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

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE ABOU BEKR BELKAID TLEMCEN
FACULTE DE TECHNOLOGIE

DEPARTEMENT DE TELECOMMUNICATIONS

Laboratoire STIC

MEMOIRE

Pour l'obtention du diplôme de
MASTER

Réseaux Mobiles et Services de Télécommunications

Réalisé par
BENHAMIDA Kamel
ATMANI Sid Ahmed

THEME

Développement d'un crypto-système pour l'échange des SMS sous Android.

Soutenu en JUIN 2015 devant les Jurys :

HADJILLA Mourad	M.C.A à l'Université de Tlemcen	Président
MOUSSAOUI Djilali	M.A.A à l'Université de Tlemcen	Examinateur
KADRI Benamar	M.C.A à l'Université de Tlemcen	Encadreur

Année universitaire : 2014-2015

Remerciements

Tout d'abord, nous remercions Allah, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce travail modeste.

Nous remercions vivement notre encadreur Monsieur KADRI Benamar qui a proposé le thème de ce mémoire, et pour ses précieux conseils, remarques, observations et constatations tout au long de la préparation et la rédaction de ce document.

Nous tenons également à remercier Messieurs les membres de jury pour avoir accepté de siéger pour cette soutenance , notamment:

Monsieur le Président HADJILA Mourad de nous avoir honoré de présider le jury, sans pour autant oublié Monsieur l'Examinateur MOUSSAOUI Djilali pour sa persévérance et d'avoir examiné et étudie notre mémoire, devant permettre de nous évaluer dans les conditions les plus adéquates possibles.

Nous saisissons cette occasion pour remercier également l'ensemble du staff pédagogique de n'avoir aménagé aucun effort pour l'acquisition de la science et technologie tout le long de notre cursus universitaire .

Dédicaces

Avec l'aide du bon Dieu le tout puissant, j'ai pu achever ce modeste travail que je dédie :

A mon très cher père pour son amour, sa patience, son soutien moral et matériel ainsi que son encouragement afin de m'assurer cette formation dans les meilleures conditions, et pour tout ce qu'il a fait pour moi. Que Dieu le garde et lui préserve une bonne santé et longue vie.

A ma très chère mère pour toute sa tendresse, son appui, son amour, sa compréhension, son aide, et pour ses nombreux sacrifices. Que dieu la garde et lui réserve une bonne santé et longue vie.

Et à mon grand père et ma grand mère pour toute leurs soutenance, ainsi que toute ma famille pour ses précieuses aides .

A tous mes ami(e)s pour la merveilleuse ambiance qui caractérise et caractérisera toujours notre amitié.

Enfin à toute la promotion RMST 2014/2015.

ATMANI Sid Ahmed

Dédicaces

Avec l'aide du bon Dieu le tout puissant, j'ai pu achever ce modeste travail que je dédie :

A mon très cher père pour son amour, sa patience, son soutien et son encouragement afin de m'avoir aidé à accomplir cette formation dans les meilleures conditions, en mettant à ma disposition touts les moyens nécessaires.

Que Dieu le garde et lui préserve une bonne santé et langue vie.

A ma très chère défunte mère, que Dieu l'accueil dans son vaste paradis, pour sa tendresse, son amour, son éducation ainsi que pour ses précieux conseils et ses sacrifices illimités.

Et à toute ma famille qui m'a toujours soutenue.

A tous mes ami(e)s pour la merveilleuse ambiance qui caractérise notre amitié.

Et enfin à toute la promotion RMST 2014/2015

BENHAMIDA Kamel

Abbreviations

UMTS: *Universal Mobile Telecommunications System*

LTE: *Long Team Evolution*

WIMAX: *Worldwide Interoperability for Microwave Access*

OS: *Operating System*

IOS: *Internetwork Operating System*

SDK: *Software Development Toolkit*

API: *Application Program Interface*

AVD: *Android Visual Device*

AuC: *Authentification Center*

GSM: *Global System for Mobile Communications*

MS*: Mobile Station*

SIM*: Subscriber Identification Module*

BSS*: Base Station Subsystem*

BTS*: Base Transceiver Station*

BSC*: Base Station Controller*

NSS*: Network Subsystem*

MSC*: Mobile Switching Center*

GMSC*: Gateway MSC*

HLR*: Home Location Register*

VLR*: Visitor Location Register*

EIR*: Equipment Identity Register*

OMC*: Operations and Maintenance Center*

IMSI*: International Mobile Subscriber Identity*

MSISDN*: Mobile Station ISDN Number*

***IMEI**: International Mobile Equipment Identity*

***TMSI**: Temporary Mobile Subscriber Identity*

***SM MO**: Short Message Mobile Originated*

***SM MT**: Short Message Mobile Terminated*

***CBS**: Cell Broadcast Service*

***DES**: Data Encryption Standard*

***NSA**: National Security Agency*

***AES**: Advanced Encryption Standard*

***NIST**: National Institute of Standards and Technologies*

***WEP** : Wired Equivalent Privacy*

***RSA**: Rivest, Shamir et Adleman*

***SHA**: Secure Hash Algorithm*

***PKI**: Public Key Infrastructure*

***PGP**: Pretty Good Privacy*

***ART :** Android RunTime*

Liste des figures

Table des matières

Chapitre II: Généralités sur la Cryptographie.

Chapitre III : SecureSMS.

INTRODUCTION GENERALE

Introduction générale

La téléphonie mobile, ou téléphonie cellulaire est un moyen de télécommunications par téléphone sans fil (téléphone mobile). Ce moyen de communication s'est largement répandu à la fin de l'année 1990. La technologie associée bénéficie des améliorations des composants électroniques, notamment leur miniaturisation, ce qui permet aux téléphones d'acquérir des fonctions jusqu'alors réservées aux ordinateurs.

Depuis les années 2010, la majorité des téléphones mobiles dispose de nombreuses fonctions supplémentaires, rendues possibles grâce à l'intégration d'un système d'exploitation évolué dans le téléphone : ce sont les Smartphones (ou ordi-phones).

Contrairement aux téléphones classique, les Smartphones et leurs systèmes d'exploitation (ex : Android, iOS, Windows Phone, Symbian OS, etc.) permettent d'installer des applications, apportant de nombreuses fonctionnalités non présentes lors de l'achat.

C'est dans ce cadre que s'inscrit notre projet de fin d'étude (PFE). En effet, on cherche à mettre sur pied un environnement apte pour développer et déployer une application destinée à des téléphones portables. L'objectif de ce travail consiste à réaliser un crypto-système Android pour l'échange des SMS dans le réseau GSM. Par conséquent, nous avons composé notre travail en quatre parties. La première partie du projet est dédiée essentiellement à l'étude du réseau GSM, le service SMS ainsi que la sécurité dans GSM. Ensuite, la deuxième partie contient des explications sur la cryptographie ainsi que le fonctionnement des systèmes cryptographies (PGP, PKI, RSA…..etc). La troisième partie contient des généralités sur l'espionnage des SMS, les applications mobiles et le système d'exploitation ANDROID. Et enfin, la quatrième partie explique le fonctionnement de notre application.

CHAPITRE I

Généralités sur Les réseaux mobiles

Introduction

Le GSM (Global System for Mobile communications), est un système cellulaire et numérique de télécommunication mobile. Il a été rapidement accepté et a vite gagné des parts de marché aujourd'hui. On note plus de 180 pays qui ont adopté cette norme et plus d'un milliard d'utilisateurs sont équipés d'une solution GSM. L'utilisation du numérique pour transmettre les données ont nettement évolué par rapport à se qui existait dans un passé pas si lointain. On peut citer à titre d'exemple la possibilité de téléphoner depuis n'importe quel réseau GSM dans le monde.

Dans ce chapitre nous avons jugé utile de donner on une vue globale de l'architecture du réseau, la sécurité du réseau GSM ainsi que le service SMS.

I.GSM

L'appellation GSM (Global System for Mobile Communications) regroupe deux types de réseaux cellulaires numériques de télécommunications pour abonnés mobiles :

- **Le réseau GSM900** : il utilise des fréquences porteuses dans la gamme des 900 MHz et il a été le premier type de réseau mobile cellulaire numérique européen.
- **Le réseau DCS1800 :** (Digital Cellular Télécommunications System) qui utilise des fréquences porteuses dans la gamme des 1800 MHz.

Les réseaux GSM/DCS permettent d'offrir au public des services de télécommunication avec une couverture continue sur un vaste territoire. Cette disponibilité du service est obtenue par la localisation automatique de la station mobile et par des accords d'itinérance (roaming) entre opérateurs.

I.1. Architecture générale de GSM [1]

Le système GSM est constitué des entités suivantes (Figure I.1):

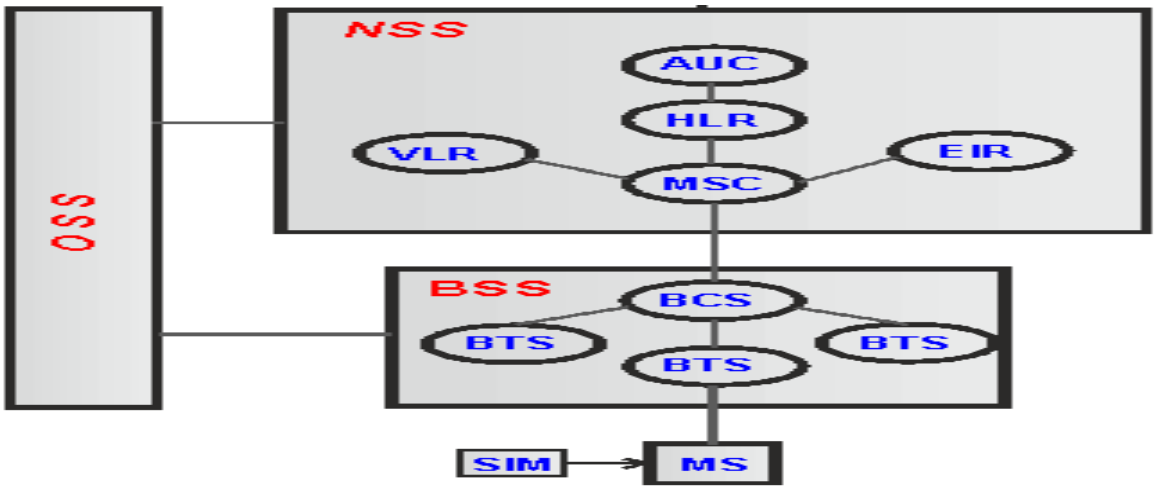

Figure I.1 : architecture de réseau GSM

I.1.1. 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 :

I.1.1.1.Un équipement mobile

Fournit les capacités radio et logicielles nécessaires au dialogue avec le réseau et demeure indépendant de l'abonné utilisateur.

I.1.1.2.Une carte SIM (Subscriber Identification Module)

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.

I.1.2. Sous-système Radio (BSS, Base Station Subsystem)

I.1.2.1. 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 24 communications.

I.1.2.2. 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.

I.1.3. Sous-système réseau (NSS, Network Subsystem)

I.1.3.1. Mobile Switching Center (MSC)

Le centre de commutation des services mobiles (MSC) assure les fonctions de commutation téléphonique. Une fonction spécifique de MSC est la passerelle (GMSC : *"Gateway MSC"*) qui coordonne le trafic en provenance d'autres réseaux. Il comprend également les fonctions de commutation, d'interfaçage avec le réseau de signalisation par canal sémaphore. Un MSC constitue l'interface entre le système radio et les réseaux fixes.

I.1.3.2. Gateway MSC (GMSC)

Gateway MSC (GMSC) est un MSC qui a le droit de recevoir un appel d'un autre réseau et qui assure le routage de cet appel vers la position de localisation d'un mobile. Il peut s'agir du même MSC.

I.1.3.3. Home Location Register (HLR)

Il s'agit de la base de données centrale d'un opérateur de réseau mobile, comportant les informations relatives à tout abonné autorisé à utiliser ce réseau GSM . Afin que les données soient cohérentes sur l'ensemble du réseau.

I.1.3.4. 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 MSC.

Sa mission est d'enregistrer des informations dynamiques relatives aux abonnés actuellement connectés.

I.1.3.5. 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.

I.1.3.6. 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).

I.1.4. Le réseau d'exploitation et maintenance OSS

Le réseau d'exploitation et maintenance comprend les centres d'exploitation maintenance (OMC : Operations and Maintenance Center) qui sont les entités fonctionnelles permettant à l'opérateur du réseau de contrôler son système.

- Un OMC-R (OMC-Radio) prend en charge la supervision et le contrôle d'un ensemble de BSC et BTS.
- Un OMC-S (OMC-Switching) permet de superviser et contrôler un ensemble de MSC/VLR.

Au-delà des OMC-R et OMC-S, on peut trouver, si l'importance du réseau le justifie, un NMC (Network Management Centre) qui assure l'administration générale centralisée du réseau. Les fonctions suivantes peuvent être spécifiquement identifiées :

- Gestion de la sécurité
- Gestion des performances
- Gestion de la configuration
- Maintenance, gestion des alarmes.

I.2. Interfaces GSM [2]

Le système GSM normalise un ensemble d'interfaces entre les entités afin de permettre l'interfonctionnement entre équipements de fournisseurs différents (Figure I.2).

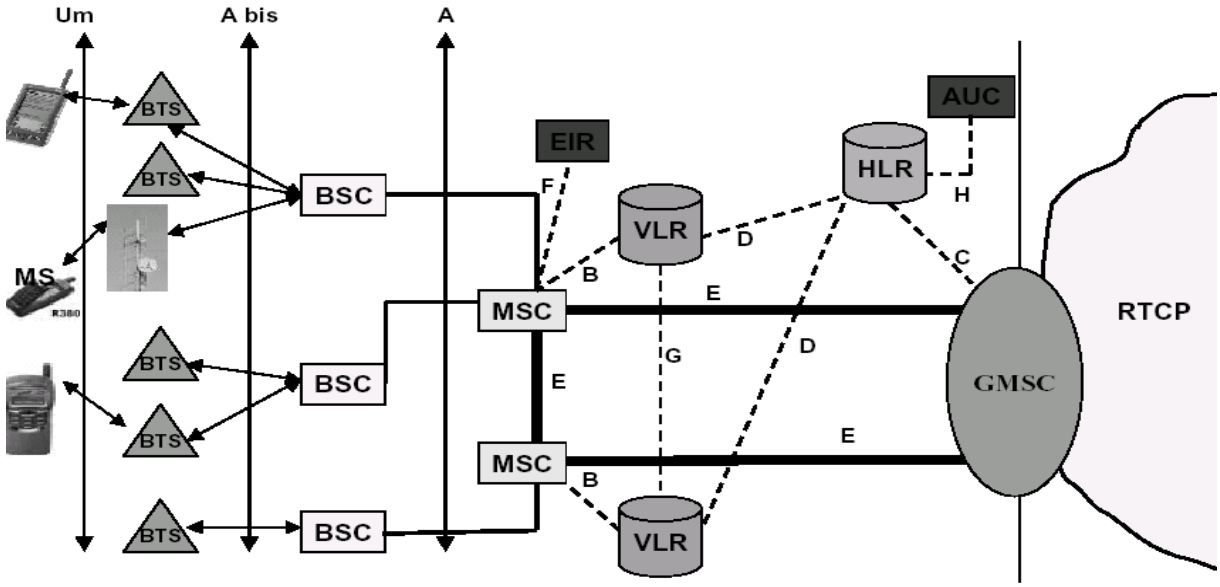

Figure I.2 : interfaces GSM

I.2.1.interface Um

La station mobile (MS) communique avec la BTS par le biais de l'interface radio **Um** qui utilise le protocole de signalisation LAPDm. Cela permet à la station mobile d'établir une connexion de niveau 2 avec la BTS pour fiabiliser le dialogue sur le canal dédié. Le sens montant désigne les activités radio de la station mobile vers le réseau; le sens descendant désigne les activités radio du réseau vers la station mobile. **[4]**

I.2.2.interface Abis

Le BSC et la BTS partagent une interface **Abis** qui utilise au niveau physique des liens à 2 Mbit/s. Le protocole LAPD (Link Access Protocol for the D channel) du RNIS est utilisé pour le transport de la signalisation. **[5]**

I.2.3.interface A

Le BSC et le MSC disposent de l'interface **A** basée sur l'utilisation d'une ou plusieurs liaisons numériques à 2Mbit/s qui supportent le trafic ainsi que la signalisation nécessaire.

I.2.4.interface B

Le biais de l'interface **B** est utilisé lorsqu'un MSC nécessite des informations concernant une station mobile localisée dans sa zone de couverture radio, il interroge le VLR qui lui est dédié. Lorsqu'un mobile démarre une procédure de mise à jour de sa localisation avec un MSC, le MSC en informe son VLR toujours à travers l'interface **B** qui sauvegarde les informations appropriées.

I.2.5.interface C

Le GMSC et le HLR disposent de l'interface **C** permettant au GMSC d'interroger le HLR contenant les caractéristiques d'abonnement d'un abonné mobile, afin d'établir un appel vers sa station mobile.

I.2.6.interface D

L'interface **D** est utilisée entre VLR et HLR pour échanger les données relatives à la localisation d'un mobile ainsi que pour la gestion des caractéristiques de l'abonné.

I.2.7.interface E

Cette interface est utilisée entre deux MSC ou bien entre MSC/GMSC, pour l'exécution des Handover inter MSC ou bien le transport des messages court entre MSC/GMSC.

I.2.8.interface F

L'interface **F** est utilisée entre MSC et EIR afin d'échanger des données pour que l'EIR puisse vérifier l'état de l'identité de l'équipement mobile.

I.2.9.interface G

Lorsqu'un abonné mobile se déplace d'une zone contrôlée par un MSC/ VLR à une autre sous la responsabilité d'un autre MSC/VLR, une procédure de mise à jour de localisation a lieu. Cette procédure peut comprendre l'échange de signalisation entre VLR sur l'interface **G** afin que le nouveau VLR puisse obtenir de l'ancien VLR, l'IMSI et les triplets d'authentification concernant la station mobile.

I.2.10.interface H

Cette interface utilisée entre HLR et l'AUC pour l'échange des données d'authentification.

I.3.Identités dans un réseau GSM [3]

I.3.1.IMSI

IMSI (International Mobile Subscriber Identity) est un identifiant unique affecté à un abonné souscrit à un abonnement mobile auprès d'un opérateur. Cet IMSI est un concept d'adressage spécifique au GSM. Le numéro d 'IMSI n'est pas connu de l'abonné mobile et n'est utilisé que par le réseau GSM.

I.3.2.MSISDN

MSISDN est le numéro de téléphone associé à la station mobile (Mobile Station ISDN Number).

I.3.3.IMEI

L'IMEI (International Mobile Equipment Identity) identifie de façon unique un terminal mobile au niveau international. Il s'agit d'un numéro de série. Ce numéro est alloué par le constructeur du terminal mobile. L'IMEI est utilisé de manière optionnelle par les opérateurs GSM pour lutter contre les vols de terminaux ou pour interdire l'accès au réseau à des terminaux qui auraient un comportement perturbant ou non conforme aux spécifications.

I.3.4. TMSI

TMSI (Temporary Mobile SubscriberIdentity) est un numéro temporaire unique alloué par le VLR à chaque mobile se localisant dans sa zone de couverture. De manière à conserver la confidentialité de l'identité de l'IMSI.

Le TMSI n'est connu que sur la partie MS __ MSC/VLR. Le HLR n'en n'a jamais connaissance.

A chaque changement de VLR, un nouveau TMSI est attribué. L'utilisation du TMSI est optionnelle. On peut avoir recours à l 'IMSI uniquement.

I.3.5. MSRN

Le MSRN (numéro de réacheminement) est un numéro de roaming attribué temporairement à la MS et qui permet de router et d'acheminer l'appel vers le MSC dans l'aire duquel se trouve la MS.

Le schéma suivant décrit les étapes de l'établissement d'un numéro MSRN (figure I.3)

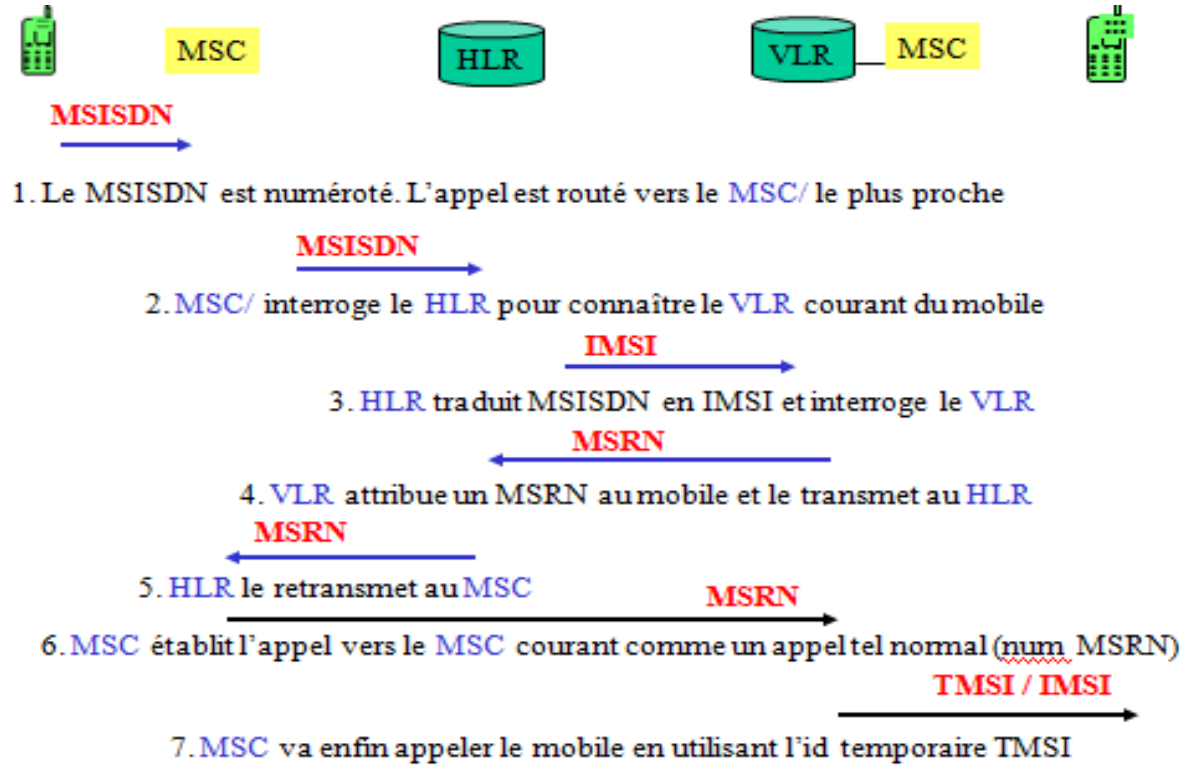

Figure I.3:L'échange lors d'un appel

I.3.6.LAI

Un réseau GSM est divisé en aires de service. Chaque MSC/VLR dans un réseau GSM contrôle une aire de service, composée d'un ensemble de zones de localisation (LA, Location Areas), chaque LA représentant un ensemble de cellules. (La figure I.4) décrit de manière simplifiée un exemple de réseau GSM avec des aires de services.

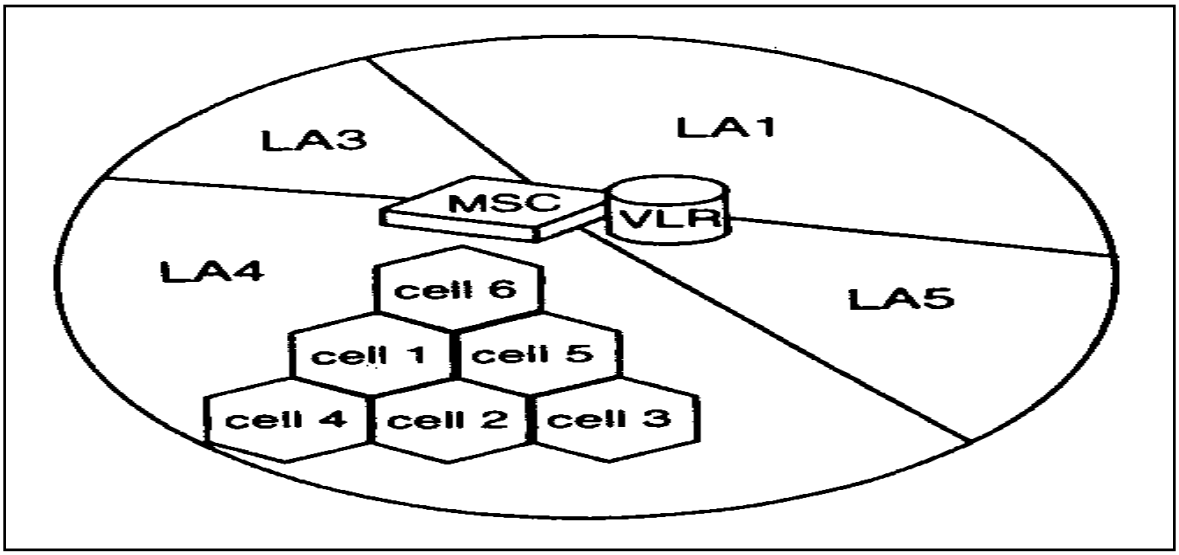

Figure I.4: zone de localisation MSC

I.3.7.CGI

La cellule au sein d'une zone de localisation est identifiée en rajoutant un numéro de cellule (CI, Cell Identity) à l'identification de la zone de localisation. L'identification globale de la cellule (CGI, Cell Global Identification) qui est unique, est donc la concaténation LAI+CI.

II. Développement des réseaux d'accès radio mobiles

II.1.GPRS

Le standard GPRS représente une évolution majeure de la norme GSM et une transition vers la troisième génération, on parle généralement de 2.5 pour classifier ce standard.

Les débits théoriques autorisés par cette génération (9.6 kb/s à 171.2 kb/s) permettent d'envisager de nombreuses applications tels que la consultation du Web, le transfert de fichiers, la transmission de vidéo compressée, etc. La facturation en GPRS se fait selon le volume échangé plutôt qu'a la durée de connexion, ce qui signifie notamment qu'il peut rester connecté sans surcout.

II.2.HSCSD ou EDGE

EDGE représente une seconde forme d'évolution des systèmes 2G. Il s'agit d'une simple évolution de la technologie GSM/GPRS et du système TDMA permettant d'obtenir un débit pouvant atteindre 384 kb/s.

Un terminal mobile dans un réseau EDGE est capable de transmettre et de recevoir sur plusieurs intervalles de temps (IT). Ce qui permet d'envisager des débits de l'ordre 19.2 kb/s, 28.8 kb/s, 38.4 kb/s, 48 kb/s, 56 kb/s, ou 64 kb/s suivant le nombre des canaux alloués.

II.3.UMTS (3G)

Cette norme UMTS est une évolution de la deuxième génération à la troisième génération. Elle constitue une voie royale pour le développement de produits et de services multimédias. Les technologies développées autour de cette norme conduisent à une amélioration significative des services et des vitesses de transfert avec des débits supérieurs à 144 kb/s et pouvant aller jusqu'à 2 Mb/s. Cette amélioration des débits est rendue possible grâce à l'évolution des technologies radio qui autorisent une meilleure efficacité spectrale et l'exploitation de bandes de fréquences supérieures à celles utilisées par la technologie GSM.

II.4. Technologie 4G (LTE, WIMAX)

La 4G est la quatrième génération des standards pour la téléphonie mobile. Elle est le successeur de la 2G et de la 3G. Elle permet le « très haut débit mobile », c'est-à-dire des transmissions de données à des débits supérieurs à 100 Mb/s. Une des particularités de la 4G est d'avoir un «cœur de réseau » basé sur IP et de ne plus offrir de mode commuté, ce qui signifie que les communications téléphoniques utiliseront la voix sur IP.

Les réseaux mobiles WiMAX (Wordwide Interoperability for Microwave Access) et LTE (Long Term Evolution) lancés partout dans le monde sont commercialisés sous l'appellation « 4G ».

III. Sécurité dans GSM [9]

La sécurité dans les réseaux mobiles GSM (sécurité dans les domaines circuit et paquet) repose sur les trois aspects de la sécurité: l'authentification, la confidentialité et la protection de l'intégrité de la signalisation. L'authentification consiste à vérifier l'identité d'un usager. La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction, en la chiffrant. Protéger l'intégrité des données de signalisation consiste à déterminer si les données de signalisation échangées n'ont pas été altérées.

III.1. Clés et algorithmes pour la sécurité GSM

Lorsqu'un abonné souscrit à un abonnement mobile auprès d'un opérateur, il reçoit un identifiant unique appelé IMSI (International Mobile Subscriber Identity). Ce numéro d 'IMSI est stocké sur la carte SIM. Un téléphone mobile ne peut être utilisé que si une carte SIM valide a été insérée dans l'équipement mobile.

Une clé Ki est attribuée à l'usager, lors de l'abonnement, avec l'IMSI. (Figure I.5) elle est stockée dans la carte SIM de l'abonné et dans l'AUC (Authentication Center) au niveau du réseau. Afin d'éviter toute possibilité de lecture de la clé Ki, celle-ci n'est jamais transmise, ni sur l'interface radio, ni sur le réseau.

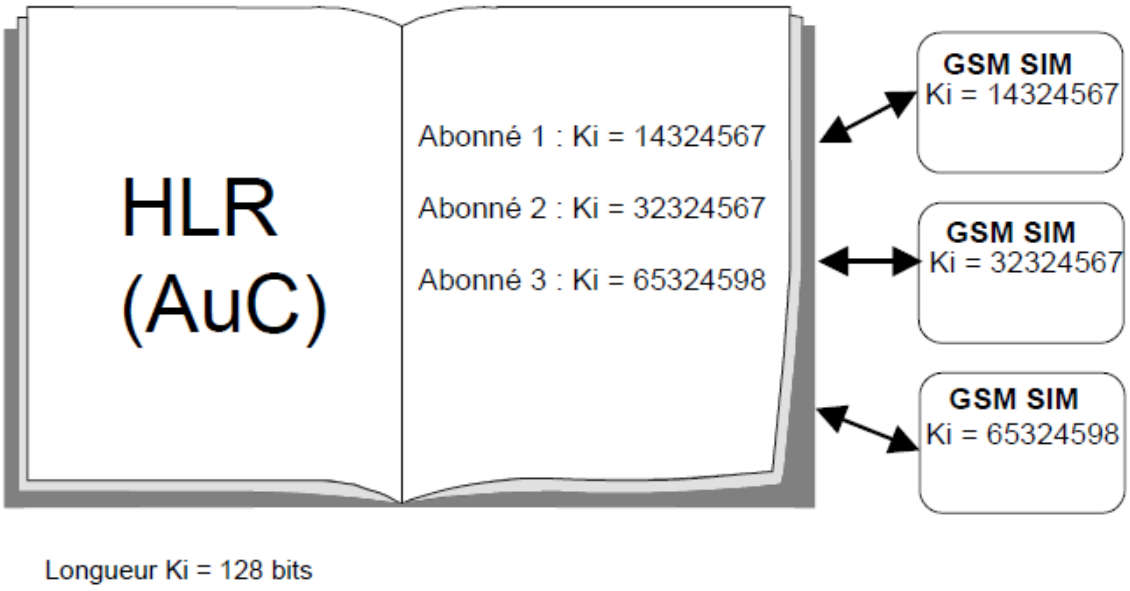

Figure I.5: Clé d'authentification Ki

- Le centre d'authentification AUC dispose de l'algorithme d'authentification **A3**, de l'algorithme de génération de la clé de chiffrement **A8** et des clés Ki des clients du réseau GSM.
- Le BTS dispose de l'algorithme de chiffrement **A5** pour le chiffrement des données usager et des données de signalisation.
- La carte SIM du mobile dispose de l'algorithme d'authentification **A3**, de l'algorithme de génération des clés de chiffrements **A8**, de la clé d'authentification individuelle de l'utilisateur Ki.
- L'algorithme de chiffrement **A5** est contenu dans l'équipement mobile.
- Les algorithmes **A3** et **A8** sont quant à eux les mêmes pour tous les clients d'un même réseau GSM.

III.2.Authentification et Chiffrement GSM

La sécurité GSM est adressée sur deux plans (Figure I.6) : authentification et chiffrement. L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.

- Après que l'usager se soit identifié au réseau à l'aide de son IMSI ou de son TMSI (Temporary IMSI), il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification A3 sont utilisés.
- L'AuC et la carte SIM contiennent la même clé Ki et l'algorithme A3.

- Pour initier le processus d'authentification, l'AuC génère un nombre aléatoire, RAND, d'une longueur de 128 bits.
- Ce nombre RAND ainsi que la clé Ki de l'usager mobile servent de paramètres d'entrée à l'algorithme d'authentification A3.
- Le résultat est appelé SRES. Il s'agit du résultat d'authentification attendu.
- Les mêmes paramètres RAND et Ki sont passés en paramètres de l'algorithme A8 qui produit un résultat Kc.
- Cette clé Kc sert de clé de chiffrement pour le trafic de l'usager et le trafic de signalisation entre le mobile et le BTS.
- Le HLR retourne au MSC/VLR plusieurs triplets (RAND, SRES, Kc).
- Le MSC/VLR utilise le premier triplet et demande au mobile de s'authentifier à partir de la valeur RAND.
- Le mobile réalise la même procédure que l'AuC et produit un résultat d'authentification RES et une clé de chiffrement Kc à partir de la valeur RAND reçue du réseau, de la clé Ki présente sur la SIM et des algorithmes A3 et A8 aussi présents sur la SIM.
- Le mobile soumet le résultat RES au réseau (MSC/VLR) qui le compare au SRES soumis pas le HLR.
- S'ils sont égaux, l'authentification du mobile a réussi.

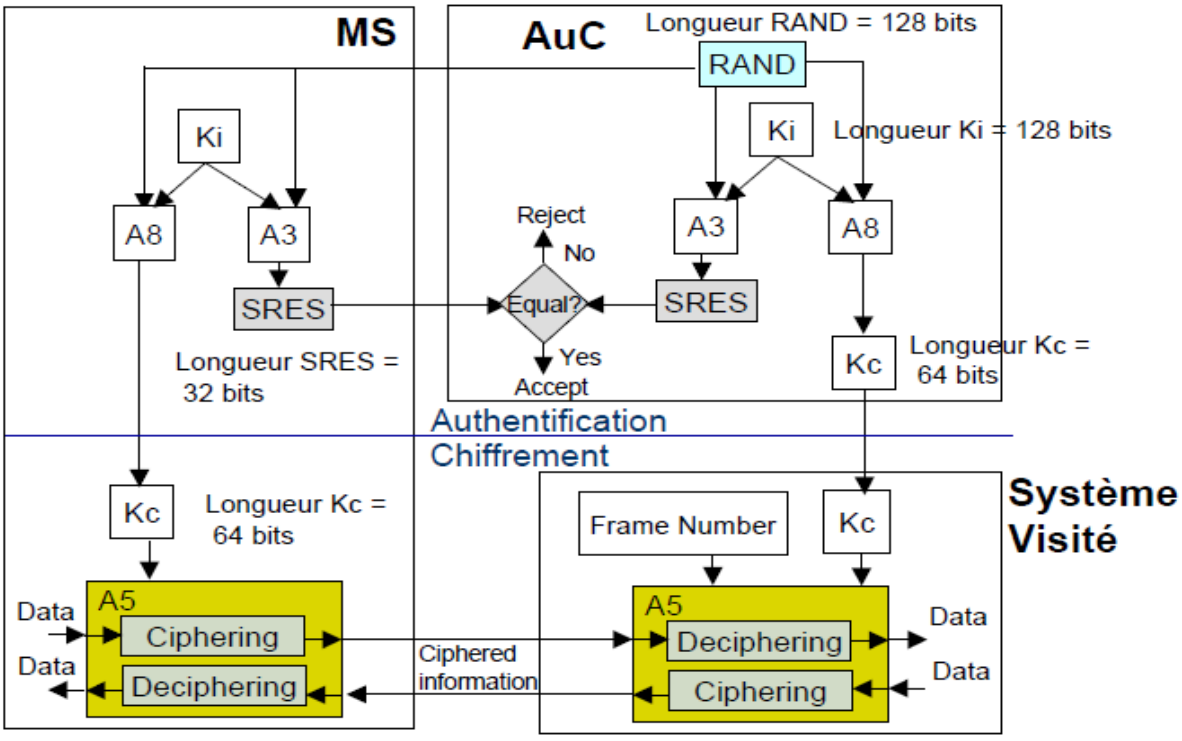

Figure I.6: Sécurité GSM

III.2.1.Le Chiffrement

Un algorithme de chiffrement A5 présent sur la station mobile et la BTS est alors utilisé pour chiffrer/déchiffrer les données de signalisation et de trafic en utilisant Kc. Cet algorithme A5 est normalisé et est le même pour tous les opérateurs mobiles.
La carte SIM contient les informations Ki, A3, A8. L'AuC/HLR contient les informations A3, A8, IMSI/Ki. La station mobile et la BTS contiennent l'algorithme A5.

III.2.2. L'authentification

C'est COMP128-2, l'algorithme de base utilisé par les opérateurs GSM pour la procédure d'authentification et d'échange de clés (Figure I.7).

COMP-128 génère le SRES en utilisant l'algorithme A3 et Kc en utilisant l'algorithme A8 en une seule étape. Il prend en entrée les paramètres Ki et RAND et produit un résultat sur 128bits. Les 32 premiers bits de ce résultat forment le SRES et les 54 derniers bits de ce résultat forment la clé secrète Kc. Les derniers 10 bits du Kc sont positionnés à 0 pour bourrage.

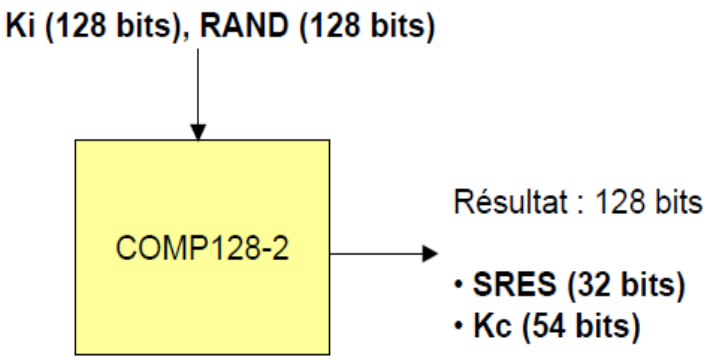

Figure I.7: Algorithme COMP128-2

III.3. Attaques sur les réseaux GSM

L'attaquant peut chercher à briser le chiffrement du réseau mobile. Le chiffrement des réseaux GSM fait partie de la famille des algorithmes A5. Du fait de la politique de sécurité par l'obscurité il n'a pas été permis de tester publiquement la solidité de ces algorithmes. Il y avait principalement deux variantes de l'algorithme qui étaient déployées : A5/1 et A5/2 (chiffrement par flot), ce dernier étant une version plus faible de chiffrement pour les pays ayant des restrictions légales sur l'utilisation des schémas cryptographiques. Depuis que l'algorithme de chiffrement a été rendu public, il a été prouvé qu'il était possible de casser ces algorithmes de chiffrement en environ 6 heures.

D'autres algorithmes publiques plus résistants ont été introduits : le A5/3 et le A5/4 (chiffrement par blocs). Si le réseau ne supporte pas A5/1 ni d'autres algorithmes A5 supportés par le téléphone mobile, le réseau peut à tout moment forcer l'utilisation de A5/0, qui veut dire que la communication n'est pas chiffrée. Même si le téléphone est capable de communications radio 3G ou 4G qui possèdent des algorithmes bien plus résistants que ceux du 2G GSM, le réseau peut limiter la communication radio au 2G (GSM) et forcer l'utilisation d'A5/0 (non chiffré). Ceci permet l'attaque par IMSI catcher. Une fois l'algorithme cassé, l'attaquant peut intercepter en clair toute les communications effectuées par le Smartphone victime.

III.4.Limites de la sécurité GSM

L'authentification GSM est basée sur un protocole de type challenge/réponse ainsi que sur des algorithmes de cryptographie à clé secrète. La 2G ne fournit pas d'authentification mutuelle. Seule une authentification du client est réalisée. La carte SIM du mobile n'est pas en mesure de vérifier l'identité et la validité du réseau auquel le mobile est rattaché. Ceci laisse en théorie la porte ouverte à des attaques de l'homme du milieu. Cependant, de part le coût élevé des stations de base GSM (BTS) ou de solutions commerciales dédiées a l'interception, l'attaque n'est possible qu'avec des moyens financiers assez conséquents.

IV.SMS

IV.1. Définition

Le service de messagerie SMS, plus connu sous le sigle de SMS (*Short Message Service*) ou les noms de texto ou de « mini message », permet de transmettre de courts messages textuels. C'est l'un des services de la téléphonie mobile (il a été introduit par la norme GSM).

Le SMS permet de transmettre des messages de plusieurs milliers de caractères découpés en sous-messages de 160 caractères alphanumériques en encodage sur 7 bits si on utilise l'alphabet latin, soit par 140 caractères binaires en encodage sur 8 bits si on utilise des données binaires , soit encore par 70 caractères en encodage sur 16 bits pour les langues non-Latines comme l'arabe ou chinois.

IV.2. Utilisations des SMS

Les SMS ont pris le pas sur d'autres moyens de communication, et offrent aux clients plus de liberté et d'instantanéité. Les SMS sont aujourd'hui majoritairement utilisés dans les

circonstances où l'écrit est le mieux adapté en particulier lorsque l'on a besoin de transmettre un message à une personne sans vouloir la déranger (réunion, heure tardive…) ou bien lorsque son environnement immédiat ne permet pas une conversation téléphonique dans de bonnes conditions (bus, train, lieux bruyants). Mais de plus en plus les SMS sont aussi utilisés pour partager des émotions, permettre l'attention sympathique, le témoignage d'affection : souhaiter bon anniversaire, adresser ses félicitations et aussi pour partager des sucrés. **[17]**

IV.3.L'aspect commerciale des SMS

Le SMS offre aux Entreprises ce qu'aucun autre médias ne peut Proposer ; avec le SMS vous avez instantanément et à temps réel une interaction dynamique avec vos Prospects, Clients ou partenaires. Ensemble, Mettons en place votre système de marketing par SMS. Construisons ensemble un Processus efficace de fidélisation de vos clients en utilisant les SMS. **[6]**

IV.3.1.Avantages du SMS pour les Entreprises/ Organisations

- Prospecter et mobiliser les clients : Le SMS permet d'établir des relations de travail durables avec vos clients où qu'ils soient et cela de manière professionnelle.
- Promouvoir les nouveaux produits et services : Vos clients actuels sont des prospects chauds pour vos nouveaux produits/services ; le SMS facilite le contact avec ceux-ci. Et si l'offre envoyée est alléchante, le client peut la faire suivre à ses amis en quelques secondes.
- Rassurer et fidéliser les clients : Les entreprises perdent annuellement environ 10% de leur clients tout simplement par manque d'attention portée sur leurs clients ou négligence. Le SMS vous permet une présence continue dans l'esprit du client de façon simple et efficace.
- Annoncer ou rappeler les évènements : La réactivité de ce support est aussi très bonne puisque les cibles consultent leurs SMS dès réception la plupart du temps dans la mesure où chacun garde sur soi son portable que ce soit au bureau, à la maison ou pendant les déplacements. Le SMS est une pratique très abordable.
- Annoncer les arrivages, les déstockages, les baisses des prix, les nouvelles astuces sur l'utilisation de certains produits : Un puissant outil qui permet une interaction instantanée entre les opérateurs d'un même secteur d'activité, des partenaires, des clients professionnels ou autres.

- Communiquer avec vos collaborateurs : les communications SMS offrent un moyen efficace et rapide pour transmettre à vos collaborateurs en déplacement toute information utile à leur travail (consultants, chauffeurs, personnels de terrain …).
- Réduire les coûts de communication interne : l'introduction du SMS en interne réduira vos dépenses en télécommunications de façon considérable.
- Améliorer votre business au quotidien : l'intégration de nos solutions de communication mobile à votre système de marketing rendra votre travail plus efficace et de qualité supérieure.

IV.4.Les dangers pour les SMS sur les téléphones mobiles

Plusieurs types d'attaques menacent les données contenues dans les téléphones mobiles :

- Les vols. En cas de vol, le risque est de voir certaines de ses données usurpées et utilisés à des fins malveillantes.
- Les virus. Le premier virus sur mobile a été détecté en 2004. Depuis, les logiciels malveillants continuent à se propager sur les téléphones : que ce soit par l'intermédiaire de messages piégés (SMS, emails), de logiciels infectés installés sur l'OS, ou d'une connexion Wifi ou Bluetooth mal configurée (interception des mots de passe).

Dans les deux cas, les données personnelles et confidentielles sont exposées au piratage :

- codes secrets.
- coordonnées bancaires en cas de consultation de comptes.
- photos personnelles.
- coordonnées du carnet d'adresses.
- SMS.

IV.5.Le service SMS

Pour mettre en place ce service de messages courts, l'opérateur doit prévoir un ou plusieurs serveurs dédiés et reliés au réseau. On appelle ce serveur le Short Message Service Centre (SMSC). Son rôle est de récupérer les messages envoyés afin de les redistribuer aux destinataires lorsque ceux-ci sont connectés au réseau. Dans le cas contraire, il stocke ces messages. Lorsque le mobile du destinataire peut être de nouveau localisé, le réseau notifie le SMSC qui est alors en mesure de relayer le message. Pour transmettre un message à un mobile, le SMSC utilise les services du MSC ou SGSN auquel est rattaché le destinataire. La livraison du message court est donc garantie même lorsque le terminal mobile est

indisponible (ex, lorsqu'il est éteint ou hors d'une zone de couverture radio) grâce à des fonctions du SMSC.

En fait, il existe deux types de services SMS. Le service point à point et le service cell broadcast.

IV.5.1. Service SMS point à point

La figure I.8 présente un exemple d'architecture SMS.

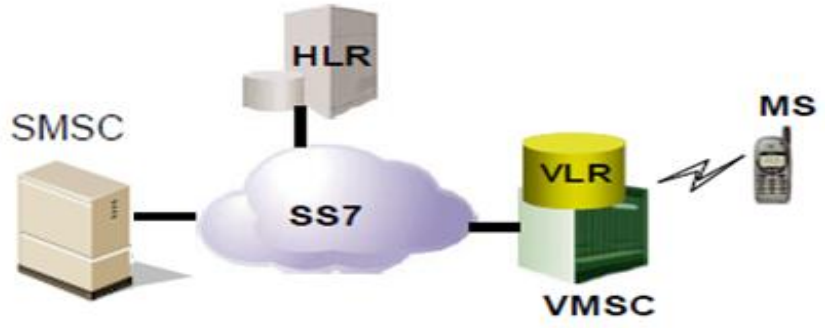

Figure I.8: architecture SMS

IV.5.1.1. Réseau Sémaphore SS7 (figure I.9)

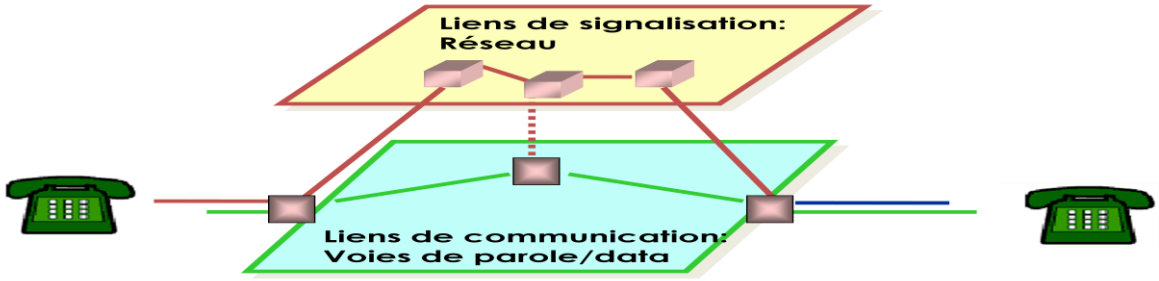

Figure I.9:architecture du réseau SS7

- La signalisation SS7 consiste à séparer logiquement l'aspect signalisation de l'aspect transmission des informations usagers.
- Le réseau de transmission achemine seulement les informations usager, le réseau sémaphore, la signalisation.
- Mais, les deux réseaux peuvent éventuellement partager les mêmes supports physiques de transmission.

IV.5.1.2. Procédure de transfert SMS point à point

Les procédures de transfert de messages courts sont similaires à celles relatives à l'établissement d'appels téléphoniques, à ceci près qu'aucun circuit de parole n'est réservé.

La transmission du message court est prise en charge par le réseau SS7 sur des canaux de signalisation. L'utilisation de ces canaux élimine l'utilisation des ressources limitées de voix**.[23]**

Le service message court point-à-point consiste en deux services de base :

IV.5.1.2.1.Service SM MO (Short Message Mobile Originated Point-to-Point)

SM MO dénote la capacité du réseau GSM à transférer un message court soumis par la station mobile (MS, Mobile station) à une autre station mobile ou à un SME via un SMSC, et celle de fournir un rapport de livraison indiquant la bonne livraison ou toute erreur ayant pu survenir (Figure I.10). **[7]**

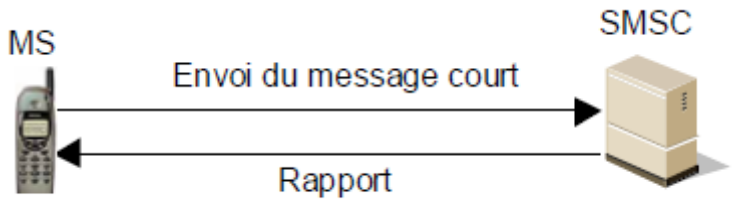

Figure I.10: Service de base SM MO

IV.5.1.2.2.Service SM MT (Short Message Mobile Terminated Point-to-Point)

SM MT dénote la capacité du réseau GSM à transférer un message court soumis par le SMSC à une station mobile et celle de fournir un rapport de livraison indiquant la bonne livraison ou toute erreur ayant pu survenir. Dans ce dernier cas, un mécanisme pour la livraison ultérieure du message court est prévu (Figure I.11). **[7]**

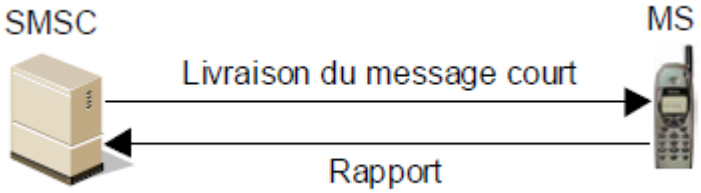

Figure I.11: Service de base SM MT

IV.5.2. Service SMS Cell Broadcast

Le service Cell Broadcast (CBS, Cell Broadcast Service) est analogue au service télétex proposé sur son téléviseur. Comme lui il permet la diffusion d'un certain nombre de messages non acquittés à tous les récepteurs dans une région donnée, messages qui sont diffusés sur des aires appelées Cell Broadcast Areas. Une aire peut comporter une ou plusieurs cellules, voire même inclure l'ensemble du réseau mobile. Après commun accord entre le fournisseur de contenu et l'opérateur mobile une aire de diffusion est affectée à un message CBS. **[8]**

Tous les mobiles présents dans l'aire de diffusion du message CBS sont capables de recevoir d'une BTS ce message dès lors qu'ils sont mis sous tension.

II.2.1 Architecture du service SMS cell broadcast

L'architecture SMS Cell Broadcast est présentée à (figure I.12). Les entités intervenant dans cette architecture sont les suivantes :

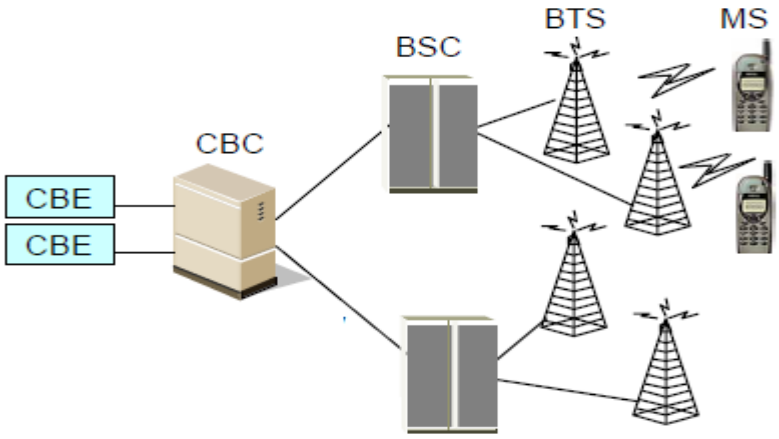

Figure I.12: Architecture du service SMS Cell Broadcast

L'entité CBE est responsable du formatage du message CBS, y compris la fragmentation d'un message CBS en un certain nombre de pages.

Le CBC peut être connecté à plusieurs CBE et plusieurs BSC. Le CBC est responsable de la gestion des messages CBS et des fonctions suivantes en particulier :

- Il alloue un numéro de série au message.
- Il modifie ou supprime les messages pris en charge par le BSC.
- Il désigne l'ensemble des BTS où le message doit être diffusé.

- Il détermine la période de rediffusion du message.
- Il détermine quand le message ne doit plus être diffusé.
- Il diffuse des messages de taille fixe (82 octets) au BSC. Si le message à émettre a une taille inférieure à 82 octets, il le complète avec des octets de bourrage.

V. Conclusion

GSM ne fournit pas de protection de la signalisation (mis à part le chiffrement GSM qui protège les données de l'usager ou la signalisation sur l'interface radio). Cela signifie que les messages de signalisation peuvent être altérés par les équipements radios. C'est ce que la protection de l'intégrité (integrity protection) cherche à prévenir.

Le chiffrement (GSM circuit) s'arrête à la BTS, donc vulnérabilité de l'interface BTS/ BSC.

CHAPITRE II

Généralités sur la Cryptographie

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer.

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

I. La cryptologie

La cryptologie est un art ancien et une science nouvelle : un art ancien car Jules César l'utilisait déjà ; une science nouvelle parce que ce n'est un thème de recherche scientifique académique, c'est-à-dire universitaire, que depuis les années 1970.

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.

I.1.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.

La cryptographie 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 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. **[10]**

I.1.1. Les objectifs de la cryptographie [11]

L'utilisation de la cryptographie a pour objectif d'assurer cinq grandes fonctions de sécurité:

- **L'intégrité**

L'intégrité est la prévention d'une modification non autorisée de l'information.

L'intégrité du système et de l'information garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime.

- **La confidentialité**

Il s'agit de rendre l'information inintelligible à tous les opposants tant lors de sa conservation qu'au cours de son transfert par un canal de communication.

- **L'authentification**

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

- **La non-répudiation**

La non-répudiation consiste à prouver qu'un message a bien été émis par son expéditeur ou reçu par son destinataire.

I.2. La cryptanalyse

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

I.2.1.Les objectifs de la cryptanalyse

On distingue habituellement quatre méthodes de cryptanalyse :

- Une attaque sur texte chiffré seulement 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.
- Une attaque sur texte clair choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair.

- Une attaque sur texte chiffré choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de texte en clair.

II. Le chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement. (Figure II.1)

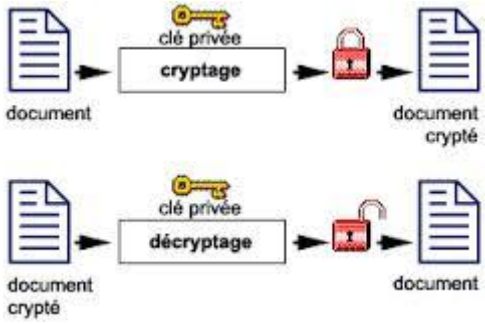

Figure II.1:schéma montre le chiffrement symétrique

Le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles. Ainsi, le moindre algorithme (tel qu'un OU exclusif) peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas).

Toutefois, dans les années 40, Claude Shannon démontra que pour être totalement sûr, les systèmes à clefs privées doivent utiliser des clefs d'une longueur au moins égale à celle du message à chiffrer. De plus le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

Le principal inconvénient d'un crypto-système à clefs secrètes provient de l'échange des clés. En effet, le chiffrement symétrique repose sur l'échange d'un secret (les clés). Ainsi, se pose le problème de la distribution des clés.

D'autre part, un utilisateur souhaitant communiquer avec plusieurs personnes en assurant de niveaux de confidentialité distincts doit utiliser autant de clés privées qu'il a d'interlocuteurs. Pour un groupe de N personnes utilisant un crypto-système à clés secrètes, il est nécessaire de distribuer un nombre de clés égal à N * (N-1) / 2.

Ainsi, dans les années 20, Gilbert Vernam et Joseph Mauborgne mirent au point la méthode du One Time Pad (traduisez méthode du masque jetable, parfois appelé « One Time Password » et noté OTP), basée sur une clé privée, générée aléatoirement, utilisée une et une

seule fois, puis détruite. À la même époque, le Kremlin et la Maison Blanche étaient reliés par le fameux téléphone rouge, c'est-à-dire un téléphone dont les communications étaient cryptées grâce à une clé privée selon la méthode du masque jetable. La clé privée était alors échangée grâce à la valise diplomatique (jouant le rôle de canal sécurisé).

II.1. DES (Data Encryption Standard) [12]

Jusque dans les années 1970, seuls les militaires possédaient des algorithmes à clé secrète fiables. Devant l'émergence de besoins civils, le NBS (National Bureau of Standards) lança le 15 mai 1973 un appel d'offres dans le Registre Fédéral (l'équivalent du Journal Officiel américain) pour la création d'un système cryptographique. Le cahier des charges était le suivant :

- l'algorithme repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement.
- l'algorithme doit être facile à implémenter, logiciellement et matériellement, et doit être très rapide.
- le chiffrement doit avoir un haut niveau de sûreté, uniquement lié à la clé, et non à la confidentialité de l'algorithme.

Les efforts conjoints d'IBM, qui propose Lucifer fin 1974, et de la NSA (National Security Agency) conduisent à l'élaboration du DES (DataEncryption Standard), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXIe s. Le DES fut publié comme standard par le NBS le 15 janvier 1977.

Le DES a progressivement été abandonné à la fin des années 1990. Il a dans un premier temps été remplacé par le triple DES, qui consiste en trois applications de DES à la suite avec 2 clés différentes (d'où une clé de 112 bits). (Figure II.2)

Figure II.2:schéma bloc DES

Si la sécurité était largement assurée, le triple DES était malheureusement trois fois plus lent que le DES. C'est pourquoi, en janvier 1997, le NIST (National Institute of Standards

and Technologies) lance un nouvel appel pour créer un successeur au DES. Une nouvelle saga commence pour l'AES (Advanced Encryption Standard).

II.2.AES (Advanced Encryption System)

Avec le temps, et les progrès de l'informatique, les 256 clés possibles du DES n'ont plus représenté une barrière infranchissable. Il est désormais possible, même avec des moyens modestes, de percer les messages chiffrés par DES en un temps raisonnable. En janvier 1997, le NIST (National Institute of Standards and Technologies) des Etats-Unis lance un appel d'offres pour élaborer l'AES, Advanced Encryption System. Le cahier des charges comportait les points suivants :

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

Au 15 juin 1998, date de la fin des candidatures, 21 projets ont été déposés. Certains sont l'œuvre d'entreprises (IBM,...), d'autres regroupent des universitaires (CNRS,...), les derniers sont écrits par à peine quelques personnes. Pendant deux ans, les algorithmes ont été évalués par des experts, avec forum de discussion sur Internet, et organisation de conférences. Le 2 octobre 2000, le NIST donne sa réponse : c'est le Rijndael qui est choisi, un algorithme mis au point par 2 belges, Joan Daemen et Vincent Rijmen. Depuis, le Rijndael, devenu AES, a été largement déployé et a remplacé progressivement le DES. **[13]**

II.3. RC4 (RivestCipher 4)

RC4 est un algorithme de chiffrement à flot destiné aux applications logicielles. Il a été conçu par R. Rivest en 1987 pour les laboratoires RSA. Malgré un certain nombre de faiblesses, il est encore très utilisé aujourd'hui, notamment du fait de sa vitesse élevée (7 cycles par octet sur un Pentium III par exemple). Il est employé par exemple dans SSL/TLS, protocole permettant d'assurer la confidentialité des transactions Web, dans la norme de chiffrement WEP (Wired Equivalent Privacy) pour les réseaux sans fil, IEEE 802.11b.

L'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 octets. La table d'état est employée pour la génération d'octets pseudo-aléatoires et ensuite pour produire le flux pseudo-aléatoire avec lequel le texte clair sera transformé avec l'opération de l'OÙ-Exclusif. **[14]**

III. Le chiffrement asymétrique

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman.

Dans un crypto-système asymétrique (ou crypto-système à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :(Figure II.3)

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement.

Figure II.3:schéma montre le chiffrement asymétrique

Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé. Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire LDAP). Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

III.1.Diffie Hellman

Le protocole d'échange de clés de Diffie et Hellman repose sur l'arithmétique modulaire, et sur la figure suivante, Tout ce qui est en **vert** est publique (diffusé sur internet). Tout ce qui est en **rouge** est privé. (Figure II.4)

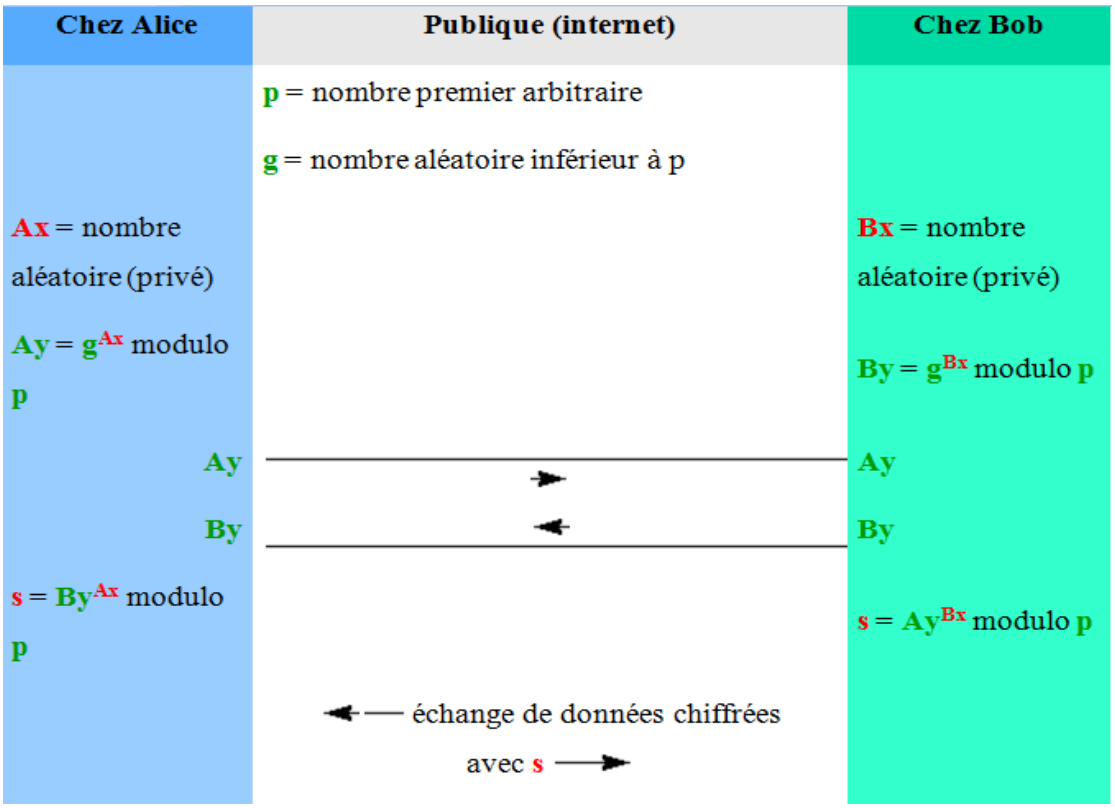

Figure II.4 : échange de clés de Diffie et Hellman

(Modulo est le reste de la division entière.)

À la fin du protocole, Alice et Bob sont donc en possession d'une même clé secrète s, qu'ils ne se sont pas échangés directement. Si quelqu'un a espionné leurs conversations, il connait p, g, Ay et By. Il ne peut pas retrouver s comme le font Alice ou Bob, car il lui manque toujours l'une des informations nécessaires, à savoir Ax ou Bx.

Cette découverte de Diffie et Hellman est une vraie révolution dans l'histoire de la cryptographie. Le problème de l'échange des clés est en effet résolu. Ce protocole a cependant un défaut : il exige la simultanéité des actions d'Alice et de Bob. Si Alice veut envoyer un message à Bob alors que celui dort ou n'est simplement pas connecté, elle ne pourra pas le faire immédiatement. C'est pourquoi ce protocole fut en réalité très vite supplanté par les méthodes de chiffrement à clé publique de type RSA, pour lesquels on met à la disposition de tout le monde une clé publique. **[15]**

III.2.RSA (Rivest, Shamir et Adleman)

La méthode de cryptographie RSA a été inventée en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman. Le RSA est encore le système cryptographique à clé publique le plus utilisé de nos

jours. Il est intéressant de remarquer que son invention est fortuite : au départ, Rivest, Shamir et Adleman voulaient prouver que tout système à clé publique possède une faille. **[16]**

IV. Fonction de hachage

Une fonction de hachage est une méthode permettant de caractériser une information, une donnée. En faisant subir une suite de traitements reproductibles à une entrée, elle génère une empreinte servant à identifier la donnée initiale. De telles fonctions datent de la fin des années 1980 (algorithme MD2) mais l'idée est plus ancienne, et a germé dés l'apparition des codes correcteurs d'erreurs (théorie de l'information).

Une fonction de hachage prend donc en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. On obtient à la sortie une chaine de caractères hexadécimaux, le condensé, qui résume en quelque sorte le fichier. (Figure II.5)

Cette sortie a une taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1).

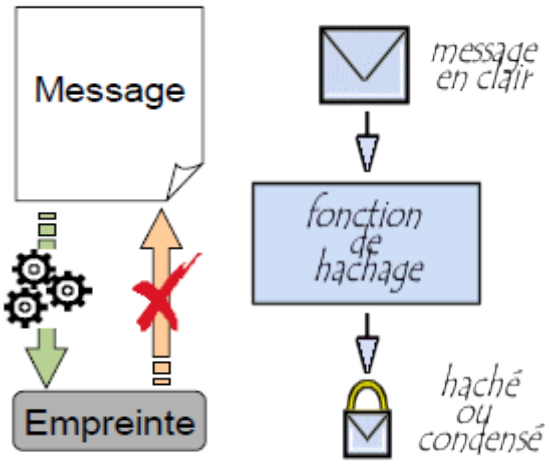

Figure II.5: fonction de hachage a sens unique

IV.1.MD5 (MD signifiant Message Digest)

MD5 Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier).

IV.2.SHA (Secure Hash Algorithm)

SHA pouvant être traduit par Algorithme de hachage sécurisé) crée des empreintes d'une longueur de 160 bits.

SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 2^{64}bits en le traitant par blocs de 512 bits.

V. Signature électronique

Une signature numérique fournit les services d'authentification de l'origine des données, d'intégrité des données et de non-répudiation. Ce dernier point la différencie des codes d'authentification de message, et a pour conséquence que la plupart des algorithmes de signature utilisent la cryptographie asymétrique.

Sur le plan conceptuel, la façon la plus simple de signer un message consiste a chiffrer celui-ci a l'aide d'une clef privée : seul le possesseur de cette clef est capable de générer la signature, mais toute personne ayant accès a la clef publique correspondante peut la vérifier. Dans la pratique, cette méthode est peu utilisée du fait de sa lenteur.

La méthode réellement utilisée pour signer consiste à calculer une empreinte du message à signer et a ne chiffrer que cette empreinte. Le calcul d'une empreinte par application d'une fonction de hachage étant rapide et la quantité de données a chiffrer étant fortement réduit, cette solution est bien plus rapide. **[18]**

V.1. Vérification de signature

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.

Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas. (Figure II.6)

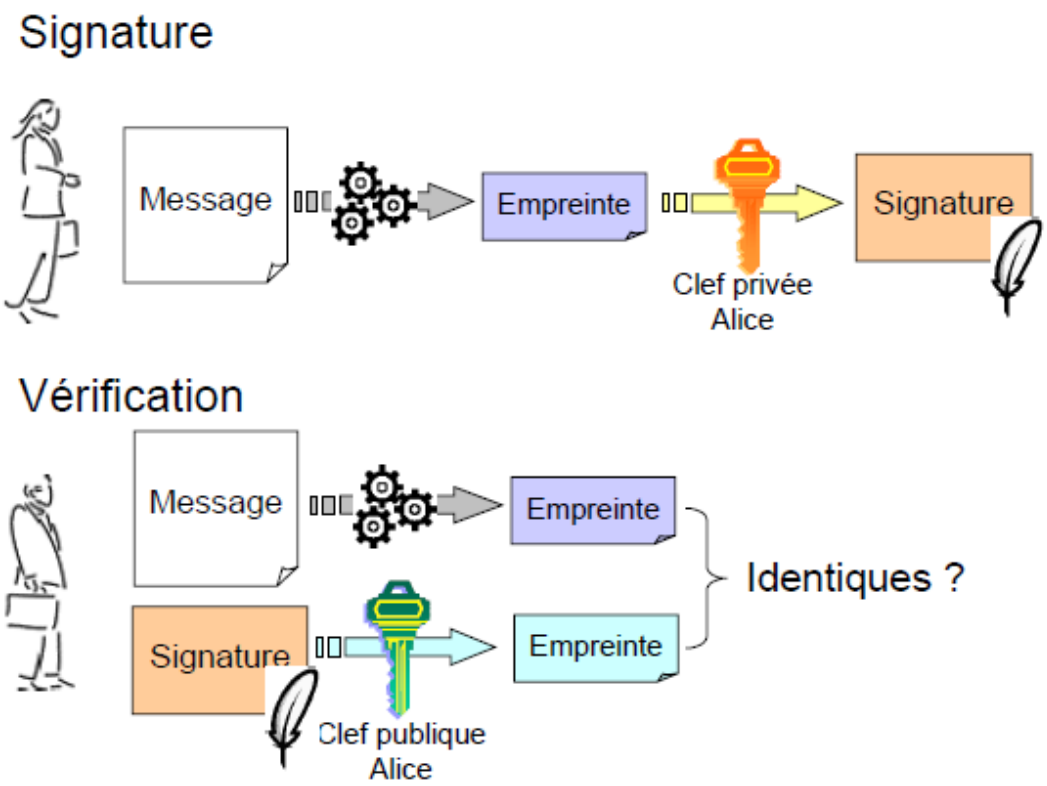

Figure II.6: vérification de signature

VI.PKI (Public Key Infrastructure)

PKI est un système de gestion des clefs publiques qui permet de gérer des listes importantes de clefs publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur.
Une infrastructure PKI fournit donc quatre services principaux:

- fabrication de bi-clés.
- certification de clé publique et publication de certificats.
- Révocation de certificats.
- Gestion la fonction de certification.

Une infrastructure à clé publique utilise des mécanismes de signature et certifie des clés publiques qui permettent de chiffrer et de signer des messages ainsi que des flux de données, afin d'assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation. **[19]**

VI .1.Les composants d'une PKI

Une PKI contient plusieurs composants principaux essentiels à son bon fonctionnement :

- Une Autorité d'enregistrement (AE): Son principal rôle est de vérifier la demande d'enregistrement d'un nouvel utilisateur dans l'infrastructure. Les méthodes de vérification de cette étape sont définies en fonction de la politique de certification choisie pour l'infrastructure. Si l'autorité d'enregistrement valide la demande d'enregistrement, alors la requête de certificat passera entre les mains de l'autorité de certification.
- Une Autorité de Certification (AC): Son principal rôle est de générer un certificat pour l'utilisateur. Le certificat contiendra des informations personnelles sur l'utilisateur mais surtout sa clef publique et la date de validité. L'autorité de certification signera ce certificat avec sa clef privée, ainsi ce certificat sera certifié authentique par lui même.
- Un Annuaire : L'annuaire est indépendant de la PKI cependant la PKI en a besoin. Les seules contraintes de l'annuaire sont qu'il doit accepter le protocole X.509 pour le stockage des certificats révoqués et le protocole LDAP. Son rôle est comme dit précédemment de stocker les certificats révoqués et par la même occasion, les certificats en cours de validité afin d'avoir un accès rapide à ces certificats. De plus, l'annuaire peut stocker les clefs privées des utilisateurs dans le cadre du recouvrement de clef. (Figure II.7)

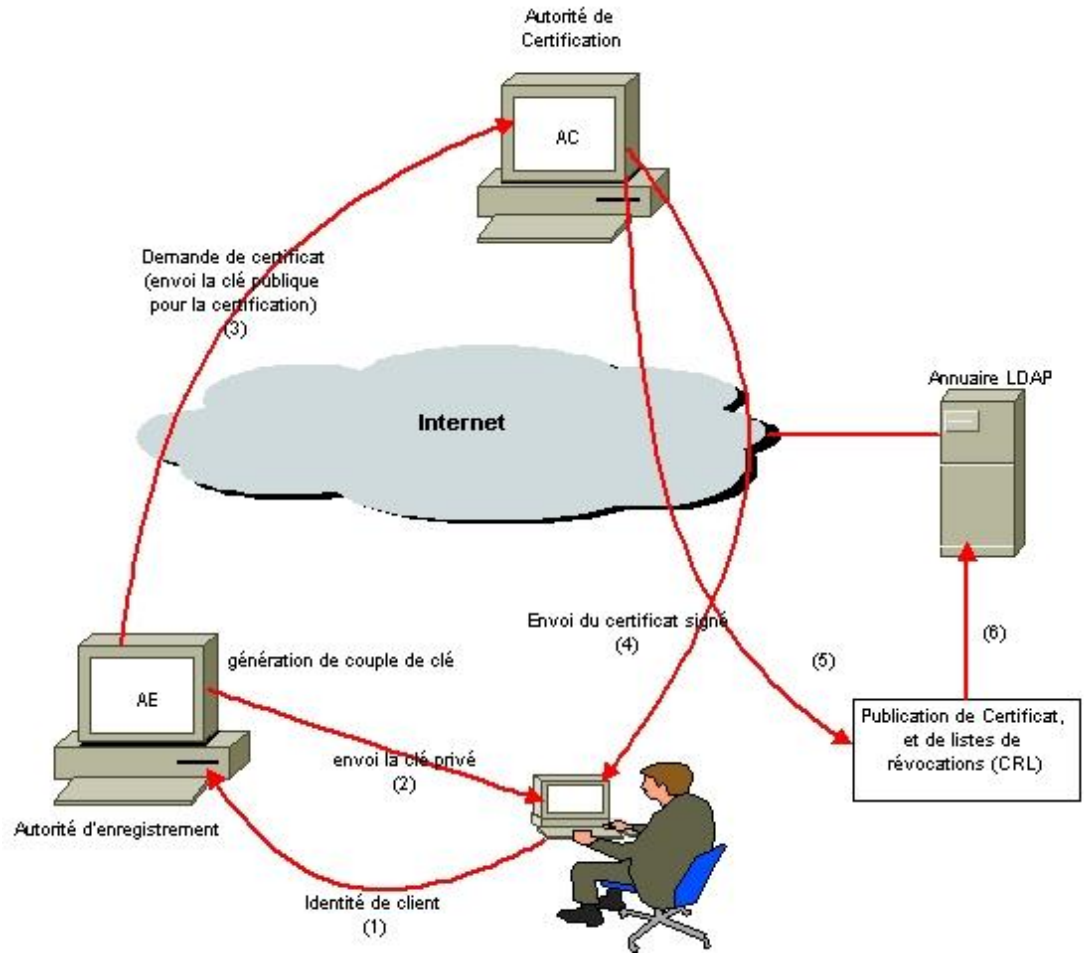

Figure II.7: Organisation d'une PKI

VI.3.Structure d'un certificat (Figure II.8)

- **Version :** indique à quelle version de X509 correspond ce certificat
- **Numéro de série :** Numéro de série du certificat
- **Algorithme de signature:** identifiant du type de signature utilisée
- **Emetteur :** Distinguished Name (DN) de l'autorité de certification qui a émis ce certificat.
- **Valide à partir de:** la date de début de validité de certificat
- **Valide jusqu'à :** la date de fin de validité de certificat
- **Objet:** Distinguished Name (DN) de détenteur de la clef publique
- **Clé publique :** infos sur la clef publique de ce certificat
- **Contraintes de base :** extensions génériques optionnelles
- **Utilisation de la clé :** l'objet d'utilisation de la clé
- **Algorithme thumbprint :** algorithme de signature

- **Thumbprint :** signature numérique de l'autorité de certification sur l'ensemble des champs précédents.

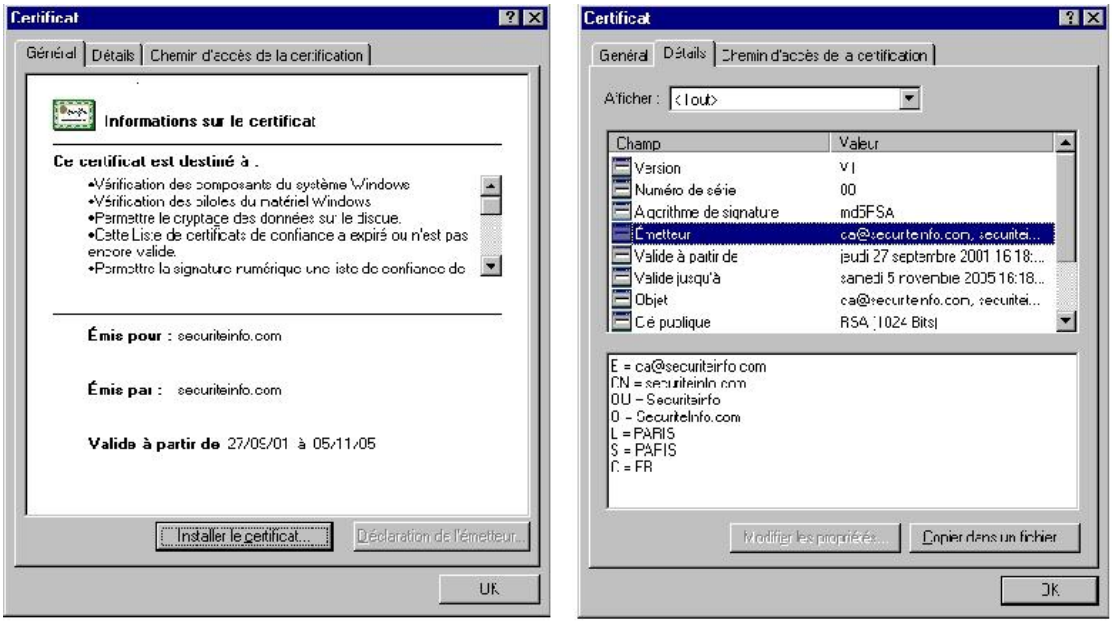

Figure II.8: Exemple d'un Certificat X509

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

VII. PGP (Pretty Good Privacy) [20]

PGP (Pretty Good Privacy) est un crypto-système (système de chiffrement) inventé par Philip Zimmermann, un analyste informaticien. Philip Zimmermann a travaillé de 1984 à 1991 sur un programme permettant de faire fonctionner RSA sur des ordinateurs personnels (PGP).Cependant, étant donné que celui-ci utilisait RSA sans l'accord de ses auteurs, cela lui a valu des procès pendant 3 ans, il est donc vendu environ 150$ depuis 1993.

Il est très rapide et sûr ce qui le rend quasiment impossible à crypt-analyser.

VII.1. Le principe de PGP

PGP est un système de cryptographie hybride, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique.

Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.

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

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

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

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

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

Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clef publique à la vitesse du cryptage conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que les algorithmes de chiffrement à clé publique. Le chiffrement à clé publique résout le problème de la distribution des clés. Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clefs, sans pour autant compromettre la sécurité. (Figure II.9)

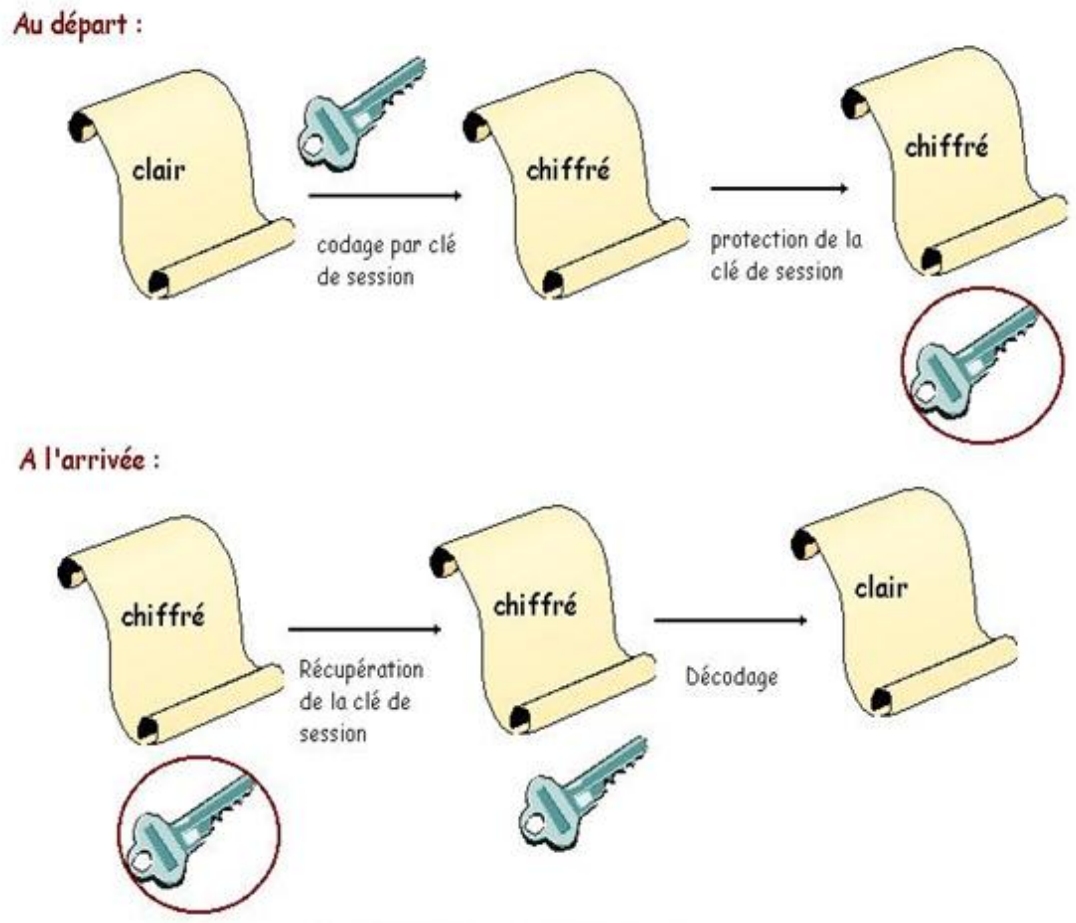

Figure II.9: Principe de chiffrement du PGP

Le PGP implémente donc le meilleur de la cryptographie à clé secrète et à clé publique. Il utilise la rapidité de la cryptographie à clé secrète, et résout l'échange des clés secrètes grâce à la cryptographie à clé publique. Par ailleurs, PGP implémente aussi les fonctions de certificat (l'expéditeur est sûr qu'il envoie son message au bon destinataire) et de signature électronique (le destinataire est sûr que le message vient bien de l'expéditeur).

Une propriété particulièrement intéressante de PGP, et qui contribua beaucoup à son succès, est qu'il agit de façon totalement transparente pour l'utilisateur, qui peut toujours utiliser son logiciel e-mail préféré sans se soucier de la façon dont le chiffrement est implémenté. Par exemple, le couple clé publique/clé privée est généré par PGP lors de son installation à partir des mouvements de souris de l'utilisateur. Voici une bonne façon de générer des nombres aléatoires!

Une autre fonction particulièrement intéressante de PGP est sa façon de gérer les certificats. Alors que la procédure générale consiste à faire certifier son identité par une autorité de certification, procédure bien adaptée aux entreprises, mais pas aux particuliers,

PGP fait fonctionner les réseaux sociaux. Si je fais toute confiance à Laurent, et que Laurent me garantit la clé publique de Yanick, j'ai toutes les raisons de faire moi aussi confiance en la clé de Yanick. On se constitue ainsi un trousseau de clés avec pour chacune une note de confiance, et on partage ce trousseau avec ses amis!

VIII. Conclusion

La cryptographie a défini les notions de sécurité et prouvé la sécurité de crypto systèmes de chiffrement, de codes d'authentification de messages et de signatures numériques. De plus, des protocoles de plus haut niveau, comme des systèmes de communications sécurisées ou de votes électroniques, ont été conçus.

CHAPITRE III

SecureSMS

La planète se rétrécit, tout le monde sait tout de tout le monde. Dans cet univers créé par les TIC, le respect de la confidentialité et de la vie privée sont sérieusement menacés. C'est en tout cas l'argument sur lequel s'appuient les sceptiques, ceux qui hésitent encore à créer des espaces personnels sur les réseaux sociaux et autres sites Internet de correspondance. Pour les abonnés cellulaires, la question de la confidentialité des SMS et des MMS échangés se pose également : est-ce que les agents des services opérateurs GSM lisent les messages que nous envoyons à partir de notre cellulaire ?ou part quelqu'un d'autre?

I. Espionnage

I.1 Espionnage des SMS dans le réseau de l'opérateur

De façon basique, lorsque nous envoyons un SMS, celui-ci transite par le centre de messagerie de l'opérateur, avant d'atterrir chez le destinataire final. Le cycle de vie du texto est établi de sorte qu'un point de transit central installé chez l'opérateur coordonne la transmission. C'est ce centre de messagerie qui identifie le type de message, le numéro d'origine, le réseau cible, le numéro cible, qui gère les périodes de validité, et établit la connexion entre deux téléphones portables distants. C'est dire que nos opérateurs à travers leurs infrastructures réseaux ont le contrôle de nos messages et peuvent en user pour des besoins spécifiques.

Tout se passe dans les attestations de licence qui autorisent nos opérateurs à exploiter un service numérique GSM. D'abord, auprès des fournisseurs de nos opérateurs il y a des restrictions. Car nos opérateurs sont eux aussi clients chez Erickson, Nokia, Alcatel-Lucent qui leur fournissent les plateformes matérielles et logicielles de messagerie (SMSC). En général, les fonctionnalités qui permettent de lire le contenu des SMS des abonnés sont désactivées, en accord avec des licences spécifiques qui leurs sont allouées par ces géants de la télécommunication. Tout comme au niveau local, l'autorité de régulation des télécommunications a fixé des clauses similaires pour les opérateurs du pays. Et même sans cela, ces derniers ne disposeraient pas de temps suffisant pour lire le contenu des millions des textos échangés toutes les heures. Le contenu du SMS relève de la vie privée de l'abonné.

En réalité, ce qui se fait, c'est qu'ils lisent les en-têtes des messages sans toucher au contenu. Ainsi dans les agences, les services commerciaux et les centre d'appel disposent d'applications informatiques qui leur permettent de retracer l'historique des messages échangés : numéro cible, nombre de messages, taille du message, format, facturation appliquée. Ces applications servent à fournir un historique de chaque SMS qui passe par

l'opérateur afin d'améliorer la qualité du service et résoudre des problèmes ponctuels des utilisateurs. «Les applications dont nous disposons au service commercial ne fournissent pas de fonctions qui nous permettraient de lire les messages des abonnés. C'est au niveau des services techniques, les plus en amont que cela est envisageable, mais ils n'ont pas le droit», confie une conseillère client chez un opérateur GSM.

En somme, les opérateurs GSM peuvent lire les SMS que nous envoyons, ils ont les moyens techniques pour le faire. Mais cela est proscrit par les lois. **[21]**

I.2 Espionnage des SMS par logiciel

Espionner les SMS est aujourd'hui possible et très facile. C'est une fonction de base proposée par tous les logiciels espions permettant d'espionner un portable.

Utiliser un logiciel espion SMS n'a jamais été aussi facile. Il suffit d'installer le logiciel espion sur un portable et celui-ci va faire une copie de chaque SMS envoyé et reçus par le téléphone. Peu importe que le message original soit effacé, car de toute façon, le logiciel espion aura déjà sa propre copie. Ensuite c'est très simple le logiciel va envoyer une copie des SMS sur votre espace client. Toutes les données envoyées ou reçues par le portable sont copiées puis envoyées sur votre espace client que vous pouvez consulter depuis n'importe quel appareil équipé d'une connexion internet. Avec votre identifiant et le mot de passe que vous aurez choisi vous pourrez consulter votre espace client et donc espionner les SMS n'importe où et n'importe quand. **[22]**

Il existe plusieurs logiciels espions on va citer quelques un:

- Flexispy.
- Mspy.
- Mobile-spy.
- Spybubble.
- Mobistealth.

I.3 L'espionnage des SMS par NSA

La NSA n'arrête décidément pas de faire parler d'elle. Le journal britannique The Guardian, vient de publier de nouvelles informations basées sur d'autres documents du jeune consultant Edward Snowden. On apprend que l'Agence de sécurité nationale américaine a récupéré près de 200 millions de SMS par jour dans le monde, et ce de façon systématique.

Ce programme a pour nom de code « Dishfire ». La NSA utilise cette base de données pour obtenir des renseignements sur les voyages, les contacts, les transactions financières des utilisateurs de téléphones portables. L'espionnage concerne également les individus qui ne sont soupçonnés d'aucune activité illégale. Le programme collecte et analyse des messages automatiques tels que ceux signalant les appels en absence ou les textos envoyés par les banques. **[23]**

I.4 Equipement d'espionnage

Le CVKA-G108 est un émetteur audio utilisant a technologie GSM pour surveiller un lieu à la demande. il suffit en fait de placer une carte SIM à l'intérieur et de téléphoner au numéro de Plus fort encore cette même carte pour écouter tout ce qui se passe dans a pièce ou vous avez mais l'appareil: comme vous ne savez pas toujours quand il se passera quelque chose, il est même possible de se faire prévenir par SMS lorsque l'appareil détectera du bruit ou des voix aux alentours. L'appareil en lui-même est assez petit (52x40x15 mm) pour être dissimulé dans une pièce, dans une voiture ou un sac à dos. (Figure III.1) **[24]**

Figure III.1.a: CVKA-G108 **Figure III.1.b:** dimension de CVKA-G108

I.5 Espionnage des opérateurs par NSA

La question de la sécurité de nos données sur nos téléphones portables vient d'être remise sur le tapis. Edward Snowden(ex-informaticien de la CIA et de la NSA) nous révèle que la NSA ne surveille pas que les américains ou les britanniques, mais tous les réseaux mobiles du monde entier grâce à un programme Top Secret : l'Opération Auroragold. L'opération Auroragold existe depuis 2011 et semble être encore mise en application aujourd'hui. Et le programme semble très puissant puisqu'en l'espace d'un seul mois, en l'occurrence mai 2012, la NSA aurait récolté les informations de 701 réseaux cellulaires. Cela représente 70% des 985 réseaux mobiles au monde. La NSA a fouillé dans plus de 1200 comptes d'employés de grands opérateurs mondiaux.

Elle a ainsi pu accéder à des fichiers ultrasecrets contenant les détails sur les chiffrements des données des opérateurs. A partir de là, le plus dur était fait. La NSA n'avait plus qu'à introduire des failles dans les protocoles pour pouvoir accéder à tout ce qu'elle voulait. Et évidemment, tout cela est fait pour nous protéger. C'est en tout cas ce que sous-entend l'argument très (trop ?) souvent entendu de l'organisme de surveillance, qui a insisté sur le fait que la loi autorise ce genre de pratiques à des fins de sécurité. Selon William Binney (ancien employé de la NSA), la NSA enregistre et conserve près de 80% de tous les appels audio. **[25]**

II. Les applications mobiles [26]

II.1. Définition

Une application mobile est un logiciel applicatif développé pour être installé sur un appareil électronique mobile, tel qu'un assistant personnel, un téléphone portable, un « Smartphone », ou un baladeur numérique. ...etc.

II.2. Développement

Les applications mobiles sont développées sur des ordinateurs ; le langage utilisé dépend du système sous lequel l'application sera exécutée. Les applications pour les terminaux Apple sont développées dans un langage principalement dédié à ces applications mobiles, l'Objective C. Celles pour Windows Mobile, sont développées en C#, langage aussi utilisé pour les programmes exécutables .ex. Le système Android utilise, quant à lui, un langage universel, le Java, langage pouvant être utilisé pour les ordinateurs, le développement Web (JavaScript).

II.3.Objectifs

Elles visaient d'abord la productivité et à faciliter la récupération d'informations. La demande du public et la disponibilité d'outils de développement ont conduit à une expansion rapide dans d'autres domaines, comme :

- Les jeux mobiles.
- Les automatismes industriels.
- Le GPS et les services basés sur la localisation.
- Les opérations bancaires.
- Les suivis des commandes, l'achat de billets.
- Des applications médicales mobiles.
- La réalité virtuelle.

II.4. Les avantages et Les inconvénients d'une application mobile [27]

II.4.1. Les avantages d'une application mobile

Le principal avantage d'une application mobile est son ergonomie conçue spécifiquement pour le terminal qui la supporte. Cela procure une meilleure expérience pour l'utilisateur. Par exemple, les boutons et les moyens de passer d'une page à l'autre ne sont pas les mêmes sur iPhone et BlackBerry.

De plus elle permet d'utiliser et d'intégrer toutes les fonctionnalités du téléphone (accéléromètre, gyroscope, GPS, caméra…), ce qui n'est pas forcément le cas des WebApps. L'expérience utilisateur est du surcroit enrichie. Par exemple, une application avec un accès au GPS permettra de vous géo-localiser et de vous trouver une information pertinente à proximité.

Une fois téléchargée et installée, elle peut fonctionner sans connexion à internet et se lance plus rapidement que les WebApps. Il n'est plus nécessaire de retenir une adresse web à rallonge, ouvrir son navigateur puis taper le lien, puisqu'il suffit désormais la plupart du temps de seulement toucher une icône.

II.4.2. Les inconvénients d'une application mobile

Le principal inconvénient d'une application mobile est qu'elle doit respecter les règles définies par les différentes sociétés des plateformes mobiles. Que ce soit l'approbation nécessaire des Apps Store pour diffuser l'application ou ses mises à jour, les conditions

tarifaires imposées ou le non compatibilité avec les autres systèmes d'exploitation mobiles.

Le coût lié au développement d'une application mobile est un frein car généralement plus élevé si elle est portée sur plusieurs plateformes (afin d'être disponible pour un maximum de mobinautes) que le coût d'un site mobile ou d'une Web App. Il faudrait potentiellement prévoir un développement sur chaque technologie, et donc un coût supplémentaire si l'on souhaite se positionner sur tous les modèles.

Pour que l'utilisateur ait accès à la dernière version, il faut qu'il la mette à jour depuis le store contrairement aux sites mobiles et WebApp qui se mettent à jour directement.

III. Création d'Android

Quand on pense à Android, on pense immédiatement à Google, et pourtant il faut savoir que cette multinationale n'est pas à l'initiative du projet. D'ailleurs, elle n'est même pas la seule à contribuer à plein temps à son évolution. À l'origine, « Android » était le nom d'une PME américaine, créée en 2003 puis rachetée par Google en 2005, qui avait la ferme intention de s'introduire sur le marché des produits mobiles. La gageure, derrière Android, était de développer un système d'exploitation mobile plus intelligent, qui ne se contenterait pas uniquement de permettre d'envoyer des SMS et transmettre des appels, mais qui devait permettre à l'utilisateur d'interagir avec son environnement (notamment avec son emplacement géographique). C'est pourquoi, contrairement à une croyance populaire, il n'est pas possible de dire qu'Android est une réponse de Google à l'iPhone d'Apple, puisque l'existence de ce dernier n'a été révélée que deux années plus tard.

Au début de Novembre 2007, Google a annoncé la création de son propre système mobile, open source sous le nom Android cette alliance était basée entreprise Open Handset Alliance, qui regroupe des entreprises comme Google, HTC, Intel, Motorola, Qualcomm, Samsung, LG, T-Mobile, Nvidia, Wind River Systems et d'autres. Son objectif est de développer des normes ouvertes pour les appareils mobiles. Pour 12 le nombre a été publié la première version du SDK Android, et après que Google a annoncé un concours «Android Développer Challenge», avec un fonds de prix de 10 millions de dollars US. La tâche de la concurrence - de créer leur application mobile préférée. Des manifestations ont été organisées en 2008 et a fini avec 50 finalistes pour l'attribution de grands prix en argent (25 à 275000 dollars) 23 Septembre 2008 est décerné Android SDK 1.0 r1, et Open Handset Alliance a

publié le code source du système Android. Le code source Android totale de 2,1 Go ». Licence préférée" dans le code source Android est le code de licence 2.0.Iskhodny Apache est

disponible sur la plateforme Android source. Android.comNa lendemain mis en vente le premier Smartphone fonctionnant sur le système d'exploitation Android 1.0 «Applebread ». Système (tarte aux pommes) basé sur le noyau Linux 2.6.25. . L'appareil est fabriqué par HTC et portait le nom de T-Mobile G1 (HTC Dream) Aussi ce jour-là (Figure III.2), il a été annoncé dans le Market Android d'ouverture - les applications de vente en ligne de Google. Depuis sa création, la popularité d'Android a toujours été croissante. C'est au quatrième trimestre 2010 qu'Android devient le système d'exploitation mobile le plus utilisé au monde, devançant Symbian. Désormais, on le retrouve non seulement dans les tablettes et Smartphones, mais aussi dans les téléviseurs, les consoles de jeux, les appareils photos, etc. **[28]**

Figure III.2: HTC Dream le premier Smartphone commercialisé avec le système d'exploitation Android

Les applications Android sont de nature très variables :

- jeux
- mobile commerce
- utilitaire
- service d'information ...

Les applications Android s'obtiennent sur Google Play (Figure III.3.b), anciennement dénommé AndroidMarket (Figure III.3.a).

Figure III.3.a:Ancien logo d'AndroidMarket

Figure III.3.b: Logo de Google Play

Figure III.4: Android-logo

L'écosystème d'Android s'appuie sur deux piliers:

- le langage Java
- le SDK qui permet d'avoir un environnement de développement facilitant la tâche du développeur

Le kit de développement donne accès à des exemples, de la documentation mais surtout à l'API de programmation du système et à un émulateur pour tester ses applications.

III.1 La philosophie et les avantages d'Android [29]

- **Open source**

Le gros point fort d'Android vient du fait qu'il utilise le noyau Linux et est un système libre. Contrairement à Windows ou Mac OSX, vous pouvez à tout moment consulter le code source (qui, une fois compilé, donne l'O.S.), le télécharger, l'adapter… bref, vous avez un véritable droit de regard et de modification (à vos risques et péris) sur la manière dont est fait Android et comment il fonctionne.

- **Gratuit (ou presque)**

Android est gratuit, autant pour vous que pour les constructeurs. S'il vous prenait l'envie de produire votre propre téléphone sous Android, alors vous n'auriez même pas à ouvrir votre porte-monnaie. En revanche, pour poster vos applications sur le Play Store, il vous en coûtera la modique somme de 25$. Ces 25$ permettent de publier autant d'applications que vous le souhaitez, à vie !

- **Facile à développer**

Toutes les API mises à disposition facilitent et accélèrent grandement le travail. Ces APIs sont très complètes et très faciles d'accès. De manière un peu caricaturale, on peut dire que vous pouvez envoyer un SMS en seulement deux lignes de code (concrètement, il y a un peu d'enrobage autour de ce code, mais pas tellement).

- **Facile à vendre**

Le Play Store est une plateforme immense et très visitée ; c'est donc une mine d'opportunités pour quiconque possède une idée originale ou utile.

- **Flexible**

Le système est extrêmement portable, il s'adapte à beaucoup de structures différentes. Les Smartphones, les tablettes, la présence ou l'absence de clavier, différents processeurs... On trouve même des fours à micro-ondes qui fonctionnent à l'aide d'Android ! Non seulement c'est une immense chance d'avoir autant d'opportunités, mais en plus Android est construit de manière à faciliter le développement et la distribution en fonction des composants en présence dans le terminal (si votre application nécessite d'utiliser le Bluetooth, seuls les terminaux équipés de Bluetooth pourront la voir sur le Play Store).

- **Ingénieux**

L'architecture d'Android est inspirée par les applications composites, et encourage par ailleurs leur développement. Ces applications se trouvent essentiellement sur internet et leur principe est que vous pouvez combiner plusieurs composants totalement différents pour obtenir un résultat surpuissant. Par exemple, si on combine l'appareil photo avec le GPS, on peut poster les coordonnées GPS des photos prises.

III.2 L'historique des versions d'Android [30]

Le système de Google n'aurait pas connu un tel succès s'il était resté le même en six ans. C'est là que l'on voit la puissance d'un tel OS qui a su s'adapter aux besoins des utilisateurs à chaque version majeure et qui s'enrichit de nouveautés. La dernière version de la plateforme est maintenant *Android 5.1.1* alias *Lollipop*. (Figure III.5)

Il existait auparavant deux variantes de la plateforme. Une dédiée aux petits écrans principalement les téléphones mobiles (toutes les versions en dessous de 3.0), et une variante dédiée pour les tablettes: *Honeycomb Android 3.0.*

Android 4 ou "*Ice Cream Sandwich*", est sorti *en octobre 2011* elle fusionne les deux variantes pour avoir une plateforme plus versatile et uniforme. C'est la première version qui

combine "*Gingerbread*" et "*Honeycomb*" pour une plateforme à la fois pour les tablettes et les téléphones.

Android 5.0 ou Lollipop cible encore plus d'appareils tel que les smart-watches, les lecteurs pour la télévision, ou dans la voiture. Les appareils avec seulement 512 de mémoire peuvent supporter cette nouvelle version.

Enfin le dernier gros changement concerne le runtime du système. Ainsi Lollipop marque l'abandon de la machine virtuelle Dalvik au profit d'ART (Android Runtime). Avec ce dernier, on nous promet de meilleures performances au niveau général du système. Que de bonnes choses donc pour les utilisateurs qui ont déjà adopté Android 5.0 (ou supérieur) !

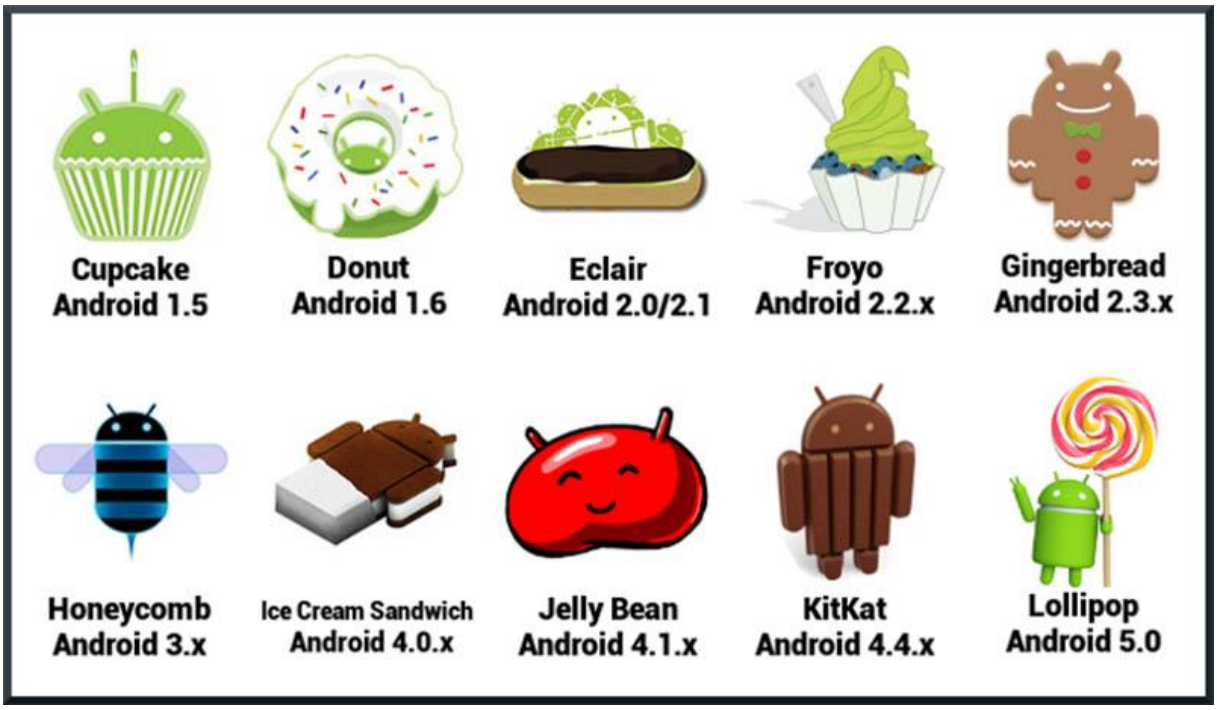

Figure III.5: déférents versions d'Android

III.3.Le marché mondiale des OS mobiles [31]

La domination d'Android sur le marché mondial des Smartphones est indiscutable. Sur l'ensemble de l'année 2014, 1,059 milliard de Smartphones Android ont été livrés dans le monde par les constructeurs. Non seulement ces livraisons ont progressé de 32%, mais surtout elles représentent 81,5% des Smartphones écoulés sur la planète en 2014. Avec iOS, les deux OS mobile ont représenté pas moins de 96,3% de l'ensemble des Smartphones écoulés dans le monde en 2014. C'est plus encore qu'en 2013 (93,8%). Quant aux autres, ils se livrent d'abord une bataille d'arrière-garde. (Figure III.6)

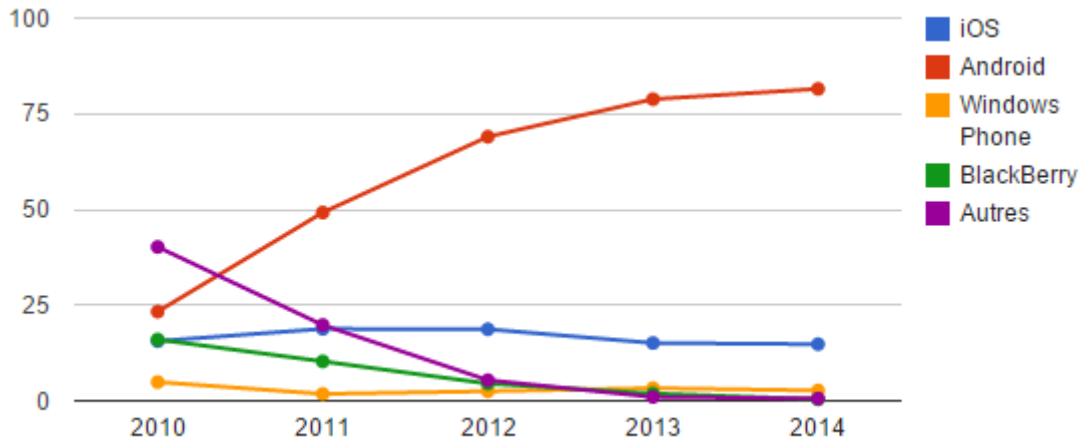

Figure III.6: Part de marché mondiale des OS mobiles (%)

Android est la plate-forme mobile qui a le plus profité de la croissance du marché mondial des Smartphones (+32%). Entre 2011 et 2014, le nombre d'andro-phones est ainsi passé de 243,5 à 1059 millions d'unités. La part de marché d'Android a sur la même période progressé de plus de 30 points, bondissant de 49,2% à 81,5% en 2014.

Android bénéficie de l'entrée de gamme. Pour autant, et malgré une avance confortable, l'écosystème Android connaît quelques évolutions. En raison du fort ralentissement de Samsung en 2014, la croissance des livraisons de Smartphones repose désormais plus sur des constructeurs de taille moindre. Derrière Android et iOS, seul Windows Phone semble encore pouvoir exister. (Figure III.7)

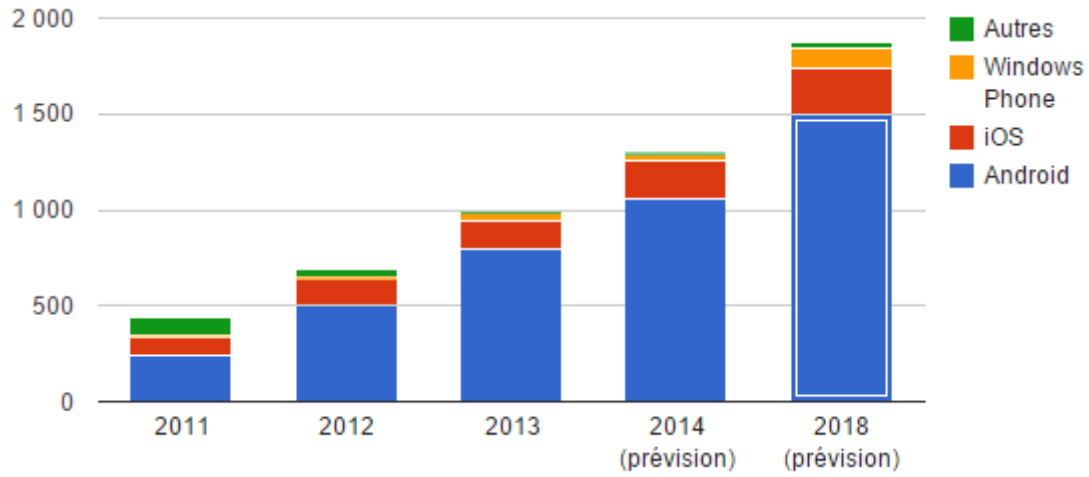

Figure III.7: Répartition par OS des livraisons mondiales de Smartphones

III.4.Les avantages et les inconvénients d'Android

III.4.1. Avantages

- disponibles sur un grand nombre de modèles de téléphones la diversité et le volume des ventes des Andro-phones étant sans limites ;
- une personnalisation et un choix presque illimités ;
- un téléphone globalement plus rapide puisqu'il est dépossédé des surcouches imposées par les constructeurs ;
- des possibilités de sur-cadencement ou de sous-cadencement des composants afin d'obtenir un téléphone plus réactif, plus puissant ou plus autonome que la version originale.
- Certains téléphones ne peuvent pas être mis à jour. Les versions alternatives permettent d'utiliser une version plus récente d'Android afin de rester à jour.

III.4.2.Inconvénients

- le principal reste la stabilité qui peut poser des conflits entre les processus et conduire au redémarrage intempestif du téléphone, ce problème étant de moins en moins fréquent avec Android 4.4
- certaines fonctionnalités sont plus lentes d'autres plus rapides parfois inexistantes (Appareil photo, touches en façade, réactivité de l'écran)
- du fait du grand choix de ROM disponibles, l'utilisateur risque de perdre beaucoup de temps à sélectionner celle qui lui convient le mieux.

IV. Android et la plateforme Java

Android comporte une machine virtuelle nommée Dalvik, qui permet d'exécuter des programmes prévus pour la plate-forme Java. C'est une machine virtuelle conçue dès le départ pour les appareils mobiles et leurs ressources réduites - peu de puissance de calcul et peu de mémoire. En effet les appareils mobiles contemporains de 2011 ont la puissance de calcul d'un ordinateur personnel vieux de dix ans. La majorité, voire la totalité des applications est exécutée par la machine virtuelle Dalvik.

IV.1.Anatomie d'Android (Figure III.8)

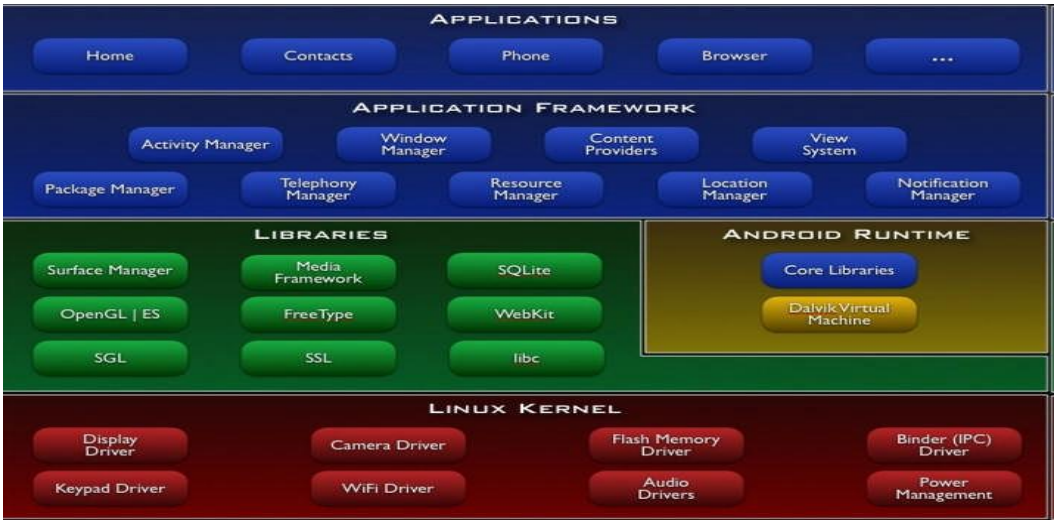

Figure III.8: Anatomie d'Android

- Android est basé sur un kernel linux 2.6.xx.
- Au-dessus de cette couche, on retrouve les librairies C/C++ utilisées par un certain nombre de composants du système Android.
- Au même niveau des librairies, on retrouve l'AndroidRuntime. Cette couche contient les librairies cœurs du Framework ainsi que la machine virtuelle exécutant les applications.
- Au-dessus de la couche "AndroidRuntime" et des librairies cœurs, on retrouve le Framework permettant au développeur de créer des applications. Enfin au-dessus du Framework, il y a les applications. **[32]**

V. Environnement de développement

Android Studio représente la plateforme officielle, soutenue par Google, pour le développement d'applications Android. Il repose sur IntelliJ (Community Edition) de JetBrain et devrait permettre aux développeurs d'être plus rapides et plus productifs. Android Studio 1.0 permet de rationaliser le processus de développement Android. Au premier démarrage, un assistant de configuration installe le SDK Android, met en place les paramètres de votre environnement de développement et crée un émulateur optimisé pour tester vos applications. (Figure III.9)

Figure III.9: logo Android Studio

Android Studio propose entre autres des outils pour gérer le développement d'applications multilingues et permet de visualiser la mise en page des écrans sur des écrans de résolutions variées simultanément. (Figure III.10)

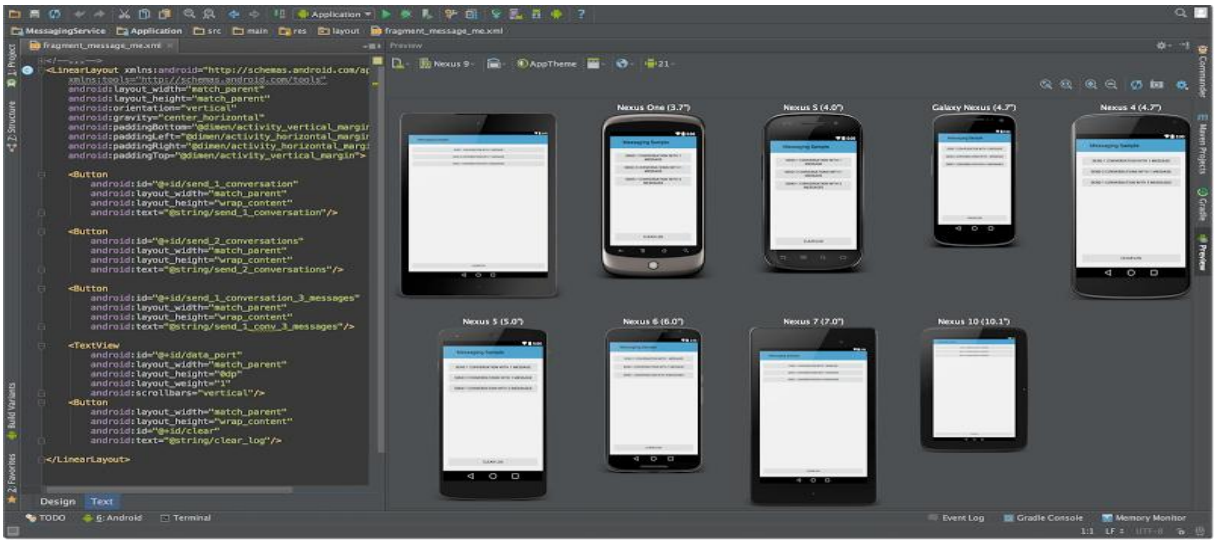

Figure III.10:interface Android Studio avec plusieurs écrans de résolutions différentes

V.1. Les éléments d'une application

Une application Android peut être composée des éléments suivants:

- des activités (android.app.Activity): il s'agit d'une partie de l'application présentant une vue à l'utilisateur
- des services (android.app.Service): il s'agit d'une activité tâche de fond sans vue associée

- des fournisseurs de contenus (android.content.ContentProvider): permettent le partage d'informations au sein ou entre applications
- des widgets (android.appwidget.*): une vue accrochée au Bureau d'Android
- des Intents (android.content.Intent): permettent d'envoyer un message pour un composant externe sans le nommer explicitement
- des récepteurs d'Intents (android.content.BroadcastReceiver): permettent de déclarer être capable de répondre à des Intents
- des notifications (android.app.Notifications): permettent de notifier l'utilisateur de la survenue d'événements.

VI. Développement de SecureSMS

Dans cette section on va présenter notre application pour assurer la sécurité des SMS dans un Smartphone Android.

Cette application a comme objectif la sécurisation des SMS a la fois dans le portable de l'utilisateur et pendant leur transfert dans le réseau GSM a travers le monde.

Le fonctionnement de l'application se base sur l'utilisation de l'API cryptographique de Android afin d'encrypter et décrypter le texte des SMS et cela en utilisant des algorithmes cryptographique tel que AES ou DES « dans notre cas on a utilisé AES » avec des clefs cryptographiques allant de 128 à bits et cela pour assurer une haute sécurité.

VI.1. Fonctionnement de l'application

Le fonctionnement de l'application se compose en deux phases :

Les deux correspondants se mettent d'accord sur une secret pour générer les clefs cryptographiques, ce secret est une phrase de 16 caractère et elle est demandée par l'application pour générer les clefs cryptographiques utilisée ultérieurement pour crypter et décrypter les SMS. Cette phrase peut être transférer de n'importe qu'elle façon dont les correspondant voient sécurisé.

La deuxième phase est l'utilisation de l'application pour crypter et décrypter les SMS et cela en demandant à l'utilisateur d'entrer la phrase secrète pour envoyer ou lire un SMS crypté. (Figure III.11)

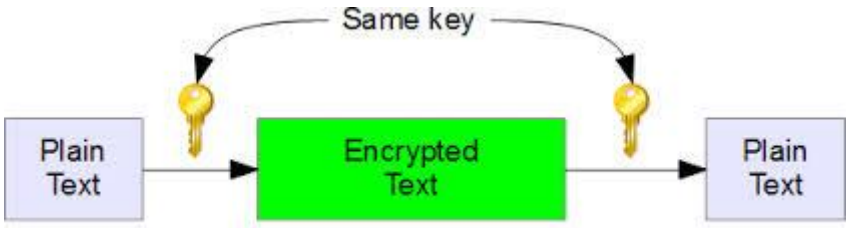

Figure III.11: Principe de fonctionnement

VI.2. Envoie des SMS

L'application est composée de diverses interfaces graphiques donnant à l'utilisateur toutes les fonctionnalités nécessaires pour envoyer ou recevoir des SMS.

La première interface donne a l'utilisateur le choix entre l'envoie des SMS cryptés ou en claire, et cela pour permettre a notre application d'être utilisée dans les deux cas et ne pas limiter son utilisation pour les SMS crypté. (Figure III.12)

Figure III.12: Interface principale

Si l'utilisateur choisie d'envoyer un SMS en claire, une autre interface « activité » s'affiche lui donnant la possibilité de saisir le numéro de téléphone du correspondant et le message et un bouton pour lancer l'opération d'envoie du SMS. (Figure III.13)

Figure III.13: Interface de l'activité "envoyer_en_clair "

Cette interface contienne deux zones de texte (Numéro et Message) et deux Boutons (Envoyer et Retour)

- Le premier zone de texte pour entrée le numéro de correspondant.
- Le deuxième pour écrire le message.
- Le Bouton "**Envoyer**" permet d'envoyer le message en clair.
- Le Bouton "**Retour**" permet de reculer à l'interface principale.

Dans le cas ou l'utilisateur veux envoyer des SMS cryptés, il va choisir la deuxième option « envoyer crypté » cette option doit être exécuté après que les deux correspondants se mettent d'accord sur une phrase secrète pour générer les clefs cryptographiques.

Dans cette activité l'utilisateur sera demandé d'introduire la phrase secrète ainsi que le numéro de son correspondant et le message. Le lancement de l'envoie sera exécuté après l'activation du bouton envoyer. (Figure III.14)

Figure III.14 : Interface de l'activité "crypter"

Cette interface est constitué de trois zones de texte (numéro, mot de passe et message) et deux bottons (envoyer et retour)

- Le premier zone de texte pour entrer le numéro de correspondant.
- Le deuxième de texte pour entrer le mot de passe.
- La troisième zone de texte pour écrire le message.
- Le Bouton" **Envoyer**" permet d'envoyer le message crypté.
- Le Bouton "**Retour**" permet de reculer à l'interface principale.

VI.3. Réception des SMS

La réception des SMS s'effectue de manière habituelle en entrant a la boite de réception dans laquelle s'affiche la liste de tous les SMS « cryptés ou non » . (Figure III.15)

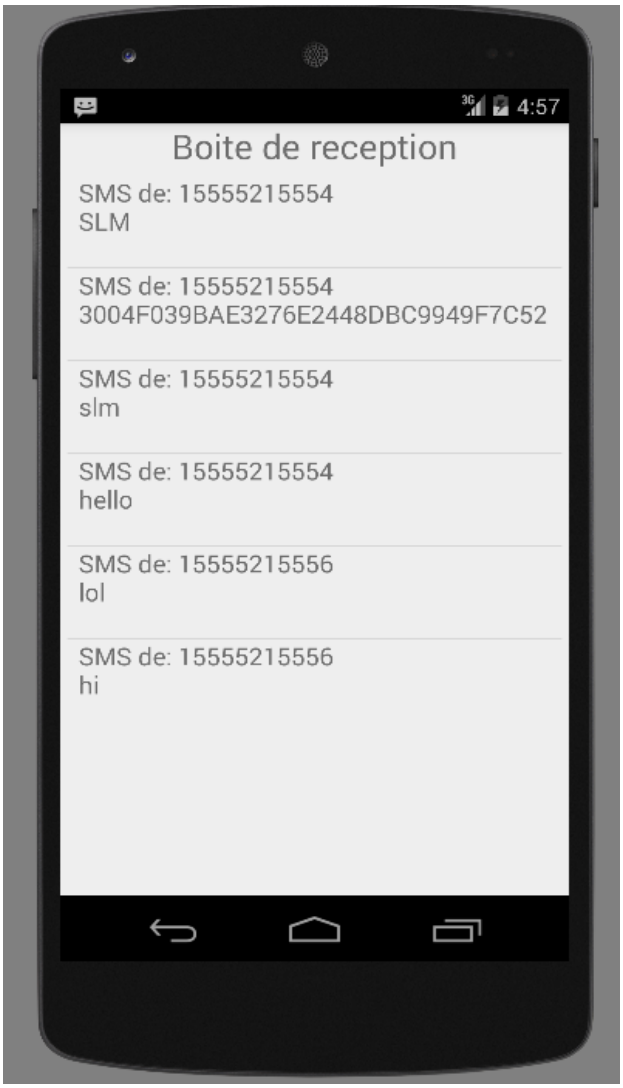

Figure III.15: Interface boite de réception

L'utilisateur peut ouvrir n'importe quel SMS « cryptés ou non » dans le cas ou le SMS est en claire, l'utilisateur lit ce SMS sans aucun problème, dans le cas contraire il constate que le SMS est crypté il va choisir l'option de le décrypté, il va être demandé a introduire la phrase secrète « outil pour générer les clefs cryptographiques » et par la suite lancer l'opération de décryptage qui décrypte et affiche le message. (Figure III.16)

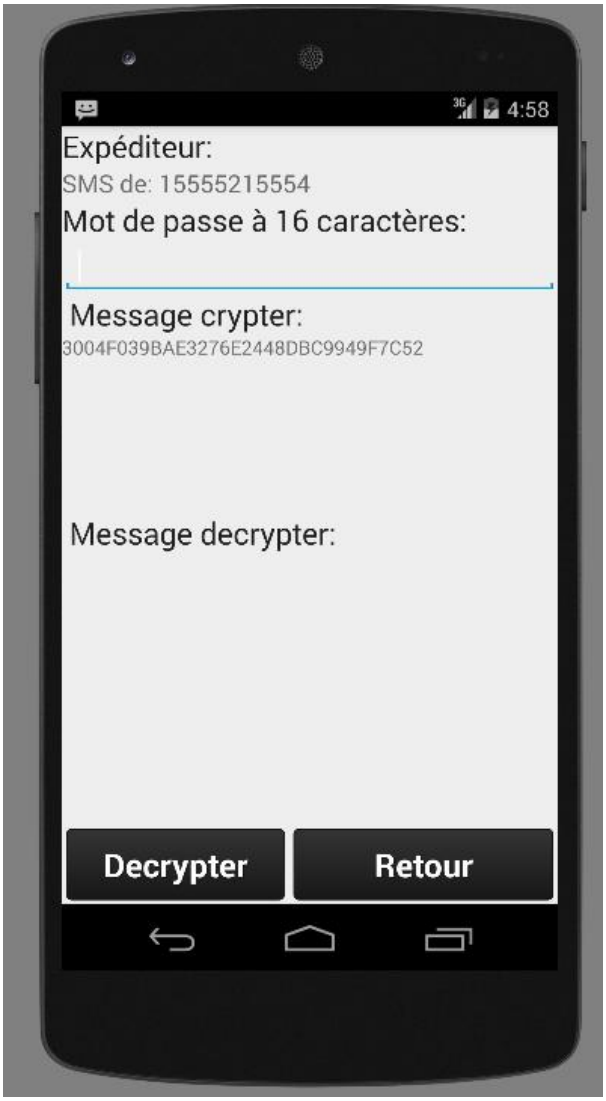

Figure III.16: Interface de l'activité décrypter

Cette interface contienne le numéro de la source, trois zones de texte (mot de passe, message crypter et message décrypter) et deux Boutons (décrypter et retour)

- Le premier zone de texte pour saisir le mot de passe équivalent a celui de cryptage.
- Le deuxième zone texte affiche le message crypté.
- Le troisième zone de texte affiche le message décrypté.

- Le Bouton "**Décrypter**" pour déchiffrer le message cryptera l'aide de mot de passe saisie.
- Le Bouton "**Retour**" permet de reculer a l'interface précédente (boite de réception)

VII. Conclusion

Dans ce dernier chapitre nous avons présenté notre application SecureSMS qui sert comme outil pour s'échanger des SMS cryptés a travers le réseaux GSM. Cette application est semblable aux applications habituelles dans lecture et l'envoie des SMS seulement qu'elle donne la possibilité de crypter et décrypter les SMS. L'algorithme utilisé est l'AES qu'est reconnu comme un outil puisant pour la cryptographie est utilisé comme standard cryptographique dans le monde.

CONCLUSION GENERALE

Conclusion générale

Le protocole de communication pour la téléphonie mobile, GSM, est encore très utilisé à travers le monde. Malheureusement c'est un système vieillissant, reposant sur des algorithmes de chiffrements obsolètes qui ne permettent pas de garantir aux abonnées une parfaite confidentialité de leurs communications.

Notre projet s'intègre dans cette perspective pour réaliser un crypto-système avec un algorithme plus puissant que ces algorithmes du GSM, dans le but d'assurer la confidentialité de nos SMS à travers le réseau GSM.

Pour aboutir à ces objectifs, nous avons exploité les technologies avancées des nouveaux mobiles présents sur le marché. Particulièrement, la technologie ANDROID sur laquelle a été développée notre application.

Cette expérience a été une occasion pour nous familiariser avec les notions de l'informatique embarquée sur les terminaux mobiles. De plus, nous avons approfondi nos connaissances dans le développement orienté objet à base du langage JAVA et la programmation des applications mobile ANDROID. Nous avons programmé une application qui permet l'échange des SMS en clair ou bien crypté à l'aide de l'algorithme cryptographie symétrique AES.

REFERENCES BIBLIOGRAPHIQUES

Références

[1] www.radio-electronics.com/.../ GSM architecture

[2] www.technologuepro.com/gsm/chapitre_2

[3] ETSI, GSM Specification series 03.01-3.88. "GSM PLMN Functions". Architecture, Numbering and addressing procedures.

[4] ETSI. GSM Specification series 04.01-4.88. "MS-BSS Interface"

[5] ETSI, GSM Specification series 08.01-8.60. "BSS-MSC Interface". BSC-BTS Interface.

[6] www.conseilsmarketing.info/SMS-Marketing.html.

[7] ETSI, ETS TS 300 901, Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (GSM 03.40 version 5.8.1 Release 1996).

[8]ETSI, ETSI TS 100 902, Digital cellular telecommunications system (Phase 2+); Technical Realization of Short Message Service Cell Broadcast (SMSCB) (3GPP TS 03.41 version 7.4.0).

[9] Sécurité Mobile 2G, 3G et 4G : Concepts, Principes et Architectures, http://www.efort.com

[10] http://www.commentcamarche.net/contents/203-cryptographie

[11] Pierre BARTHELEMY, "IML - UPR 9016 CNRS'', Campus de Luminy - Case 907 13288 MARSEILLE Cedex 9 - FRANCE , 2000

www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/des **[12**]

[13] http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/aes

[14] http://www.uqtr.uquebec.ca/~delisle/Crypto/prives/flux_rc4.php

[15] http://sebsauvage.net/comprendre/encryptage/crypto_dh.html

[16] http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/rsa

[17] EURONEXT PARIS: *France Telecom.* Article publié sur Internet http://www.euronext.com/

[18] Ghislaine Labouret, " introduction a la cryptographie'', support de cours du cabinet HSC

[19] https://www.securiteinfo.com/cryptographie/pki.shtml

[20] http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/pgp

[21] http://cartunelo.akendewa.net/les-operateurs-de-telephonie-nous-espionnent-ils/

[22] http://www.espionner-un-portable.fr/espionner-les-sms.html

[23] http://www.phonandroid.com/la-nsa-intercepte-200-millions-de-sms-chaque-jour-dans-le-monde.html

[24] Magazine Pirate Informatique N7- Novembre 2010

[25] http://www.phonandroid.com/auroragold-comment-nsa-espionne-telephones-depuis-2011.html

[26] http://blog.needeo.com/2011/07/lutilite-de-developper-une-application-mobile

[27] marketing-webmobile.fr

[28]http://mob-core.com/fr/articles/410-istorija-android.html

[29] Créer des applications Android par Frédéric Espiau(Apollidore)

http://www.phonandroid.com/toute-l-histoire-et-la-chronologie-d-android-dossier.html
[30]

[31] http://www.zdnet.fr/actualites/chiffres-cles-les-os-pour-smartphones-39790245.htm

[32] Source Telecom Valley - Jeudi 2 Juillet 2009 -

[33] http://www.developpez.com/actu/78841/Android-Studio-disponible-en-version-1-0-Google-lance-son-nouvel-EDI-dedie-au-developpement-Android

Résumé :

L’utilisation des réseaux GSM comme moyen de communication a devenu dans les deux dernières décennies indispensable, vu le nombre important des services offerts ainsi que la possibilité de mobilité dans le monde entier. Le service SMS est un des services de GSM mais son utilisation comme support de secret important reste condamné par la possibilité d’espionnage pour cela nous avons développé une application Android permettant d’assurer la sécurité des SMS dans le mobile de l’utilisateur ainsi que dans son transfert dans le réseau GSM. La sécurité des SMS dans cette application est basée sur l’utilisation de l’AES connu comme le standard le plus performant pour chiffrer les données.

The use of GSM networks as a tool of communication has become in the last two decades essential, given the opportunity to a large number of services as well as the possibility of mobility worldwide. The SMS service is the most known GSM service but its use for important secret remains convicted of spying. In our work we have developed an android application that can ensure the safety of SMS in user’s mobile as well as its transfer in the GSM network. The security of SMS in this application is based on the use of AES algorithm known as the most powerful standard to data encryption.

استخدام شبكات GSM كأداة للتواصل أصبح في العقدين الأخيرين الأساسي، ونظرا للفرص لعدد كبير من الخدمات، فضلا عن إمكانية التنقل في جميع أنحاء العالم. خدمة الرسائل القصيرة هي الأكثر شهرة في عالم تكنولوجيا الإعلام والاتصالات و لكن كوسيلة لنقل معلومات سرية هامة فهي عرضة للتجسس. في عملنا قمنا بتطوير تطبيق يمكنه تأمين سرية SMS على المحمول المستخدم وكذلك عبر شبكة GSM. ويستند أمن SMS في هذا التطبيق على استخدام خوارزمية AES.