime).
- les clés doivent être distribuées secrètement : c'est très difficile à l'échelle planétaire (se rencontrer, utiliser un messager sûr, etc...).
- si une clé différente est utilisée pour chaque paire différente d'utilisateurs du réseau, le nombre total des clés augmente très rapidement en fonction du nombre total d'utilisateurs. La gestion du nombre de clés devient de plus en plus gênant avec l'augmentation du nombre destinataires, comme illustré dans la **Figure II.7** (2 personnes →2 clés ; 3→3, 4→6, ….30→435 ?).

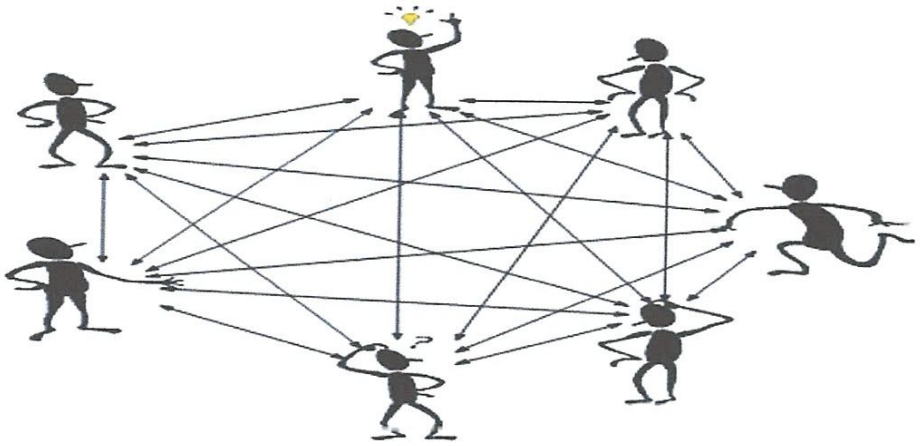

Figure II.7 : Les limites de la Cryptographie Symétrique

Le chiffrement et le déchiffrement des données sont effectués par des algorithmes cryptographiques. Ces algorithmes reposent généralement sur les problèmes mathématiques complexes, difficiles à résoudre, tels que la factorisation des nombres premiers, les logarithmes discrets, etc.

Les algorithmes cryptographiques modernes nécessitent une clé pour le chiffrement et une clé pour le déchiffrement. Il existe deux grands types d'algorithmes cryptographiques, ceux dits à clé secrète et ceux dits à clé publique :

- Algorithme cryptographique à clé secrète, ou symétrique. Les clés de chiffrement et de déchiffrement sont identiques. La sécurité repose sur la non divulgation des clés et sur la résistance des algorithmes aux attaques de cryptanalyse. Les plus connu sont : DES, IDEA, RC2, RC4 et AES

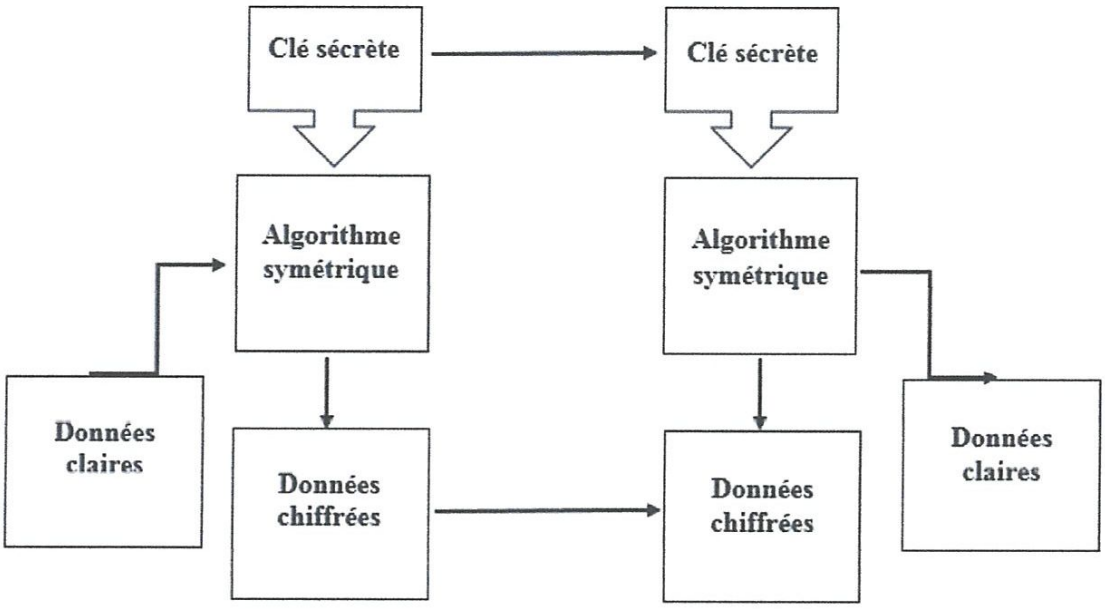

Figure II.8: Le chiffrement Symétrique (à clé Privée)

- Algorithme cryptographique à clé publique ou asymétrique. Les clés pour le chiffrement et le déchiffrement sont différentes. La sécurité repose sur le fait que le temps nécessaire pour déduire les clés secrètes associées aux clés publiques est théoriquement non raisonnable. Les plus connus sont : RSA (Rivest Shamir Adleman), les courbes elliptiques, Pohlig-Hellman, Rabin et ElGamal.

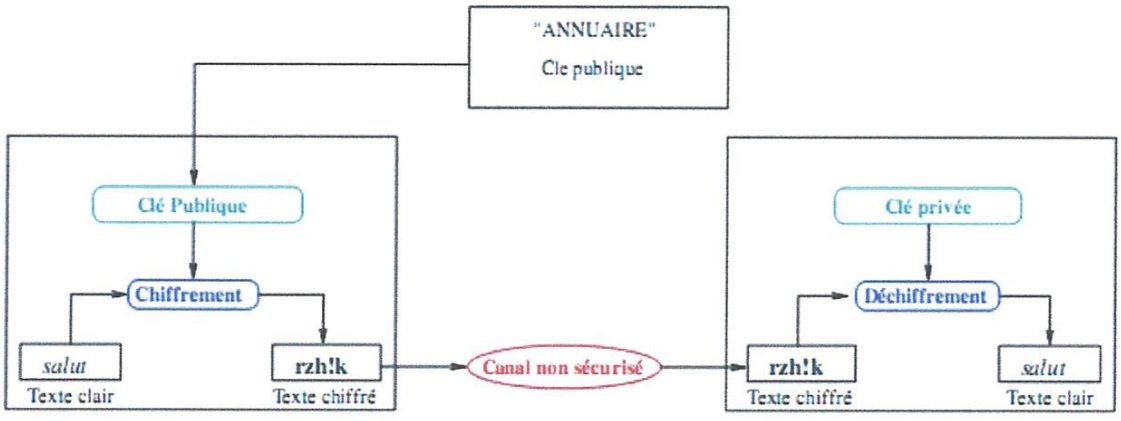

Figure II.9 : Le chiffrement Asymétrique (à clé Publique)

Les algorithmes sont beaucoup plus rapides que les algorithmes asymétriques dans des conditions identiques de test. Il ne faut pas en conclure que les algorithmes symétriques soient plus ou moins sécurisés que les algorithmes asymétriques. Ils sont simplement destinés à des usages différents. [9]

Note Bien

Parce que la cryptographie conventionnelle était autrefois le seul moyen disponible pour transmettre des informations secrètes, le coût des canaux sûrs et de la distribution des clés réservait son utilisation uniquement à ceux qui pouvaient se l'offrir, comme les gouvernements et les grandes banques. Le chiffrement à clé publique est la révolution technologique qui permet aux masses d'accéder à la cryptographie forte.

Le cryptage moderne offre 3 types de garanties

- Authenticité : permet d'assurer au destinataire d'un message crypté que son émetteur est bien celui qu'il prétend être.
- Confidentialité : permet d'assurer à l'émetteur du message crypté que son destinataire sera seul à pouvoir le lire.
- Intégrité : permet d'assurer que le contenu du message n'a subi aucune altération entre son envoi et sa réception

Il est ainsi possible, par exemple dans le cas d'un mail crypté, d'authentifier avec certitude l'auteur du message, d'assurer que le message n'a pu être lu par un tiers, et finalement que le message lu est précisément celui qui a été envoyé. Un autre exemple est le paiement en ligne.

II.1.6.3. Chiffrement mixte

Les algorithmes à clé publique sont assez lents. La méthode généralement utilisée pour envoyer un message, est de tirer au hasard une clé secrète, chiffrer le message avec un algorithme à clé privée en utilisant cette clé, puis chiffrer cette clé aléatoire elle-même avec la clé publique du destinataire. Ceci permet d'avoir la sécurité des systèmes à clé publique, avec la performance des systèmes à clé privée. Il existe un logiciel qui effectue toutes ces opérations et de manière transparente, et qui, de plus, est gratuit et téléchargeable à partir de dizaines de sites de par le monde : le célèbre **PGP** de **Phil Zimmermann**. (Il y a d'autres logiciels aussi performants, mais PGP est sûrement le plus connu.). Correctement utilisé, il est

sûr, même contre les meilleurs cryptanalystes du monde (c'est d'ailleurs pour cette raison que son utilisation est formellement interdite en France).

II.1.6.4. Chiffrement du futur

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

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

La cryptographie quantique est née au début des années 70. Elle repose sur le principe d'incertitude d'Heisenberg, selon lequel la mesure d'un système quantique perturbe ce système. Une oreille indiscrète sur un canal de transmission quantique engendre des perturbations inévitables qui alertent les utilisateurs légitimes. Ainsi, il est possible de distribuer une clef secrète aléatoire à deux utilisateurs qui ne partagent initialement aucun secret, de façon sécurisée contre des espions même de puissance de calcul infinie. Une fois cette clef secrète établie, elle peut être utilisée avec un système cryptographique classique. La cryptographie quantique ne nécessite aucune hypothèse comme "P et NP sont distincts", ou "factoriser est difficile". On obtient ainsi des preuves de sécurité reposant uniquement sur la correction des principes quantiques.

Les systèmes quantiques sont toujours à un stade expérimental, cependant depuis 1992, ils ont quitté le stade de la Science-fiction depuis que Benett et Brassard, deux chercheurs américains ont construit un prototype fonctionnant sur une courte distance (un peu moins d'un kilomètre). Cette approche souffre aujourd'hui du désavantage que les transmissions quantiques sont très faibles et sont difficilement amplifiables par la route, et que la polarisation des photons posent encore des problèmes en raison de l'imperfection de l'appareil lui-même.

Seul le futur nous dira si cette nouvelle approche, un peu plus compliquée puisque reposant directement sur la physique quantique, remplacera les systèmes utilisés actuellement. Cependant, pour l'instant les réponses aux problèmes posés restent incertaines, ce qui permet encore de beaux jours aux DES, RSA et autres standards du chiffrement moderne. [19]

II.2. Assurer la confidentialité des connexions

La confidentialité des informations transitant sur un réseau ne peut être assurée que par le **chiffrement des données** avant leur émission. Le réseau ne peut garantir par lui-même la confidentialité des données si elles ne sont pas chiffrées par un quelconque processus. Le chiffrement a pour but de chiffrer toutes les données échangées entre le mobile et la BTS. Ainsi la communication est sécurisée.

Le chiffrement des données doit aussi avoir un sens. Il doit, par exemple, se référer à une politique de classification des informations au sein de l'entreprise. Une telle classification a pour objectif d'établir clairement des niveaux de confidentialité des données et de définir les moyens à mettre en œuvre ainsi les listes de diffusion. En s'appuyant sur cette politique de classification de l'information, le chiffrement applique aux données le niveau de confidentialité voulu au moyen d'algorithme cryptographique et des clés de chiffrement de longueur adéquate.

La confidentialité des connexions permet de se prémunir d'un grand nombre d'attaque, parmi lesquelles :

- Les attaques à l'aide de programme d'écoute, ou sniffer, qui permettent de reconstruire une transaction réseau de manière invisible pour les acteurs de la connexion.
- Les attaques par virus, dont l'objectif est de copier tout fichier à caractère confidentiel, notamment les documents contenant le mot confidentiel ou les fichiers contenant les mots de passe de connexion à distance, etc.
- Les attaques systèmes après divulgation de faiblesse de sécurité permettant d'obtenir des droits aux privilèges non autorisés.

Pour garantir une isolation des fonctions de sécurité d'un réseau, il est préférable de dédier le chiffrement des données à un équipement spécifique plutôt que d'ajouter une telle fonction à un routeur ou à un pare-feu. Le choix d'un protocole implémentant des fonctions de chiffrement doit tenir compte du type d'application qui sera utilisé ainsi que du besoin de sécurité désirée. [9]

Les principaux algorithmes de chiffrement symétrique sont recensés au tableau II.1

Algorithme	Description
DES (*Data Encryption Standard*), 1974	Conçu par IBM, ce système de chiffrement par bloc est fondé sur une clé de 56 bits. Longtemps, standard de chiffrement des communications gouvernementales non classées secrètes, il a été remplacé par AES. L'algorithme a été rendu public
IDEA (*International Data Encryption Algorithm*), 1990	Conçu par X. Lai et J. Massey, ce système de chiffrement par bloc s'appuie sur une clé de 128 bits. L'algorithme a été rendu public.
RC5 (*Rivest's Code 5*), 1995	Conçu par R. Rivest, ce système de chiffrement par bloc s'appuie sur une clé de longueur variable. L'algorithme a été rendu public.
AES (*Advanced Encryption Standard*), 2000	Conçu par J. Daemen et V. Rijmen, ce système de chiffrement par bloc s'appuie sur une clé de 128 à 256 bits. Il s'agit du standard de chiffrement pour les communications gouvernementales non classées secrètes. L'algorithme a été rendu public.
Série RC (Ron's *Code*) RC4	Cet algorithme a une longueur de clé variable (de 1 à 256 octets). Cependant à cause des lois d'exportation, la clé a souvent une longueur de 40 bits. La clé est utilisée pour initialiser une « table d'états » de 256

L'objectif actuel des protocoles d'échange de clés est de permettre à deux acteurs d'échanger en toute sécurité des clés de sessions valables pour une seule session ou pour un temps donné dans une session. Le chiffrement des informations s'effectue dans un second temps au moyen d'algorithme de chiffrement symétrique plus rapide que les algorithmes de chiffrement asymétrique.

II.3. Sécurité d'un réseau

II.3.1. Sécurité du GSM

L'introduction de la mobilité dans les réseaux GSM a nécessité la création de nouvelles fonctions par rapport aux réseaux fixes classiques. Le système doit pouvoir connaître à tout moment la localisation d'un abonné de façon plus ou moins précise. En effet, dans un réseau fixe, à un numéro correspond une adresse physique fixe (une prise de téléphone), alors que pour le réseau GSM, le numéro d'un terminal mobile est une adresse logique constante à laquelle il faut associer une adresse physique qui varie au gré des déplacements de l'usager du terminal. La gestion de cette itinérance nécessite la mise en œuvre d'une identification spécifique de l'utilisateur.

De plus, l'emploi d'un canal radio rend les communications vulnérables aux écoutes et aux utilisations frauduleuses. Le système GSM a donc recours aux procédés suivants :

- Authentification de chaque abonné avant de lui autoriser l'accès à un service
- Chiffrement (ou cryptage) des communications.

II.3.1.1. Objectifs de la sécurité du GSM:

Les aspects de sécurités lesquels sont nécessaires par la communication mobile sont :

- Confidentialité des données transmises entre le mobile et la VLR
- Confidentialité des données transmises entre le VLR et l'autre VLR ou HLR
- Authentification de l'abonné ou de la station mobile
- Authentification de la base de données laquelle le mobile est associé
- Confidentialité de la localisation de la station mobile ou de l'abonné

Les fonctions de sécurités du GSM ne concernent que la protection des réseaux contre les accès non autorisés et la confidentialité des abonnés. Le système intègre ainsi les fonctions suivantes :

- Authentification d'un abonné.
- Confidentialité de l'abonné.
- Confidentialité des données et des informations de signalisation transportées pour la liaison radio.

II.3.1.2. Structure du système de sécurité en GSM

Le système de sécurité en GSM est basé sur trois algorithmes de chiffrement (A3, A5 et A8) et trois clefs (triplet de sécurité).

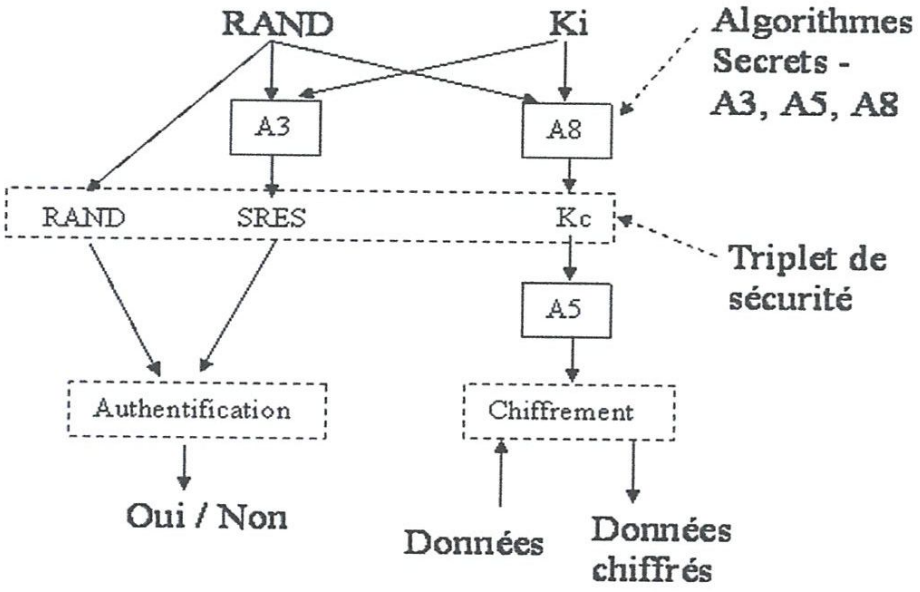

Figure II.10: Structure du système de sécurité du GSM

- Ki clef de l'utilisateur (fournie avec l'IMSI) inscrite dans le SIM
- RAND nombre aléatoire fournis par le réseau GSM
- A3 / A8 : algorithmes d'authentification – dans le SIM

Remarque : Ki, A3 et A8 sont inaccessibles.

- A8 : algorithme de chiffrement des données dans le mobile
- SRES: nombre obtenu quand les clefs RAND et Ki sont traités avec l'algorithme A3.
- Kc : nombre obtenu quand les clefs RAND et Ki sont traités avec l'algorithme A8.

Le triplet {RAND, SRES, Kc} – sont des nombres variables qui changent pour chaque conversation. L'algorithme A5 et Kc sont utilisés pour chiffrer les données de l'utilisateur (ou la voix). RAND et SRES sont utilisés pour identifier l'utilisateur. [11]

II.3.1.3. Différentes procédures relatives à la sécurité du GSM

II.3.1.3.a. Authentification

L'authentification est l'attestation de l'identité revendiquée par une entité. Les entités incluent non seulement les utilisateurs humains, mais aussi les dispositifs, les services et les applications.

Cette procédure permet d'identifier l'abonné qui essaye d'accéder au réseau. La procédure n'identifie pas le téléphone portable. Un abonné peut utiliser différents téléphones.

L'authentification permet aussi d'attester qu'une entité ne tente pas d'usurper l'identité d'une autre entité ni de reprendre sans autorisation une communication précédente.

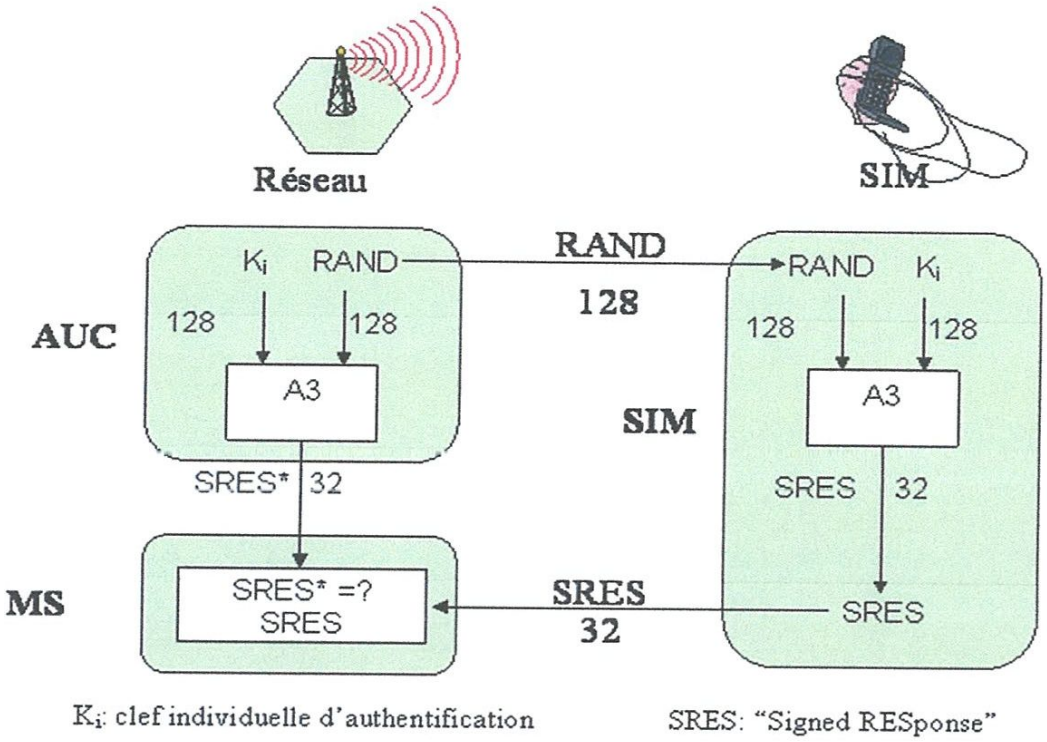

Figure II.11 : Authentification

Le réseau connaît Ki (et IMSI) de l'abonnée. Le réseau génère un nombre aléatoire RAND de 128 bits et l'envoie en clair au portable. Grâce au Ki, RAND et l'algorithme A3 le mobile et le réseau calculent deux nombres SRES (qui doivent être les mêmes) de 32 bits. Le mobile envoie son SRES et le réseau le compare avec son nombre SRES. Si les deux nombres coïncident l'utilisateur est identifié. RAND et SRES sont envoyés en clair. [11]

II.3.1.3.b. Chiffrement

Cette procédure a pour but de chiffrer toutes les données échangées entre le mobile et BTS. Ainsi la communication est sécurisée. L'utilisation ou non du chiffrement est décidé par le réseau. La clef de chiffrement Kc est générée par l'algorithme A8.

Grâce à Kc l'algorithme A5 produit une séquence de bits aléatoires Ai qui font une fonction OU EXCLUSIF (XOR) avec les données à chiffrer Di. Kc n'est jamais transmis sur l'interface radio. [11]

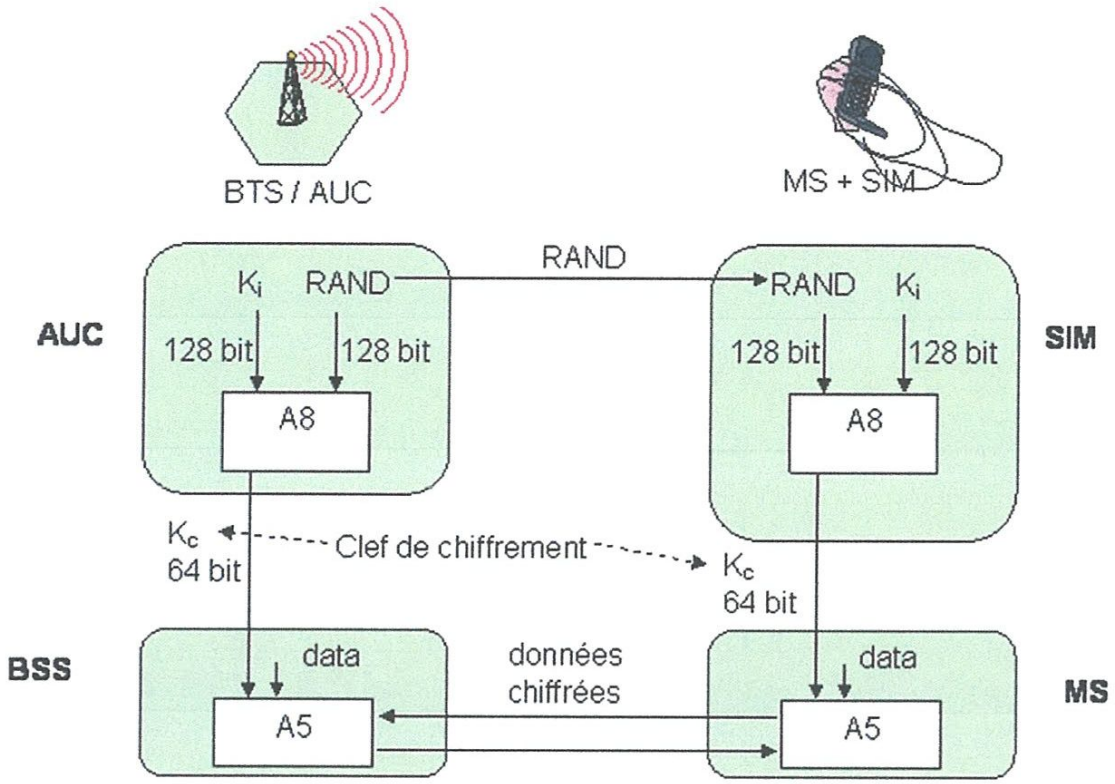

Figure I1.12 : Chiffrement de données entre le mobile et la BTS.

II.3.2 Sécurité du Wifi

Dans les réseaux sans fils, le support est partagé. Tout ce qui est transmis et envoyé peut donc être intercepté. Pour permettre aux réseaux sans fils d'avoir un trafic aussi sécurisé que les réseaux fixes, le groupe de travail 802.11 a mis au point certains protocoles de sécurité à savoir :

II.3.2.1. Le WEP (Wired Equivalent Privacy)

Pour remédier aux problèmes de confidentialité des échanges sur un réseau sans fil, le standard 802.11 intègre un mécanisme simple de chiffrement de données, le WEP. Ce cryptage travaille avec l'algorithme RC4 pour chiffrer les données et utilise des clés statiques de 64 ou 128 voire 152 bits suivant les constructeurs.

Le principe du WEP consiste à définir une clé sécrète qui doit être déclarée au niveau de chaque adaptateur sans fil du réseau ainsi que sur le point d'accès. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque élément du réseau voulant communiquer entre eux doit connaître la clé secrète qui va servir au cryptage

WEP. Une fois mis en place, toutes les données transmises sont obligatoirement cryptées. Il assure ainsi l'encryptage des données durant leur transfert ainsi que leurs intégrités.

Cependant, le WEP possède un grand nombre de failles, le rendant vulnérable. En effet, le cryptage RC4 présente des faiblesses. La clé de session partagée par toutes les stations est, nous le savons, statique. Cela signifie que pour déployer un grand nombre de stations Wifi, il est nécessaire de les configurer en utilisant la même clé de session ; ceci ayant pour conséquence que la connaissance de la clé est suffisant pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits. Dans le cas d'une clé de 40 bits, une attaque par force brute, c'est à dire essayer toutes les possibilités de clés, peut très vite amener le pirate à trouver la clé de session. Également, il existe différents logiciels, comme « WEPCrack » sous Linux ou « Aircrack » sous Windows, qui permettent de déchiffrer la clé en quelques minutes.

Concernant l'intégrité des données, le CRC32, implanté dans le WEP, comporte une faille permettant la modification de la chaîne de vérification du paquet à comparer à la chaîne finale issue des données reçues, ce qui permet à un pirate de faire passer ses informations pour des informations valides.
A noter également que l'utilisation du WEP réduit le débit de la connexion du fait du cryptage/décryptage des paquets.
Néanmoins, il s'agit d'une solution de sécurité existant dans tous les équipements Wifi, ce qui explique qu'il soit très utilisé par le grand public ainsi que par certaines entreprises.

Pour résumer, les différentes vulnérabilités du WEP sont :

- Contre la confidentialité du fait de la réutilisation de la suite chiffrée, de la faiblesse du RC4 et d'une possible fausse authentification.
- Contre l'intégrité du fait de la capacité à modifier les paquets et d'en injecter des faux.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données.

Pour autant, il sera indispensable de mettre en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum quant aux données de l'entreprise.

II.3.2.2. Le WPA (Wi-Fi Protected Access)

Le WPA, développé par l'IEEE, est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses.

En effet, le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (Temporal Key Integrity Protocol), dites dynamiques, et permet l'authentification des utilisateurs grâce au 802.1x, protocole mis au point par l'IEEE, et à l'EAP (Extensible Authentification Protocol).

Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP, lui, utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil, qui doit être compatible avec le WPA.

De plus, un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a modifiées.

Le TKIP rajoute par rapport aux clés WEP

- Vecteur d'initialisation de 48 bits au lieu de 24 bits pour le WEP. Le craquage de la clé WEP provient en effet du fait que le pirate peut déterminer la clé WEP à partir du vecteur d'initialisation de 24 bits. Donc, il sera bien plus difficile à déterminer la clé avec un vecteur d'initialisation de 48 bits.
- Génération et distribution des clés : le WPA génère et distribue les clés de cryptage de façon périodique à chaque client. En fait, chaque trame utilise une nouvelle clé, évitant ainsi d'utiliser une même clé WEP pendant des semaines voire des mois.
- Code d'intégrité du message : ce code, appelé MIC (Message Integrity Code), permet de vérifier l'intégrité de la trame. Le WEP utilise une valeur de vérification d'intégrité ICV (Integrity Check Value) de 4 octets, tandis que le WPA rajoute un MIC de 8 octets.

Mode d'authentification

- Le mode entreprise : il nécessite un serveur central qui répertorie les utilisateurs - par exemple un serveur RADIUS. Il faut pour cela un ordinateur exprès, ce qui coûte cher.
- Le mode personnel : il permet une méthode simplifiée d'authentification des utilisateurs sans utiliser un serveur central. Ce mode s'appelle également PSK (Pre-Shared Key). Il s'agit alors de saisir un mot de passe alphanumérique (« passphrase »).

Étant donné que l'entreprise ne possède pas de serveur type RADIUS, il sera nécessaire de choisir le second mode d'authentification, à savoir personnel.
Problèmes du WPA :

Quelques problèmes subsistent tout de même à ce protocole et notamment l'attaque de type « déni de service ».
En effet, si quelqu'un envoie au moins deux paquets chaque seconde utilisant une clé de cryptage incorrecte, alors le point d'accès sans fil « tuera » toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non-autorisés à un réseau protégé, mais cela peut bloquer tout un réseau sans fil.

Outre ce problème, il manquerait au WPA pour fournir une meilleure sécurité :

- Un SSID (Service Set IDentifier) sécurisé, c'est à dire une chaîne de caractères alphanumériques sécurisée permettant d'identifier un réseau sans fil
- Une déconnexion rapide et sécurisée
- Une dé-authentification et une dé-association sécurisées
- Un meilleur protocole de cryptage tel qu'AES (Advanced Encryption Standard)

II.3.2.3. Le WPA2 (Wi-Fi Protected Access 2)

Le 802.11i, nouvelle norme ratifiée en 2004, propose une solution de sécurisation poussée pour les réseaux sans fil Wifi. Il s'appuie sur l'algorithme du chiffrement TKIP, comme le WPA, mais supporte au contraire l'AES, au lieu du RC4, beaucoup plus sûr au niveau du cryptage des données. La Wifi Alliance a ainsi crée une nouvelle certification, baptisée WPA2, pour les matériels supportant le standard 802.11i.

Le WPA-2, tout comme son prédécesseur, le WPA, assure le cryptage ainsi que l'intégrité des données mais offre de nouvelles fonctionnalités de sécurité telles que le « Key Caching » et la « Pré-Authentification ».

Le Key Caching

Il permet à un utilisateur de conserver la clé PMK (Pairwise Master Key) - variante de PSK (Pre-Shared Key) du protocole WPA, lorsqu'une identification s'est terminée avec succès afin de pouvoir la réutiliser lors de ses prochaines transactions avec le même point d'accès. Cela signifie qu'un utilisateur mobile n'a besoin de s'identifier qu'une seule fois avec un point d'accès spécifique. En effet, celui-ci n'a plus qu'à conserver la clé PMK - ce qui est géré par le PMKID (Pairwise Master Key IDentifier) qui n'est autre qu'un hachage de la clé PMK, l'adresse MAC du point d'accès et du client mobile, et une chaîne de caractère. Ainsi, le PMKID identifie de façon unique la clé PMK.

La Pré-Authentification

Cette fonction permet à un utilisateur mobile de s'identifier avec un autre point d'accès sur lequel il risque de se connecter dans le futur. Ce processus est réalisé en redirigeant les trames d'authentification générées par le client envoyé au point d'accès actuel vers son futur point d'accès par l'intermédiaire du réseau filaire. Cependant, le fait qu'une station puisse se connecter à plusieurs points d'accès en même temps accroît de manière significative le temps de charge.
Pour résumer, le WPA-2 offre par rapport au WPA :

- Une sécurité et une mobilité plus efficaces grâce à l'authentification du client indépendamment du lieu où il se trouve.
- Une intégrité et une confidentialité fortes garanties par un mécanisme de distribution dynamique de clés.
- Une flexibilité grâce à une réauthentification rapide et sécurisée.

Toutefois, pour profiter du WPA-2, les entreprises devront avoir un équipement spécifique tel qu'une puce cryptographique dédiée pour les calculs exigés par l'AES.

II.3.2.4. Filtrage par adresse MAC (Medium Access Controler)

Le filtrage par adresse MAC est une fonctionnalité de sécurité que l'on trouve dans certains points d'accès. Il permet d'exclure ou de ne tolérer que certaines adresses MAC à accéder au réseau sans fil.

Une adresse MAC est en fait un identifiant unique pour chaque carte réseau. Ce système, qui permet donc de contrôler quelles cartes réseaux peuvent entrer sur le réseau, aurait permis une grande sécurité, malheureusement, le protocole 802.11b/g n'encrypte pas les trames où apparaissent ces adresses MAC.

En effet, un simple logiciel, comme « kismet » par exemple, permet de voir les adresses MAC des clients. De ce fait, comme il existe des outils ou des commandes pour modifier son adresse MAC et ainsi usurper celle d'un client, le réseau devient ainsi une vraie « passoire ».

Le filtrage par adresse MAC, associé au WEP ou WPA, ferai donc une bonne sécurité. Malheureusement, aucune sécurité n'est inviolable. [8]

Conclusion

Ce chapitre détaille la question de sécurité dans les réseaux GSM et Wifi. On a aussi décrit l'authentification, le chiffrement des données et ainsi qu'une généralité sur la cryptographie. Les différentes méthodes de sécurisation utilisées en GSM et en Wifi.

La sécurité des données téléphoniques (GSM) sont infaillibles comparés au réseau sans fil. Et concernant le Wifi, la meilleure sécurité depuis sa mise en place jusqu'à ce jour, est le WPA2, celui-ci s'appuie sur l'algorithme de chiffrement AES comparé au WEP car ce dernier est plus facile à craquer. Le tour des différents algorithmes de chiffrement seront fait dans le chapitre suivant.

Chapitre III

Algorithme de chiffrement

Introduction

Le cryptage est historiquement l'une des premières applications de l'informatique. Ce domaine, qui était il y a encore quelques années, réservé aux militaires et aux grandes entreprises, concerne aujourd'hui tous ceux qui souhaitent transmettre des données protégées, qu'ils soient professionnels ou particuliers. Pour cela, il existe de nombreuses méthodes de cryptage, mais peu d'entre elles sont reconnues comme sûres.

Si le but traditionnel de la cryptographie est d'élaborer des méthodes permettant de transmettre des données **de manière confidentielle**, la cryptographie moderne s'attaque en fait plus généralement **aux problèmes de sécurité des communications**. Le but est d'offrir un certain nombre de **services de sécurité** comme la confidentialité, l'intégrité, l'authentification des données transmises et l'authentification d'un tiers. Pour cela, on utilise un certains nombres de mécanismes basés sur ses algorithmes cryptographiques. Nous allons voir dans ce troisième chapitre quelles sont les techniques que la cryptographie fournit pour réaliser ces mécanismes.

III.1 Algorithme de chiffrement A5/1

A5/1 est l'algorithme de **chiffrement** à flot utilisé pour protéger la confidentialité des communications hertziennes pour les téléphones mobiles dans la norme GSM, c'est-à-dire pour protéger les échanges entre téléphone mobile et station de base. Il produit une suite pseudo-aléatoire avec laquelle on effectue un XOR avec les données. Une autre variante existe, l'A5/2. On trouve aussi le terme d'A5/3 (KASUMI), bien que ce dernier ne soit pas un algorithme de chiffrement par flot mais de bloc.

L'algorithme A5 utilise une clé de 64 bits mais son implémentation dans le GSM n'utilise que 54 bits effectifs (10 bits sont mis à zéro).

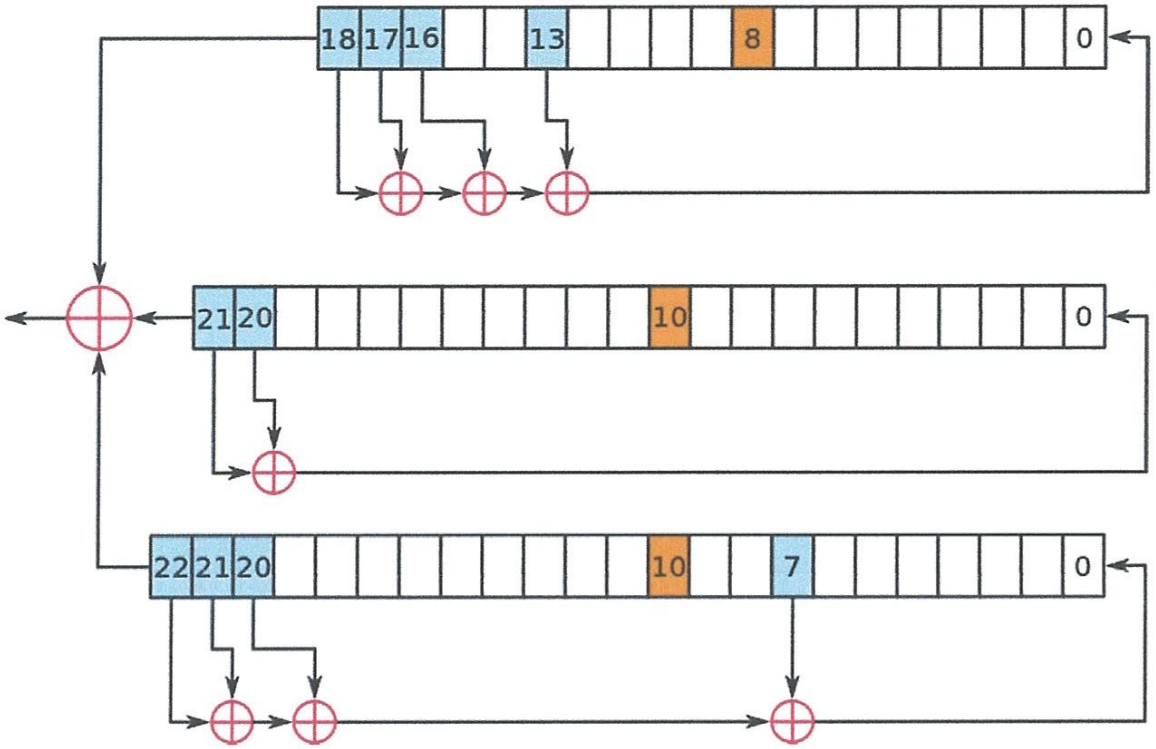

Figure III.1 : registre à décalage pour A5/1

III.1.1. Historique

La version A5/1 est utilisée en Europe. La version A5/2 est plus vulnérable mais utilisée sur d'autres marchés, notamment en Amérique du Nord. En 1994, l'architecture de l'A5/1, à l'origine secrète, est publiée. En 1999, les versions 1 et 2 sont complètement spécifiées après que l'ingénierie inverse effectuée par Marc Briceno à partir d'un téléphone GSM. En 2000, on comptait environ 130 millions d'utilisateurs du GSM basé sur A5/1.

III.1.2. Principe de fonctionnement

Une conversation GSM s'effectue par division en blocs temporels, chacun dure 4,6 millisecondes et contient 2×114 bits pour les deux canaux de communication (full-duplex). Une clé de session K est utilisée pour la communication. Pour chaque bloc, K est mélangée à un compteur de blocs et le résultat est utilisé comme état initial d'un générateur de nombres pseudo-aléatoires qui produit 228 bits. Ceux-ci servent au chiffrement après un XOR avec les données des deux canaux.

L'architecture de l'A5/1 est basée sur trois registres à décalage à rétroaction linéaire. Ils ont une longueur de 19, 22 et 23 bits. Pour insérer un nouveau bit dans le registre lors d'un décalage, on effectue pour chaque registre un XOR entre quelques bits déjà présents dans le registre. Les positions des bits utilisés sont constantes.

On récupère ensuite trois bits à des positions fixes, un par registre, avec lesquels on calcule une fonction « majorité » (le bit qui gagne est celui qui apparaît deux fois). Les deux registres ayant produit le bit qui a emporté la majorité sont alors décalés. La véritable sortie du générateur est un XOR entre les bits qui sont en tête de chaque registre.

Pour initialiser le système avec la clé de 64 bits et le compteur initial de 22 bits, on procède comme suit :

1. tous les registres sont mis à 0
2. on effectue 64 cycles pendant lesquels la clé de 64 bits est introduite dans le système
    a) pour le bit K_i de la clé, on effectue un XOR avec le bit de poids faible de chaque registre
    b) on décale tous les registres d'un cran
3. on effectue 22 cycles pendant lesquels le compteur de blocs (22 bits) est introduit dans le système
    a) pour le bit C_i du compteur, on effectue un XOR avec le bit de poids faible de chaque registre
    b) on décale tous les registres d'un cran

III.1.3. Sécurité

Plusieurs attaques ont été mises en évidence sur A5/1. Parmi ces cryptanalyses, on trouve par exemple des attaques par compromis temps-mémoire très rapides et qui nécessitent uniquement la connaissance de couples clairs-chiffrés correspondant à quelques secondes de conversation. Mais elles requièrent un temps de pré-calcul et une mémoire très élevés.

A5/1 est également vulnérable à des attaques par corrélation rapides qui exploitent notamment des faiblesses de la procédure d'initialisation. La plus récente, publiée en 2004 par Maximov, Johansson et Babbage peut être effectuée en moins d'une minute. Elle

nécessite la connaissance de quelques secondes de conversation, et ne requiert pas de pré calcul ou de mémoire trop importants.

III.1.4. Attaque utilisant l'implémentation de la norme GSM.

Certaines attaques sur A5/1 ont pour origine (ou sont grandement facilitées) par certaines propriétés du protocole de communication utilisé dans la norme GSM. Ainsi, sans mettre en cause la sécurité d'A5/1, une attaque très efficace a été proposée par Barkan, Biham et Keller : elle exploite les faiblesses du protocole qui détermine l'algorithme de **chiffrement** (A5/1 ou A5/2). Ainsi, il suffit pour l'attaquant de se faire passer pour la station de base et d'envoyer à un téléphone mobile l'instruction de chiffrer avec A5/2 pour pouvoir décrypter très facilement toutes ces communications sans avoir à attaquer A5/1.

Les mêmes auteurs ont également mis en évidence une autre erreur du protocole de communication GSM, qui ajoute au message clair des bits de redondance linéaire (destinés à corriger les erreurs de transmission) avant d'appliquer le **chiffrement**, alors que le fait de chiffrer avant d'utiliser un code correcteur d'erreur est un principe de sécurité élémentaire. L'existence de ces bits de redondance permet évidemment d'accélérer de façon significative les attaques sur A5/1 ; ils sont également utilisés dans l'attaque par corrélation rapide de Maximov, Johansson et Babbage. [12]

III.2. Algorithme de chiffrement DES (*Data Encryption Standard*)

III.2.1. Historique

Le 15 mai 1973 le **NBS** (*National Bureau of Standards*, aujourd'hui appelé *NIST - National Institute of Standards and Technology*) a lancé un appel dans le *Federal Register* (l'équivalent aux Etats-Unix du *Journal Officiel* en France) pour la création d'un algorithme de chiffrement répondant aux critères suivants :

- posséder un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement
- être compréhensible
- ne pas dépendre de la confidentialité de l'algorithme
- être adaptable et économique

- être efficace et exportable

Fin 1974, IBM propose « Lucifer », qui, grâce à la NSA (National Security Agency), est modifié le 23 novembre 1976 pour donner le **DES** (*Data Encryption Standard*). Le DES a finalement été approuvé en 1978 par le NBS. Le DES fut normalisé par l'*ANSI* (*American National Standard Institute*) sous le nom de *ANSI X3.92*, plus connu sous la dénomination *DEA* (*Data Encryption Algorithm*).

III.2.2. Principe du DES

C'est un algorithme à clé secrète, il chiffre un bloc de texte clair de 64 bits en utilisant une clé de 56 bits, pour obtenir un bloc de texte chiffré de 64 bits. Il utilise les deux grandes lois de Shannon : diffusion (en utilisant des permutations : transpositions) et confusion (en utilisant des substitutions) de bits pour casser la fréquence d'apparition des lettres dans le texte en clair, et compliquer le lien entre le fichier encodé et la clé secrète utilisée.
Les deux techniques de base pour gommer les redondances dans un texte sont selon Shannon : la **confusion et la diffusion**.
La confusion : Gomme les relations entre le texte en clair et le texte chiffré. Elle évite l'analyse du texte chiffré par recherche de redondances et de motifs statistiques. Le moyen le plus simple pour réaliser cela est la substitution.
Exemple : les tables de substitution du DES, chaque mot de 6 bits est remplacé par un seul mot de 4 bits pour une table.
La diffusion : Disperse la redondance du texte en clair en la répartissant dans le texte chiffré. Un cryptanalyste qui recherche ces redondances aura plus de difficultés à les trouver. Le moyen le plus simple de provoquer la diffusion est la transposition (appelée aussi permutation).

La clé est en fait constituée de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme (en code ASCII, cette clé est un mot de 8 caractère : 8x7=56). Les huit autres bits peuvent être utilisés pour la détection d'erreurs. Chacun des huit bits est utilisé comme bit de parité des sept groupes de 8 bits. Il repose sur 16 itérations imbriquées, et avec une clé suffisamment longue et pas trop simple (pas une succession de 1 par exemple), sa résistance aux différentes attaques possibles est bonne.

Il utilise les transformations de substitution et de transposition. Il y a donc pour le DES 2^{56} clés possibles, soit environ ... 72 millions de milliards possibilités.

Le niveau de sécurité de DES est raisonnable et il reste très utilisé dans le domaine commercial et des banques, et il est implanté dans de nombreuses cartes de crédits dédiés (smart cards, système électronique de communication). Son principal avantage est d'offrir une vitesse de chiffrement et déchiffrement élevée.

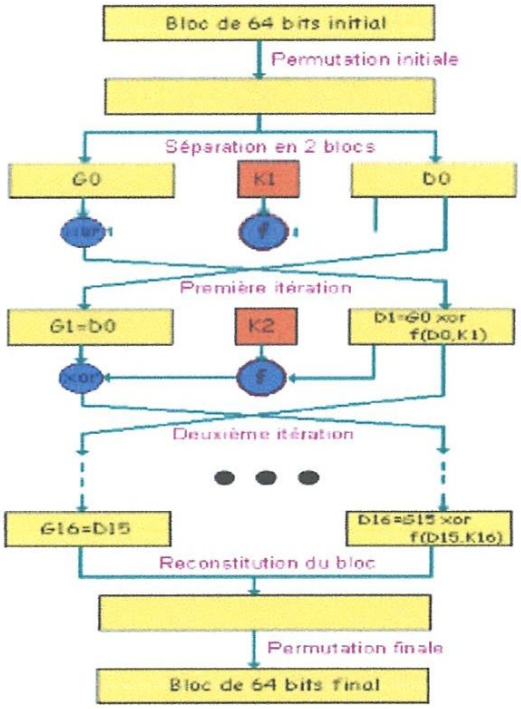

Figure III.2 : Principe du DES

- ✓ **Phase 1 : Préparation-Diversification de la clé.**

Le texte est découpé en blocs de 64 bits. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés K_1, …..K_{16} à 48 bits. Les K_i sont composés de 48 bits de K, pris dans un certain ordre.

- ✓ **Phase 2 : Permutation initiale**

Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie y=P(x), y est représenté sous la forme $y=G_0D_0$, G_0 étant les 32 bits à gauche de y, D_0 les 32 bits à droite.

✓ **Phase 3 : Itération**

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

$G_i=D_{i-1}$.

$D_{i-1}=G_{i-1}$ XOR $f(D_{i-1},K_i)$.

✓ **Phase 4 : Permutation finale**

On applique à $G_{16}D_{16}$ l'inverse de la permutation initiale.

$Z=P^{-1}(G_{16}D_{16})$ est le bloc de 64 bits chiffrés à partir de x.

L'entière sécurité de l'algorithme repose sur les clefs puisque l'algorithme est parfaitement connu de tous. La clef de 64 bits est utilisée pour générer 16 autres clefs de 48 bits chacune qu'on utilisera lors de chacune des 16 itérations du D.E.S. Ces clefs sont les mêmes quel que soit le bloc qu'on code dans un message.

En effet la sécurité du D.E.S. avec ses 16 rondes est grande et résiste à l'heure actuelle à toutes les attaques linéaires, différentielles ou par clefs corrélées, effectuées avec des moyens financiers et temporels raisonnables. La grande sécurité repose sur ses tables de substitutions non linéaires très efficaces pour diluer les informations. De plus le nombre de clefs est élevé ($2^{56}=7,2*10^{16}$) et peut être facilement augmenté en changeant le nombre de bits pris en compte. [18]

III.3. Algorithme de chiffrement AES *(Advanced Encryption Standard)*

Comme premièrement accessible au public, de la NSA pour le chiffrement avec le classement "top secret", l'Advanced Encryption Standard (AES) est l'un des algorithmes de cryptage aujourd'hui le plus fréquemment utilisé et le plus sécuritaire. Son histoire de succès a débuté en 1997, lorsque le NIST (National Institute of Standards and Technology) a annoncé la recherche pour un successeur au standard de cryptage vieillissant DES. Un algorithme, appelé "Rijndael", développé par les cryptographes belges Daemen et Rijmen, a excellé dans la sécurité aussi bien dans la performance et la flexibilité. Il est arrivé en tête de plusieurs

compétiteurs, et a été annoncé officiellement comme le nouveau standard de cryptage AES en 2001. Les algorithmes sont basés sur plusieurs substitutions, permutations et transformations linéaires, chacune réalisée sur des blocs de données de 16 octets, de là venant le terme **chiffrement par bloc**.

Ces opérations sont répétées plusieurs fois, appelées "rondes". Durant chaque ronde, une clé de ronde unique est calculée de la clé de **cryptage**, et incorporée dans les calculs. Basé sur cette structure de bloc de l'AES, le changement d'un seul bit soit dans la clé, ou soit dans le bloc de texte brut donne un bloc de texte de chiffrement complètement différent, un avantage clair sur les chiffrements de flux traditionnels. Finalement, la différence entre AES-128, AES-192 et AES-256, c'est la longueur de la clé : 128, 192 ou 256 bits, tous des améliorations drastiques comparées à la clé de 56 bits de DES. Voici un exemple . Le craquage d'une clé AES à 12 bits avec un super-ordinateur à la fine pointe de la technologie prendrait plus de temps que l'âge présumé de l'univers. Et Boxcryptor utilise même des clés à 256 bits! En date d'aujourd'hui, il n'existe pas d'attaque possible et pratique contre l'AES. Ainsi, l'AES demeure le standard de cryptage préféré pour les gouvernements, les banques et les systèmes de haute sécurité autour du monde.

III.3.1. Caractéristiques et points forts de l'AES

Le choix de cet algorithme répond à de nombreux critères plus généraux dont nous pouvons citer les suivants :

- sécurité ou l'effort requis pour une éventuelle cryptanalyse.
- facilité de calcul : cela entraine une grande rapidité de traitement
- besoins en ressources et mémoire très faibles
- flexibilité d'implémentation: cela inclut une grande variété de plateformes et d'applications ainsi que des tailles de clés et de blocs supplémentaires.
- hardware et software : il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle (câblé)
- simplicité : le design de l'AES est relativement simple

Si l'on se réfère à ces critères, on voit que l'AES est également un candidat particulièrement approprié pour les implémentations embarquées qui suivent des règles beaucoup plus strictes en matière de ressources, puissance de calcul, taille mémoire, etc... C'est sans doute cela qui a

poussé le monde de la 3G (3ème génération de mobiles) à adopter l'algorithme pour son schéma d'authentification « Millenage ».

III.3.2. Détails techniques

L'AES opère sur des blocs de 128 bits (plaintext P) qu'il transforme en blocs cryptés de 128 bits (C) par une séquence de Nr opérations ou "rounds", à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de rounds diffère : respectivement 10, 12 et 14 rounds.
Les étapes suivantes décrivent succinctement le déroulement du chiffrement :

- BYTE_SUB (Byte Substitution) est une fonction non-linéaire opérant indépendamment sur chaque bloc à partir d'une table dite de substitution.
- SHIFT_ROW est une fonction opérant des décalages (typiquement elle prend l'entrée en 4 morceaux de 4 octets et opère des décalages vers la gauche de 0, 1, 2 et 3 octets pour les morceaux 1, 2, 3 et 4 respectivement).
- MIX_COL est une fonction qui transforme chaque octet d'entrée en une combinaison linéaire d'octets d'entrée et qui peut être exprimée mathématiquement par un produit marticiel sur le corps de Galois (2^8).
- le + entouré d'un cercle désigne l'opération de OU exclusif (XOR).
- Ki est la ième sous-clé calculée par un algorithme à partir de la clé principale K.

Le déchiffrement consiste à appliquer les opérations inverses, dans l'ordre inverse et avec des sous-clés également dans l'ordre inverse. [14]

III.4. Algorithme de chiffrement RC4 *(Rivest Cipher 4)*

III.4.1. Historique

RC4 a été conçu par Ronald Rivest de RSA Security en 1987. Officiellement nommé *Rivest Cipher 4*, l'acronyme *RC* est aussi surnommé *Ron's Code* comme dans le cas de RC2, RC5 et RC6.

Les détails de RC4 furent initialement tenus secrets mais en septembre 1994, une description du chiffrement fut postée de manière anonyme sur la liste de diffusion *Cypherpunks*. Le message apparut ensuite sur le forum sci.crypt puis sur divers sites. L'algorithme avait vraisemblablement fait l'objet d'une rétro-ingénierie. Sur le plan

légal, RC4 est une marque déposée dont les implémentations non officielles sont autorisées sous un autre nom que RC4, car l'algorithme n'a pas été breveté. La version non officielle de RC4 est aussi connue sous le nom de « *ARCFOUR* », « *ARC4* » ou « *Alleged RC4* » (signifiant « RC4 supposé » puisque *RSA Security* n'a jamais officiellement publié les spécifications de l'algorithme).

Il a par la suite été utilisé dans des protocoles comme WEP, WPA ainsi que TLS. Les raisons de son succès sont liées à sa grande simplicité et à sa vitesse de chiffrement. Les implémentations matérielles ou logicielles sont faciles à mettre en œuvre. [15]

III.4.2. Principe de fonctionnement

RC4 fonctionne de la façon suivante : la clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de mélanger autant que possible le tableau. RC4 fonctionne en effectuant des XOR (OU exclusifs) entre un texte clair et un flux de nombres pseudo-aléatoires. A moins d'initialiser l'algorithme de manière réellement aléatoire, le texte clair peut être découvert. C'est la faille principale du RC4. [16]

III.4.3. Sécurité

De par sa popularité, RC4 a fait l'objet de nombreuses recherches. Il est désormais considéré comme peu sûr du point de vue cryptographique et ne devrait pas être employé pour de nouvelles applications.

Le flux aléatoire généré par RC4 est légèrement biaisé en faveur de certaines séquences d'octets. La meilleure attaque utilisant cette faiblesse a été publiée par Scott Fluhrer et David McGrew. Leur attaque arrive à distinguer un flux pseudo-aléatoire RC4 d'un flux aléatoire, moyennant des données de l'ordre du gigaoctet.

RC4 n'utilise pas un vecteur d'initialisation séparé, en plus de la clé. Un tel vecteur est en général une nécessité pour garantir une sécurité suffisante, de manière à ce que chiffrer le même message deux fois avec la même clé ne produise pas la même sortie. Une approche possible consiste à générer une nouvelle clé en hachant la concaténation de la clé principale avec un vecteur d'initialisation. Toutefois, des applications se contentent de concaténer la clé et le vecteur, sans les hacher. Une telle procédure peut s'avérer vulnérable si elle est mal conçue. [17]

III.5. Algorithme de chiffrement RSA (Rivest Shamir Adleman) :

Cet algorithme a été inventé par **R**ivest R., **S**hamir A., et **A**dlemann L. du M.I.T. (Massachussets Institute of Technology). C'est l'algorithme à clé publique le plus commode qui existe. Comme pour le D.E.S. sa sécurité repose sur l'utilisation de clés suffisamment longue (512 bits n'est pas assez, 768 est modérément sûr, et 1024 bits est une bonne clé). C'est la difficulté que l'on a à factoriser les entiers premiers (le problème des logarithmes discrets est souvent considérés comme insurmontable) qui font que l'on ne peut que difficilement casser cet algorithme car le chiffrement est basé sur une fonction trappe (à sens unique: One-way trapdoor)

Cependant de larges avancées en matière de factorisation des entiers larges, ou une augmentation considérable de la puissance des supercalculateurs rendront RSA très vulnérable.

RSA est aujourd'hui utilisé dans une large variété de produits (téléphones, réseaux Ethernet, etc.), de logiciels de différentes marques (Microsoft, Apple, Novell, Sun), dans des industries et enfin dans les télécommunications.

III.5.1. Principe de fonctionnement du Cryptosystème RSA:

- **Création des clés**

a. Choix aléatoire de deux nombres premiers p et q

b. Calcul de $n = p \times q$ et de e un nombre premier avec $f = (p-1) \times (q-1)$

c. Calcul de d tel que $e.d = 1$ modulo $f = (p-1)(q-1)$

La clé publique de Bob est constituée de n et e *et* sa clé privée est d

- **Chiffrement d'un message**

d. Transformation du message en une suite de chiffres selon une convention connue de tous

B devient $x = 02$ (Lettre → ordre dans l'alphabet)

e. Chiffrage du résultat en utilisant la clé publique de Bob (n et e) et la formule

$y = x^e \bmod(n)$

f. Envoi du résultat y à Bob

Alice veut chiffrer le message 'B' pour l'envoyer à Bob

➢ **Déchiffrement**

g. Bob déchiffre le message y en utilisant sa clé privée d pour calculer $z = y^d$ modulo n

h. Le nombre z est retranscrit en lettres selon la convention utilisée lors du chiffrement le procédé est le même pour un message de plusieurs lettres

Les nombres utilisés dans la réalité ($n, p, q, e...$) font plusieurs centaines de chiffres.

Pourquoi ça marche ?

Comment chiffrer un message avec une clé de sorte qu'il ne puisse être décodé qu'avec une autre clé associée ?

Le théorème mathématique de Fermat-Euler assure que la formule de déchiffrement $z = y^d$ modulo n redonne le message initial $z = y^d = x^{ed} = x$ modulo n

- **Exemple simple:**

Etape 1 : Choix des clés : le message à envoyer est x= 02 ?

P=3 et q=7 alors p.q=21 et (p-1)=2 , (q-1)= 6 alors (p-1) x (q-1)= 12

Choisir e tel que e soit premier avec 12. On choisit e = 5.

On calcul d tel que : e.d =1 mod(12). d = 5 car 5 x 5 = 1 mod 12

la clé publique de Bob est constituée de n et e *(21, 5)* sa clé privée est d *(5)*

Etape 2 : Chiffrage du résultat : En utilisant la clé publique de Bob (*21 et 5*) et la formule $y = x^e$ modulo n

$y = 2^5$ modulo 21 = 32 modulo 21 = 11

Envoi du résultat y à Bob

Etape 3 : Déchiffrement : En utilisant la clé privé (*21 et 5*) et la formule

$z = 11^5$ modulo 21= 161051 modulo 21 = 2

Le nombre z est retranscrit en lettres selon la convention utilisée lors du chiffrement

z = 2 => message en clair = 'B'

- **Exemple plus complexe :**

n=5141=53·97 et **e**=7, premier avec (p-1)(q-1)=52·96=4992).

Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet.

« JEVOUSAIME » devient : "10 05 22 15 21 19 01 09 13 05".

Puis il découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que **n**

Un bloc **B** est chiffré par la formule $\mathbf{C = B^e \bmod n}$, où **C** est un bloc du message chiffré que **Bob** enverra à **Alice**

Après avoir chiffré chaque bloc, le message chiffré s'écrit :

"0755 1324 2823 3550 3763 2237 2052".

Déchiffrement

Alice calcule à partir de **p** et **q**, **qu'elle a gardés secrets**, la clef **d** de déchiffrage (c'est sa **clef privée**). Celle-ci doit satisfaire l'équation $\mathbf{e \cdot d \bmod ((p-1)(q-1)) = 1}$. Ici, **d**=4279.

Chacun des blocs **C** du message chiffré sera déchiffré par la formule $\mathbf{B = C^d \bmod n}$

Elle retrouve : **"010 052 215 211 901 091 305" donc** le message original envoyé par Bob.

III.5.2. Attaques sur RSA

Toute la sécurité RSA repose sur :

1. La clé secrète d (comment un pirate pourra-t-il la trouver ?)
2. Sinon comment trouver p et q (Donc p-1 et q-1) et par conséquent calculer d. Autrement comment factoriser n = p x q ?

Les attaques actuelles du RSA se font essentiellement en factorisant l'entier n de la clé publique (retrouver p et q à partir de n).

1. La sécurité du RSA repose donc sur la difficulté de factoriser de grands entiers.
2. Les clés de 512 bits (longueur de n) ne sont plus considérées comme sûres
3. Les experts recommandent des clés de 1024, voire 2048 bits, pour un usage sensible.

La confiance dans la sécurité du système RSA ne repose pas sur une démonstration. Elle vient plutôt de l'échec répété depuis plus de 25 ans de toutes les tentatives pour casser ce système. Sur le plan théorique, la situation est décevante et le restera longtemps encore. Dès que l'on sait factoriser n en $p \times q$, on trouve immédiatement d. le risque théorique est grand puisque l'on ne sait pas démontrer la difficulté de la factorisation d'un nombre.

Est-ce que ce n'est pas déjà fait ? Des cryptanalyses pénètrent un crypto-système, ils ont intérêt à ne pas dévoiler leur exploit afin de prolonger la durée d'exploitation des informations décryptées. La réponse à cette dernière question reste suspendue. [18]

Conclusion

Ce troisième décrit les différents algorithmes utilisés dans la sécurisation des données, leurs historiques, leurs principe de fonctionnement. Concernant le dernier algorithme décrit qui est le RSA, nous avons donné un exemple de message crypté envoyé et décrypté à la réception. Les différentes attaques possibles lancées sur ces algorithmes ont été aussi cité.

Nous allons essayer de faire l'implémentation de quelques algorithmes sous Matlab.

8	Mali Algérie	uitq itomzqm	Mali Algérie
9	Mali Algérie	vjur jupnarn	Mali AlgeXie
10	Mali Algérie	wkvs kvqobso	Mali AlgeXie

Explication du processus

Message	M	A	L	I	A	L	G	E	R	I	E
Numéro de l'alphabet	13	1	12	9	1	12	7	5	18	9	5
Nombre d'itération maximal	13	25	14	17	25	14	19	21	8	17	21

Exemple 2 : P= Hello World

K	Message original	Message crypté	Message decrypté
2	Hello World	Jgnnq Yqtnf	Hello World
3	Hello World	Khoor Zruog	Hello World
4	Hello World	LippY [svph	HellU World
5	Hello World	MjqqZ \twqi	HellU World

Message	H	e	l	l	O	W	o	R	l	d
Numéro de l'alphabet	8	5	12	12	15	23	15	18	12	4

Nombre d'itération maximal	18	21	14	14	11	3	11	8	14	22

Exemple 3 : P= World Hello

K	Message original	Message crypté	Message decrypté
2	World Hello	Yqtnf Jgnnq	World Hello
3	World Hello	Zruog Khoor	World Hello
4	World Hello	Asvph Lipps	World Hello
5	World Hello	Btwqi Mjqqt	World Hello
6	World Hello	Cuxrj Nkrru	World Hello
7	World Hello	Dvysk Olssv	World Hello
8	World Hello	Ewztl Pmttw	World Hello
9	World Hello	Fxaum Qnuux	WoXld Hello

Message	W	o	r	l	d	H	e	L	l	o
Numéro de l'alphabet	23	15	18	12	4	8	5	12	12	15
Nombre d'itération maximal	3	11	8	14	22	18	21	14	14	11

Exemple 4: western union

Message	W	E	S	T	E	R	N	U	N	I	O	N
Numéro de	23	5	19	20	5	18	14	21	14	9	15	14

l'alphabet												
Nombre d'itération	3	21	7	6	21	8	12	5	12	17	11	12

Explication du processus

La valeur de k	Message original	Message crypté	Message décrypté
1	western union	xftufso vojpo	western union
2	western union	yguvgtp wpkqp	western union
3	western union	zhvwhuq xqlrq	western union
4	western union	aiwxivr yrmsr	western union
5	western union	bjxyjws zsnts	western union
6	western union	ckyzkxt atout	we tern [nion

IV.1.2. Interprétation des résultats

A travers ce programme on remarque que lorsqu'un message commence par les 20 premières lettres de l'alphabet, le nombre d'itération ne peut pas dépasser le nombre d'itération de la plus grande lettre (y compris les six dernières lettres).

Lorsque le message commence par les six dernières lettres de l'alphabet, le nombre d'itération de ces dernières lettres n'est pas pris en compte donc on peut faire une boucle avec un message commençant par les dernières lettres.

IV.2. Cryptage Symétrique

Dans ce type de chiffrement, la même clef sert à coder et à décoder le message. Par analogie, c'est le principe d'une serrure de porte : tous les utilisateurs autorisés ont une clef identique.

Avantages : Plus rapide que le chiffrement asymétrique car il utilise une clef plus réduite.
Inconvénients : Transmission préalable de la clef au correspondant, autant de clefs que de correspondants.

La sécurité dépend de la taille de la clef. Ce type de cryptage est progressivement remplacé par le système à clef publique.

IV.2.1. Cryptage d'un texte en binaire avec DES

C'est un système de chiffrement par bloc de 64 bits, dont 56bits sont utilisé pour le cryptage et 8 bits servent de parité (vérifie l'intégrité de la clé).

Cet algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte chiffré et la clé en faisant en sorte que les opérations puissent se faire dans le sens inverse (pour le décryptage).

Dans cette partie nous avons essayé de crypté et décrypté un texte en binaire avec DES. Les résultats obtenus sont représentés ci-dessous.

- **Texte original en binaire:**

Columns 1 through 21

1 0 1 1 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1 0 1

Columns 22 through 42

1 0 1 1 1 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0

Columns 43 through 63

1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 0 1 1 1 0 1

Column 64

0

Texte crypté avec la clé:

Columns 1 through 21

1 1 1 0 1 0 0 0 1 1 0 0 1 0 1 1 1 1 0 0 0

Columns 22 through 42

1 1 0 1 0 0 0 1 1 1 0 1 1 1 0 1 1 0 1 0 1

Columns 43 through 63

1 1 1 0 1 1 1 0 1 0 1 1 1 0 0 1 0 0 0 1 1

Column 64

0

- **Clé:**

Columns 1 through 21

0 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 1 0 1 1 1

Columns 22 through 42

0 0 0 0 0 0 0 1 0 0 1 1 1 1 1 0 1 1 0 1 0

Columns 43 through 63

1 0 0 1 1 0 0 0 0 1 0 0 1 0 0 1 1 1 0 0 0

Column 64

1

- **Texte décrypté avec la clé:**

Columns 1 through 21

1 0 1 1 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1 0 1

Columns 22 through 42

1 0 1 1 1 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0

Columns 43 through 63

1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 0 1 1 1 0 1

Column 64

0

A = Signal Original – Signal décrypté

$$c = t^e \bmod n$$

Pour décrypter, on utilise la même opération, mais en mettant à la puissance **d** :

$$t = c^d \bmod n$$

IV.3.1. Cryptage d'un message en RSA

Exemples

Prenons comme message **'hello world'** et faisons varier les valeurs de P et Q.

- **P=11 Q=13**

La valeur de N est : 143

La clé publique e est : 7

La valeur de Phi est : 120

La clé privée d est : 103

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

91 62 4 4 45 98 37 45 49 4 100

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

Decrypted Message is: hello world

- **P=13 Q=17**

La valeur de N est : 221

La clé publique e est : 5

La valeur de Phi est : 192

La clé privée d est : 77

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

117 186 75 75 76 2 136 76 173 75 172

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

Decrypted Message is: hello world

- **P=19 Q=23**

La valeur de N est : 437

La clé publique e est : 5

La valeur de Phi est : 396

La clé privée d est : 317

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

225 100 52 52 80 261 104 80 114 52 85

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

Decrypted Message is: hello world

- **P=809 Q=811**

La valeur de N est : 656099

La clé publique e est : 7

La valeur de Phi est : 654480

La clé privée d est : 560983

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

Columns 1 through 7

511971 24707 296430 296430 490743 489837 18754

Columns 8 through 11

490743 392960 296430 381822

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

Decrypted Message is: hello world

- **P=919 Q=929**

La valeur de N est : 853751

La clé publique e est : 5

La valeur de Phi est : 851904

La clé privée d est : 170381

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

Columns 1 through 7

577274 425691 226058 226058 98064 258143 342398

Columns 8 through 11

98064 353272 226058 14537

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

Decrypted Message is: hello world

- **P=1019 Q=1021**

La valeur de N est : 10403999

La clé publique e est : 7

La valeur de Phi est : 1038360

La clé privée d est : 890023

Entrer le message: hello world

ASCII Code of the entered Message:

104 101 108 108 111 32 119 111 114 108 100

Cipher Text of the entered Message:

Columns 1 through 7

16560 20303 727148 727148 194495 561393 363999

Columns 8 through 11

194495 641199 727148 528970

Decrypted ASCII of Message:

104 101 108 108 111 32 119 111 114 108 100

IV.3.2. Cryptage d'une image en RSA

Prenons une image et essayons de la crypter à travers l'algorithme de RSA déjà utilisé ci-dessus. Penons les mêmes exemples pour p et q (p=11 et q= 13).

Nous avons pris une image en nuance de gris que nous avons essayé de décrypter avec l'algorithme RSA sous MATLAB. Les images en nuance de gris et décryptée sont illustrées ci-dessous.

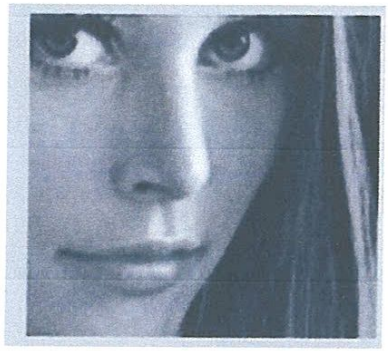

Figure IV.3 : Lena en nuance de gris

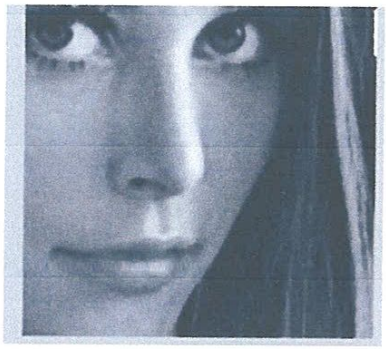

Figure IV.4 : Lena décryptée

IV.3.3. Interprétation des résultats

Toute la force de RSA provient d'un problème de calculabilité (complexité). Il dépend de la taille de **N** car il est très difficile de factoriser **N** en produit de facteur premier **p** et **q**.

Plus la valeur de **p** et **q** augmente, la clé privée **d** augmente et plus il est difficile de décrypté le message à travers les calculs mathématiques.

IV.4. Comparaison entre le cryptage symétrique et le cryptage asymétrique

En général les algorithmes de chiffrement symétrique sont très rapides. D'une part, ils ont une complexité moins élevée qu'un algorithme de chiffrement à clé publique tel que RSA et, d'autre part, ces algorithmes sont souvent très bien adapté à l'architecture du processeur utilisé. Ils sont donc très bien appropriés aux chiffrements de grandes quantités de données.

Concernant le cryptage symétrique, il demande aussi un canal secret pour envoyer la clé sécrète par contre aucun canal secret n'est nécessaire pour pratiquer l'échange de la clé publique pour le cryptage asymétrique.

2n clés seulement sont nécessaires pour que n entités communiquent entre elles pour le cryptage asymétrique par contre pour le cryptage symétrique il faut **n*(n-1)/2** clés.

Le cryptage asymétrique est 1000 fois plus lent que le cryptage symétrique et il est très difficile de trouver sa clé privé

CONCLUSION GENERALE

Conclusion Générale

En perspectives, nous souhaitons que l'étude menée servira de base pour les prochaines promotions des filières Electronique et Télécommunications en ce qui concerne la cryptographie et que dans l'avenir, les travaux seront focalisés sur les problèmes de piratage des données afin d'y mettre fin, et nous suggérons une étude plus poussée sur l'algorithme AES (Advanced Encryption Standard).

Bibliographie

BIBLIOGRAPHIE

[1]http://www.esiee.fr/~bureaud/unites/saci1/tutoriel_g8/les_differents_types_de_chiffrements.html

Date de consultation 04/12/2013

[2] Jean David Olekhnovith, Guillaume Desgeorge **« Les Réseaux locaux ».** 2003

[3] Graw Hill **« le réseau Wifi en tant que boucle locale ».** 2002

[4] http://fr.wikipedia.org/wiki/Wi-Fi

Date de consultation 02/01/2014

[5] Global System for Mobile Communications Architecture, Interfaces et Identités

[6] WLAN les réseaux sans fils et wifi

[7] http://www.gsmworld.com

Date de consultation 17/11/2013

[8] Aurélien Géron préface de Marc Taieb **« Wifi Déploiement et Sécurité ».** 2009

[9] Mémoire de fin d'étude **« La Sécurité dans les Réseaux Informatiques »**

M. Zaaimia Mohammed Zakarya. 2010

[10] Thèse : **« Implémentation d'un réseau RLAN Wifi personnel et d'entreprise »**

M. Bagua Messaoud et M. Benkhelifa Redouane. 2004

[11] iut-tice.ujf-grenoble.fr/tice-espaces/GTR/gsm2/monsite/chapitre4/4.4.htm

Date de consultation 07/12/2013

[12] http://fr.wikipedia.org/wiki/A5/1

Date de consultation : 20/12/2013

[13] http://www.commentcamarche.net/contents/204-introduction-au-chiffrement-avec-des

Date de consultation : 24/02/2014

[14] http://www.securiteinfo.com/cryptographie/aes.shtml

Date de consultation : 22/02/2014

[15] http://fr.wikipedia.org/wiki/RC4

Date de consultation : 24/02/2014

[16] http://touroff.eric.free.fr/802.11/wep.htm

Date de consultation : 24/02/2014

[17] https://www.securibox.fr/securitycenter_crypt.aspx

[18] Cours « Cryptographie » de M. Khebizi Ali (Professeur au Département Information de l'Université 08 Mai 1945 de Guelma)

[19] http://nopb.chez.com/crypto2.html

ESS	Extended Service Set
GMSC	Gateway Mobile Switching Center
GNUPG	GNU Privacy Guard
GSM	Global System for Mobile
GSM/DCS	GSM Digital Cellular System
Hi-Fi	High Fidelity
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSPA+	High Speed Packet Access
HSUPA	High Speed Uplink Packet Access
IBM	International Business Machines
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IMT-2000	Institut des Mérites et des Technologies
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
Kb/s	Kilobits par second
MD5	Message Digest 5
MHZ	Mega Hertz

MIC	Message Integrity Code
MIMO	Multiple-Input Multiple-Output
MOB1	Mobilophonie 1
MOB2	Mobilophonie 2
MS	Mobile Station
MSC	Mobile Switching Center
NBS	National Bureau of Standards
NSA	National Security Agency
NSS	Network Subsystem
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing Protocol
OSI	Organisation International des standards
PDA	Personal Digital Assistant
PI	Permutation Initiale
PMK	Pairwise Master Key
PMKID	Pairwise Master Key IDentifier
PSK	Pre-Shared Key
ROT13	Rotation 13
16-QAM	Quadrature Amplitude Modulation à 16 états
16-QAM	Quadrature Amplitude Modulation à 64 états
QoS	Quality of Service

QPSK	Quaternary Phase Shift Keying
RC2	Ron's Code 2
RC4	Rivest Cipher 4
RC5	Rivest's Code 5
RIPE-MD-160	Race Integrity Primitives Evalution Message Digeste-160
RSA	Rivest Shamir Adleman
RTC	Réseau Téléphonique Commuté
RTCP	Réseau Téléphonique de Commuté Publique
SIM	Subscriber Identification Module
SHA-1	Secure Hash Algorithm-1
SHIFT_ROW	Shifting Row
SMS	Short Message Service
SS7	Signaling system 7
SSID	Service Set Identifier
SRES	Signed RESponse
SRX	Speed and Range Expansion
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UFC	Union Fédérale des Consommateurs
USB	Universal Serial Bus
U-NII	Unlicensed National Information Infrastructure
UNIX	Uniplexed Information and Computer Service
VLR	Visitor Location Register

VPN	Virtual Personal Network
XOR	OU exclusif
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wifi	Wireless Fidelity
WinPT	Windows Privacy Tray
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WWiSE	World-Wide Spectrum Efficiency

Liste des Figures

LISTE DES FIGURES

Chapitre I :

Chapitre II :

Chapitre III :

Chapitre IV :

Liste des Tableaux

LISTE DES TABLEAUX