MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTROTECTHNIQUE

Mémoire de fin d'études

Présenté en vue de l'obtention
Du diplôme d'ingénieur d'état en électrotechnique

OPTION : Contrôle

Thème:
Gestion de la sécurité du réseau GSM application de l'algorithme A5

Dirigé par :
LAHDIR MOURAD

Etudié par
Mr: SLIMI ABDENOUR
Mr: LOUNICI ALI

Promotion **2008**

Dédicaces

Je dédie ce modeste travail à :

-A mes très chers parents.

-A toute ma famille.

-A tous mes amis.

Ali

Dédicaces

Je dédie ce modeste travail à :

-A mes très chers parents.

-A mes frères.

-A toute ma famille.

- A Tous mes amis.

-A mon ami Abdellah

-A Tous ceux qui me connaissent.

Abdenour

REMERCIEMENTS

Nous tenons à remercier vivement notre promoteur M^R LAHDIR pour nous avoir proposé ce sujet, pour la qualité de son encadrement, et son suivi durant toute la durée du projet.

Nous remercions chaleureusement les membres du jury pour l'honneur qu'ils nous font en acceptant de juger ce mémoire de fin d'études.

Enfin, nous remercions toutes les personnes ayant contribué de prés ou de loin au bon accomplissement de notre travail.

Sommaire

Chapitre II : Les mécanismes de sécurité du réseau GSM

ChapitreIII : L'authentification et chiffrement dans le réseau GSM

Chapitre IV : Application de l'algorithme de chiffrement A5

Introduction générale

Les scientifiques du monde entier font, de jour en jour ; progresser les sciences et les technologies actuelles. Les rêves technologiques des humaines n'ont presque plus de limites.

Le GSM (Global System Mobile) est né de cette avancée technologique extraordinaire, avancée dont on ne pouvait au préalable prévoir son impact sur le mode de vie des gens.
Le système GSM est maintenant opérationnel et largement utilisé, ce système est la première norme de téléphonie cellulaire numérique. Il a connu beaucoup de succès, mais l'utilisation d'un canal radio rend les communications plus vulnérables aux écoutes et aux utilisations frauduleuses.

Le réseau GSM a donc recours aux procèdes de sécurité en l'occurrence l'authentification et le chiffrement, le premier permet à l'abonné d'accéder au système grace à l'algorithme A3 ; le deuxième consiste à chiffrer la communication par l'algorithme A5 , après avoir généré la clé de chiffrement par l'algorithme A8.

L'algorithme de chiffrement A5 recouvre en fait de deux algorithmes différents : A5/1 dit «fort» réservé à la Communauté Européenne et à l'Amérique du NORD

A5/2 dit «faible» réserve au reste du monde

Le design de s'est deux algorithmes n'a pas été rendu public, mais obtenu grâce à du

« *reverse enginering* » par Marc Briceno et Ian Goldberg en 1998.

La sécurité offerte par le réseau GSM est assurée par les protocoles de sécurité (L'authentification et chiffrement), Bien qu'ils soient complexes et sécurisants n'empêche pas de proposer d'autres protocoles pour l'améliorer.

Dans ce mémoire, nous présentons au premier chapitre les généralités sur le réseau GSM, qui décrit l'architecture du réseau GSM afin de connaître le fonctionnement des différents équipements ainsi que leurs emplacements dans le réseau, le deuxième chapitre traite d'une manière générale les mécanismes de sécurité GSM en l'occurrence l'authentification et le chiffrement en passant par le protocole de la mise à jour de la localisation ainsi que la numérotation liée à l'abonné ; alors que dans le troisième chapitre, nous expliquons en détaille les processus d'authentification et de chiffrement. Puis On termine par une application sur l'algorithme A5 (A5/1et A5/2).

I- Introduction

Parmi les systèmes radios de communications mobiles, le GSM en particulier, est aujourd'hui à la tète des systèmes cellulaires numériques, très répandu dans le monde, il offre un très grand nombre de services, et permet l'échange d'information entre deux ou plusieurs usagers avec une qualité raisonnable.

II. Architecture du réseau GSM :

L'architecture d'un réseau GSM est divisée en trois sous-systèmes :

1) Le sous-système radio contenant la station mobile, la station de base et son contrôleur.
2) Le sous-système réseau ou d'acheminement.
3) Le sous-système opérationnel ou d'exploitation et de maintenance

Ces différents sous-systèmes sont référencés à la figure I.1.

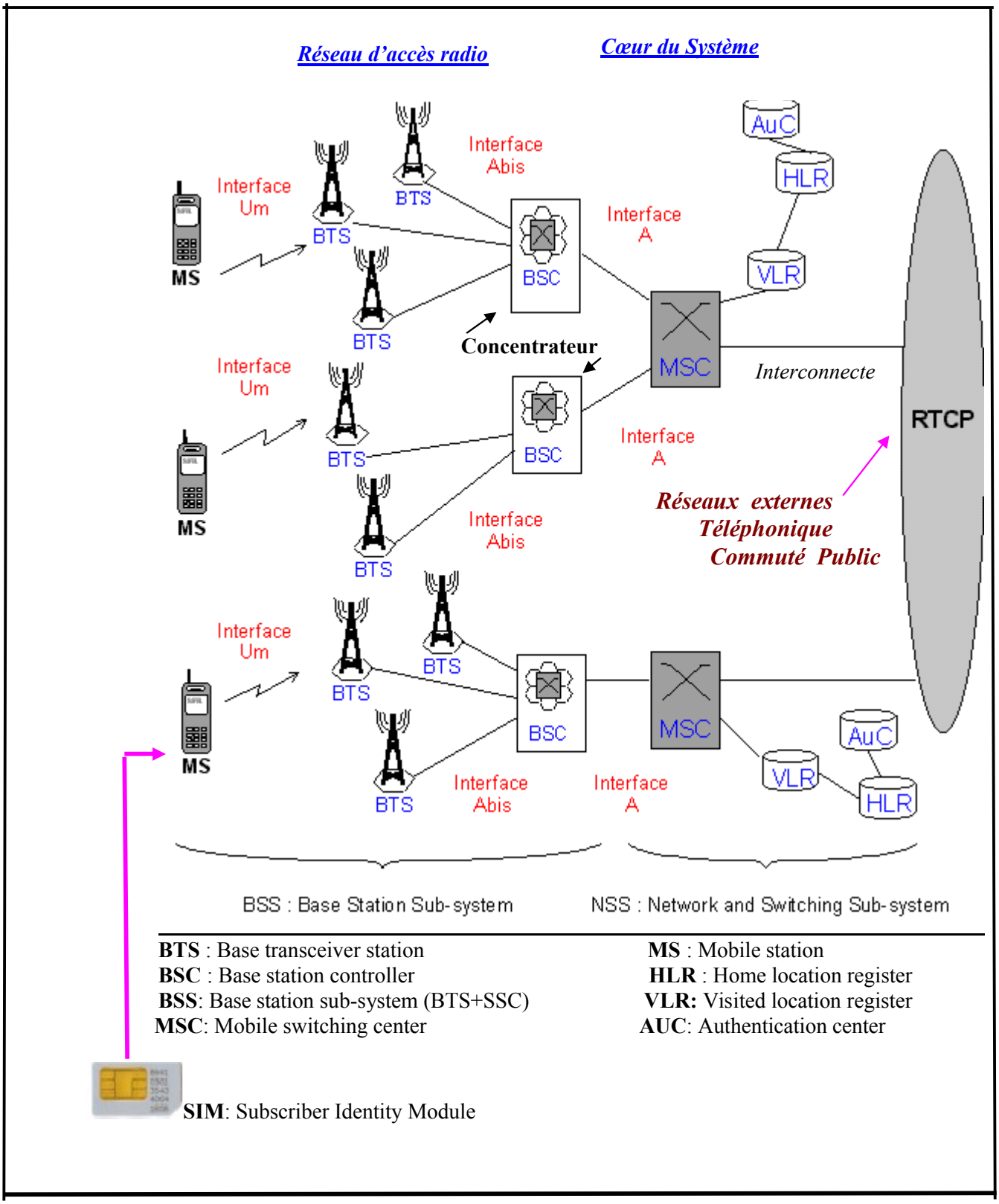


Fig.I.1 : Architecture réseau GSM

II.1. Le sous-système radio :

Le sous-système radio gère la transmission radio. Il est constitué de plusieurs entités dont le mobile (**MS**), la station de base (**BTS**, Base Transceiver station) et un contrôleur de station de base (**BSC**, Base station controller).

II.1.1. La station mobile :

La station mobile est constituée du téléphone portable et d'une carte SIM(Subscriber Identity Module). Ces deux éléments suffisent à réaliser l'ensemble des fonctionnalités nécessaires à la transmission et à la gestion des déplacements.
La principale fonction de la carte SIM est de contenir et de gérer une série d'informations de l'abonné. Elle se comporte donc comme une mini-base de données.

Paramètres	Commentaires
Données administratives	
PIN/PIN2	Mot de passe demandé à chaque connexion
PUK/PUK2	Code pour débloquer une carte
Language	Langue choisie par l'utilisateur
Données liées à la sécurité	
Clé K_i	Valeur unique, connue de la seule carte SIM et du HLR
CKSN	Séquence de chiffrement
Données relatives à l'utilisateur	
IMSI	Numéro international de l'abonné
MSISDN	Numéro d'appel d'un téléphone GSM
Données de "roaming"	
TMSI	Numéro attribué temporairement par le réseau à un abonné
Location updating status	Indique si une mise à jour de la localisation est nécessaire
Données relatives au réseau	
Mobile Country Code (MCC), Mobile Network Code (MNC), etc	Identifiants du réseau mobile de l'abonné
Numéros de fréquence absolus	Fréquences utilisées par le PLMN

Tableau1: le contenu de la carte SIM

L'identification d'un mobile s'effectue exclusivement au moyen de la carte SIM.

En effet, elle contient des données spécifiques comme le code PIN (Personal Identification Number) et d'autres caractéristiques de l'abonnée, de l'environnement radio et de l'environnement de l'utilisateur.

L'identification d'un utilisateur est réalisée par un numéro unique IMSI (International Mobile Subscriber Identity) différant du numéro de téléphone connu de l'utilisateur (MSISDN), tous les deux étant incrustés dans la carte SIM

II.1.2. La station de base (BTS) :

La station de base est l'élément central, que l'on pourrait définir comme un ensemble émetteur/récepteur. Dans le réseau GSM, chaque cellule principale au centre de laquelle se situe une station base peut-être divisée, grâce à des antennes directionnelles, en plus petites cellules qui sont des portions de celle de départ et qui utilisent des fréquences porteuses différentes. C'est la station de base qui fait le relais entre le mobile et le sous-système réseau.

Fig.I.2: BTS

II.1.3. Le contrôleur de station de base (BSC):

Le contrôleur de station de base gère une ou plusieurs stations de base et communique avec elles par le biais de l'interface A-bis. Ce contrôleur remplit différentes fonctions tant au niveau communication qu'au niveau exploitation.

Pour les fonctions de communications, le BSC agit vis-à-vis du trafic abonné venant des stations de base comme un concentrateur puisqu'il véhicule les communications provenant des différentes stations de base. Dans l'autre sens, le contrôleur commute les données en les dirigeant vers la bonne station de base.

II.1.4. Le concept cellulaire :

Le principe du système cellulaire est de diviser le territoire en petites zones, appelées cellules, et de partager la ressource radio entre celles-ci. Comme précédemment, ces fréquences ne peuvent pas être utilisées dans les cellules adjacentes afin d'éviter les interférences. Ainsi, on définit des motifs, appelés motifs ou **clusters,** constitués de plusieurs cellules, dans lesquels chaque fréquence est utilisée une seule fois.

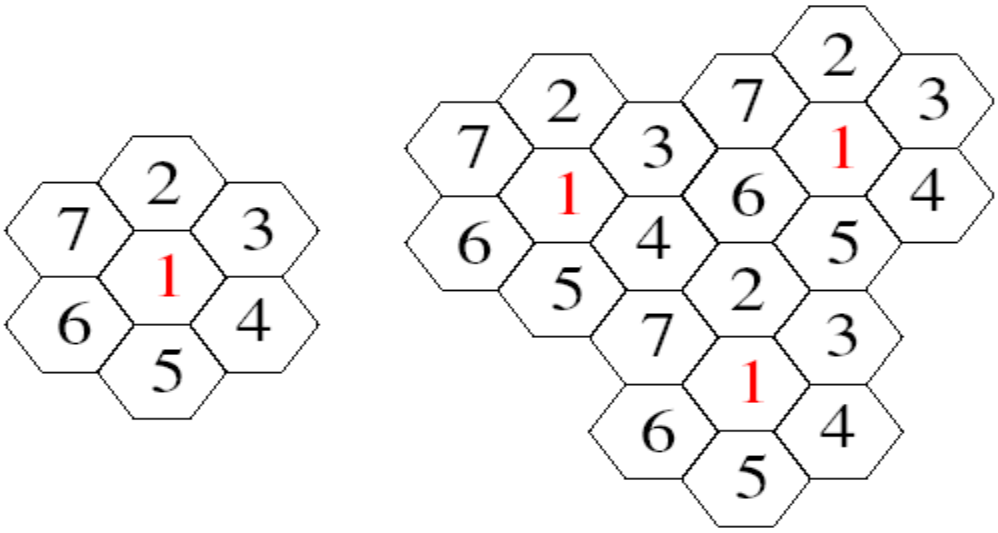


Fig.I.3:Cellules GSM

Une cellule se caractérise :

- Par sa puissance d'émission, ce qui se traduit par une zone de couvertures à l'intérieure de laquelle le niveau du champ électrique est supérieur à un seuil déterminé.

- Par la fréquence de porteuse utilisée pour l'émission radioélectrique.
- Par le réseau auquel elle est interconnectée.

Il faut noter que la taille des cellules n'est pas la même sur tous le territoire. En effet, celle-ci dépend :

- Du nombre d'utilisateurs potentiels dans la zone.
- De la configuration du terrain (plateau, montagnes,..).
- De la nature des constructions (maisons, pavillons, immeubles en bétons,…).
- De la localisation (rurale, suburbaine ou urbaine).

II.2. Le sous-système réseau :

Le sous-système réseau est l'interface entre le réseau téléphonique public commuté et les BSC. Il est constitué de commutateurs et de bases de données utilisateurs.

Le NSS est constitué de :

- Mobile Switching Center (MSC).
- Home Location Register (HLR)/Authentication Center (AuC).
- Visitor Location Register (VLR).
- Equipment Identity Register (EIR).

II.2.1. Le centre de commutation mobile (MSC) :

Cet élément peut être considéré comme le cœur d'un système cellulaire puisqu'il fait la gestion des appels et de tout ce qui est lié à l'identité des abonnés, à leur enregistrement et à leur localisation. Ce centre est relié au sous-système radio via l'interface A.

Les MSC servant de passerelle (Gateway Mobile Switching Center, GMSC) sont placées en périphérie du réseau d'un opérateur de manière à assurer une interopérabilité entre réseaux d'opérateurs.

Fig.I.4: MSC.

II.2.2. L'enregistreur de localisation nominale (HLR):

Il gère toutes les informations concernant les abonnés au réseau (numéro de l'utilisateur, numéro réseau d'un abonné, profil de l'abonnement,…) cette base de données gère également la position courante de l'abonné puisqu'elle enregistre le numéro de la zone de localisation où il se trouve. Il y a une HLR par opérateur.

Les données dynamiques sont mises à jour par le MSC. Cette base de données est souvent unique pour un réseau GSM et seules quelques personnes y ont accès directement.

II.2.3. Le centre d'authentification (AuC):

Lorsqu'un abonné passe une communication, l'opérateur doit pouvoir s'assurer qu'il ne s'agit pas d'un usurpateur. Le centre d'authentification remplit cette fonction de protection des communications. Pour ce faire, la norme GSM prévoit deux mécanismes :

1. Le chiffrement des transmissions radio. Il s'agit d'un chiffrement faible, qui ne résiste pas longtemps à la crypto-analyse.
2. L'authentification des utilisateurs du réseau au moyen d'une clé Ki qui est à la fois présente dans la station mobile et dans le centre d'authentification.

II.2.4. L'enregistreur de localisation des visiteurs (VLR) :

Cette base de données contient temporairement des informations sur les abonnés qui visitent une région desservie par un MSC. Ces informations proviennent du HLR dont l'abonné est enregistré et indiquent les services auxquels l'abonné a droit. Il est à noter que le VLR est toujours associé à un MSC.

II.2.5. L'enregistreur des identités des équipements (EIR) :

Malgré les mécanismes introduits pour sécuriser l'accès au réseau et le contenu des communications, le téléphone mobile doit potentiellement pouvoir accueillir n'importe quelle carte SIM de n'importe quel réseau. Il est donc imaginable qu'un terminal puisse être utilisé par un voleur sans qu'il ne puisse être repéré.

Pour combattre ce risque, chaque terminal reçoit un identifiant unique (International Mobile Station Equipement Identity, IMEI) qui ne peut pas être modifié sans altérer le terminal. En fonction de données au sujet d'un terminal, un opérateur peut décider de refuser l'accès au réseau. Tous les opérateurs n'implémentent pas une telle base de données.

II.3. Le centre d'exploitation et de maintenance :

Cette partie du réseau regroupe trois activités principales de gestion :

- La gestion administrative.
- La gestion commerciale.

- La gestion technique.

Le réseau de maintenance technique s'intéresse au fonctionnement des éléments du réseau.

Il gère notamment les alarmes, les dysfonctionnements, la sécurité,…ce réseau s'appuie sur un réseau de transfert de données, totalement dissocié du réseau de communications GSM.

III.1.Les Régions géographiques d'un réseau GSM :

La figure.I.5 illustre les différentes zones géographiques auxquelles, on peut relier un réseau GSM.

Une cellule correspond à la région couverte par une station de base (BTS).

Une région de repérage (LA – Location Area) est un groupe de cellules. C'est la région Par laquelle on localise un abonné. Chaque LA est servi par un ou plusieurs contrôleurs de station de base (BSC), mais par un seul MSC.

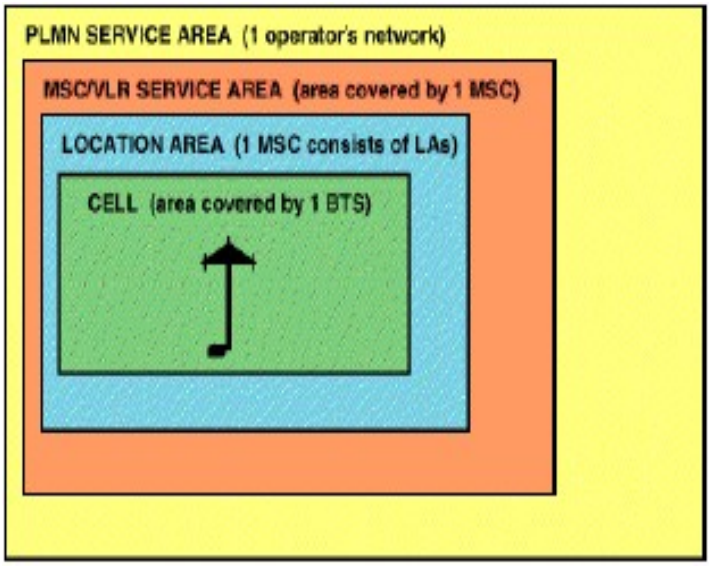


Fig.I.5: zones géographiques du GSM.

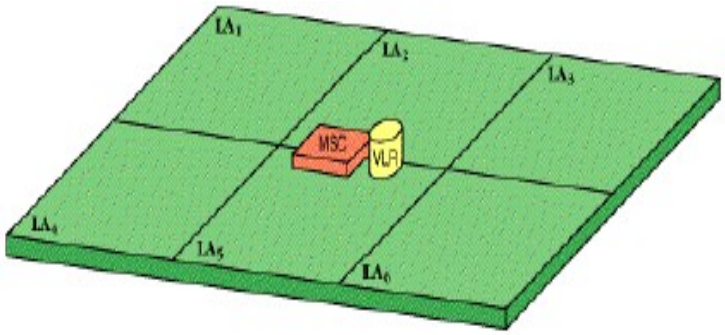


Fig.I.6:région de service.

Une région de service MSC/VLR est un groupe de LA sous le contrôle d'un seul MSC.I.

La figure suivante illustre un ensemble de régions de services MSC/VLR.

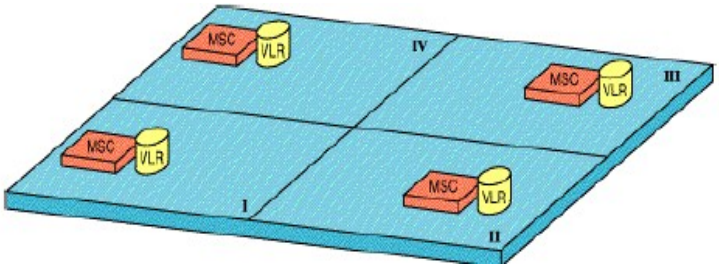


Fig.I.7: ensemble de région de service.

III.2.Présentation des interfaces :

Les interfaces sont des protocoles permettant la communication entre les différentes structures du réseau GSM.

III.2.1.Interfaces entre les entités du réseau :

III.2.1.1.L'interface radio (Um) :

L'interface radio, encore appelée l'interface Air ou elle est localisée entre le terminal (la station mobile) et la station de base (BTS). C'est elle qui permet à tout mobile de communiquer dans la totalité du réseau GSM.

III.2.1.2. Les interfaces A-bis :

L'interface A-bis est localisée entre la station de base (BTS) et le contrôleur de station de base (BSC).

Les différentes fonctions mises en œuvre sur cette interface sont :

- Le trafic de la parole et de données.
- La signalisation entre BTS et BSC.
- Le transport d'informations de synchronisation vers la BTS

III.2.1.3.L'interface A :

Entre BTS et BSC, elle est utilisée pour le transport du trafic et des donnés de signalisation. Le sous système radio et le sous système réseau se communiquent par l'intermédiaire l'interface A.

III.2.1.4.L'interface X25 :

L'interface X25 relie le BSC au centre d'exploitation et de maintenance (OMC). Elle possède une structure en 7 couches du modèle OSI.

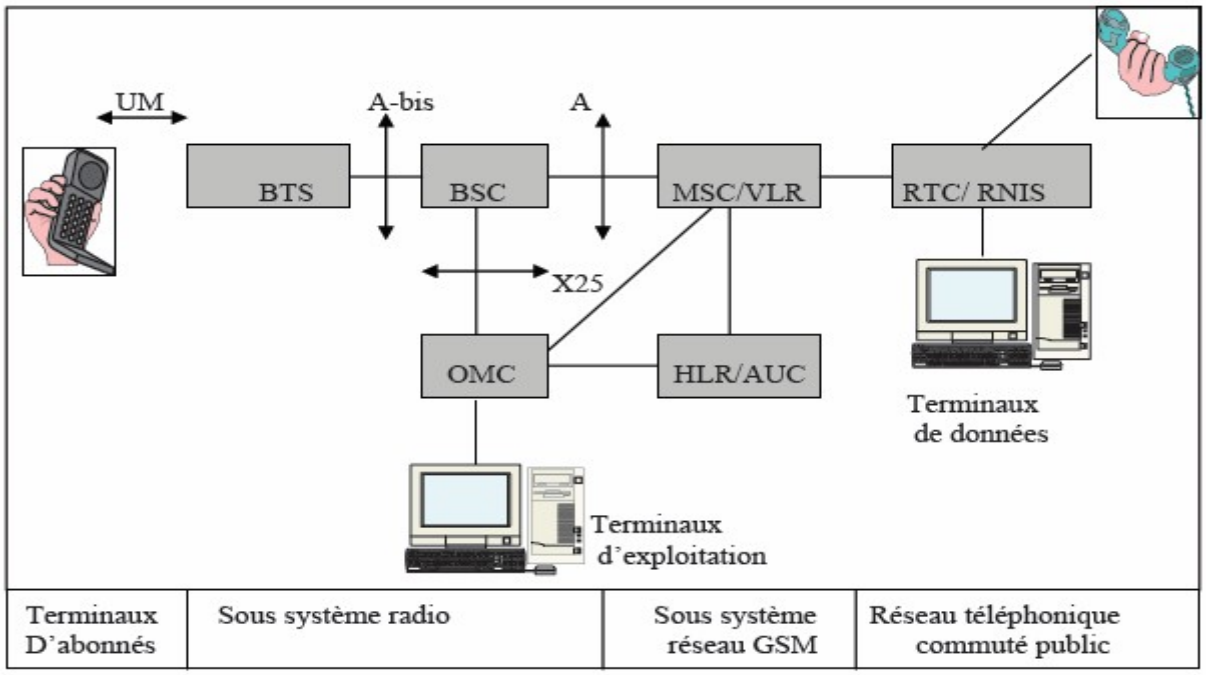


Fig.I.8 : Les interfaces dans le réseau GSM

III.3.Architecture en couche de réseau GSM :

La couche1 :C'est la physique ; elle défini l'ensemble des moyens physiques de transmission et de réception de l'information (A-bis, MIC Um : gestion du multiplixage, codage correction d'erreurs, mesures radio).

La couche2 : c'est la liaison .Elle a pour objet de fiabiliser la transmission entre deux équipements par un protocole (LAPD et LAPDmobile).

La couche3 : C'est la couche réseau .Elle établit, maintient et libère les circuits commutés. Elle se divise en 3 sous couches:

- **La sous-couche RR** : Elle intègre l'ensemble des aspects purement radio. Elle gère l'établissement, la maintenance et la libération des différents canaux logiques.La connexion RR s'établit entre MS et BSC.
- **La sous-couche MM :** Elle permet de gérer **le** caractère mobile de l'abonné. Cette sous couche prend en charge la localisation, l'authentification et l'allocation du TMSI.

  La connexion MM s'établit entre MS et MSC.
- **La sous- couche CM** : Elle gère les connexions entre MS et MSC. Elle est scindée en 3 parties :

  * CC (Call Center) : Gestion des connexions.

  * SMS (Short Message Servie) : transmission et réception de message Courts.

  * SS (Supplementary Service) : Gestion des services supplémentaires. La Connexion CM s'établit entre MS et MSC.

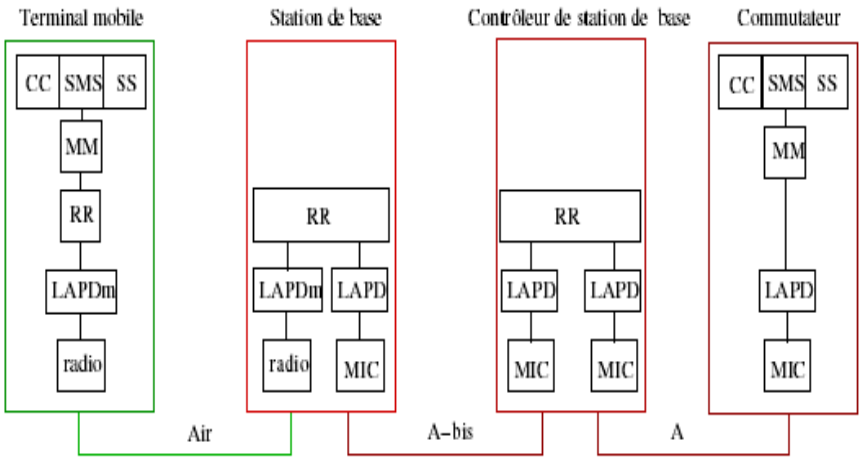


Fig.I.9 : piles de protocoles de différents sous-systèmes du réseau GSM

IV. Technique de multiplexage :

Dans un réseau GSM, deux techniques de multiplexage sont mises en oeuvre: le multiplexage **fréquentiel** FDMA (Frequency Division Multiple Acces) et le multiplexage **temporel** TDMA (Time Division Multiple Acces).

IV.1. Multiplexage fréquentiel :

Dans sa version à 900 [*MHz*], la norme GSM occupe deux bandes de 25 [*MHz*]; l'une est utilisée pour la voie montante (890, 915 [*MHz*]), l'autre pour la voie descendante (935, 960 [*MHz*]). Il est également défini que chaque porteuse de cellule possède une densité spectrale confinée dans une bande de 200 [*kHz*] ce qui signifie que, théoriquement, on peut disposer de 124 canaux. Notons au passage que la bande de fréquences du DCS-1800 étant plus large, elle peut contenir 374 canaux.

Aussi, si on indique par F_u les fréquences porteuses montantes et par F_d les fréquences porteuses descendantes, les valeurs de fréquence porteuse valent

$$\mathbf{Fu\ (n) = 890 + 0{,}2 \times (n - 1)\ [MHz]\ .}$$

$$\mathbf{Fd\ (n) = 935 + 0{,}2 \times (n - 1)\ [MHz].} \qquad \mathbf{Ou\ 1 \leq n \leq 124}$$

Tant pour des questions d'interférences électromagnétiques que pour des raisons d'augmentation de capacité, le multiplexage fréquentiel se double d'un multiplexage temporel.

IV.2. Multiplexage temporel :

Le multiplexage temporel consiste à diviser chaque canal de communication en intervalles de temps de0, 577ms.On définit dès lors une trame élémentaire de 8 intervalles pour une durée de :

$$8 \times 0,577 = 4,615 ms.$$

Comme il est exclu de transmettre toutes les informations en une fois, il faut découper l'information et la transmettre au moyen de plusieurs trames consécutives. La norme GSM prévoit une organisation spécifique de structure hiérarchique

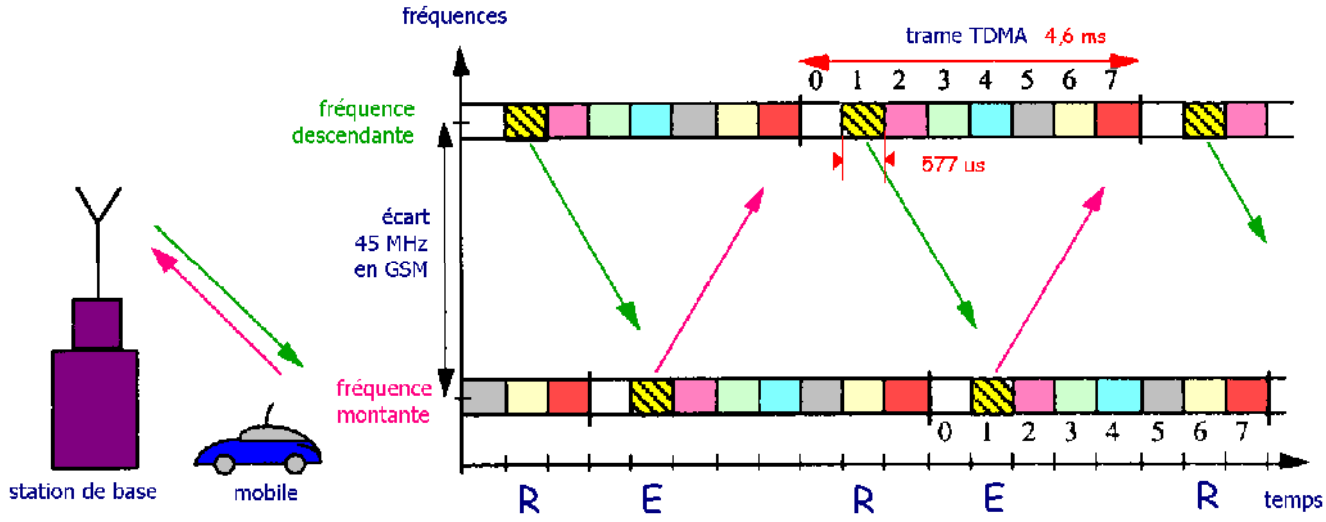


Fig.I.10 : Mobile en conversation sur le time-slot 1.

Durant une communication téléphonique, le mobile GSM reçoit des informations de la station de base et émet des informations vers celle-ci :

- ces échanges se font sur deux fréquences différentes et n'ont pas lieu au même moment
- au niveau du mobile, l'émission et la réception sont décalées dans le temps de 3 time-slots

- pour conserver la même numérotation des slots, le début de la trame TDMA du mobile est décalée de 3 time-slots / début de la trame de la base

Le mobile reçoit donc le signal émis par la base sur la fréquence descendante f durant un time slot soit 577 µs , puis 3 time-slots soit 1,7 ms plus tard, émet son signal vers la station de base sur la fréquence montante plus basse (f-45 MHz pour le GSM).

V.Les différents canaux :

Il existe deux types de canaux :

-Canaux physiques.

-Canaux logiques.

V.1.Canaux physiques :

Chaque utilisateur dispose d'un slot par trame TDMA; la répartition périodique d'un slot dans les trames sur une fréquence particulière constitue un **canal physique**.

Il est caractérisé par :

-Une paire de fréquences.

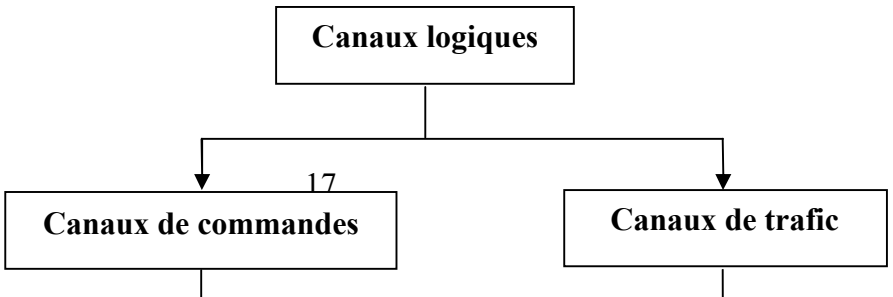
-Un slot particulier par fréquence choisi parmi huit.

V.2. Les canaux logiques :

Pour supporter les différentes fonctions spécifiques à la norme, il faut prévoir plusieurs fonctions de contrôle de nature et de niveau varié sur l'interface radio. On peut distinguer ces canaux en deux types :

-Canaux de commandes.

-Canaux de trafic.



V.2.1. Les canaux de commande (control channels) :

V.2.1.1 Canaux de diffusion BCH:

Canal FCCH :

Le canal FCCH (Frequency Correction Channel) consiste en un burst particulier émis environ toutes les 50 ms. Il est présent seulement sur le TS0 de la voie balise. Il est émis dans les trames 0, 10, 20, 30 et 40 d'une multitrame à 51 trames

Le canal FCCH permet de transmettre des informations au MS afin de synchroniser son synthétiseur aux fréquences de travail de la BTS dont il dépend.

Canal SCH :

Le burst SCH (Synchronisation Channel) n'est émis que dans le TS0 d'une trame TDMA. Il est toujours situé après le burst FCCH. En écoutant le canal SCH, le MS reçoit des informations relatives à la structure des trames dans la cellule (le N° de TDMA) ainsi que le code d'identification de station de base (BSIC) de la station de base sélectionnée. .

Canal BCCH :

Le canal de commande de diffusion (Broadcast Control Channel). Les informations qui sont diffusées sur ce canal, sont des informations concernant la cellule :

- La puissance d'émission (Max et Min) pour le MS
- Minimum de puissance reçue
- Les fréquences (porteuses) des cellules adjacentes
- Numéro de la zone de localisation (LAI)

V.2.1.2 Canaux communs de commande CCCH :

PCH (canal de recherche):

Le PCH est transmis sur la liaison downlink en mode point à point. Le MS se met à l'écoute du PCH à intervalles réguliers pour voir si un réseau désire le contacter suite à l'arrivée d'un appel, d'un message court ou une authentification. Ce message de recherche comprend le numéro de signalisation du MS (IMSI) ou un numéro provisoire (TMSI).

RACH (canal à accès aléatoire) :

Le canal RACH peut également être utilisé lorsque le MS désire entrer en contact avec le réseau. Le RACH est transmis sur la liaison montante (uplink) en mode point à point.

Canal AGCH (canal de concession d'accès) :

Il est utilise pour l'allocation d'un canal dédie à un mobile. Le message d'allocation contient la description complète du canal de signalisation utilisé : numéro de porteuse et numéro de slot utilisé ; il contient également le paramètre TA (Time Advance).

V.2.1.3. canaux de commande dédiés DCCH :

SDCCH (canal de contrôle dédié autonome):

Il est alloué aux phases d'établissement de communications et à la transmission de courts messages alphanumériques.

SACCH (canal de contrôle lent associé):

Il est associé canaux TCH et SDCCH afin les contrôler car la liaison radio est fluctuante.

Il supporte les informations suivantes :

- Compensation du délai de propagation TA.
- Contrôle de la puissance d'émission du mobile.
- Rapatriement des mesures effectuées par le MS sur les BTS voisines.

FACCH (canal de contrôle rapide associé) :

Le FACCH est utilisé lorsqu'un handover doit être effectué soudainement pendant une conversation. Il fonctionne en mode 'vol' signifiant qu'un segment de parole de 20 ms est remplacé par les informations de signalisation nécessaire au handover.

V.2.2. Canaux de trafic TCH :

Il existe deux canaux de trafic, plein débit et demi-débit. Il sera possible d'utiliser les TCH à demi débit seulement lorsque des codeurs vocaux à demi débit offrant une qualité acceptable deviendront disponibles. Un TCH à plein débit occupe un canal physique (un TS sur une porteuse) alors que 2 TCH à demi débit peuvent se partager un canal physique.

IV.Bursts et trames :

IV.1. Burst :

IV.1.1. La structure du burst :

Les données échangées entre le téléphone mobile et la base (voix ou signaux de contrôle) sont toujours transmises sous une forme précise :

- 57 bits de données (voix ou signaux de contrôle)
- 26 bits (toujours les mêmes dans une cellule) d'une séquence de formation (training Sequence), qui a pour mission de mesurer les propriétés du canal de transmission
- 57 bits de données (voix ou signaux de contrôle)
- quelques bits d'encadrement et indicateurs

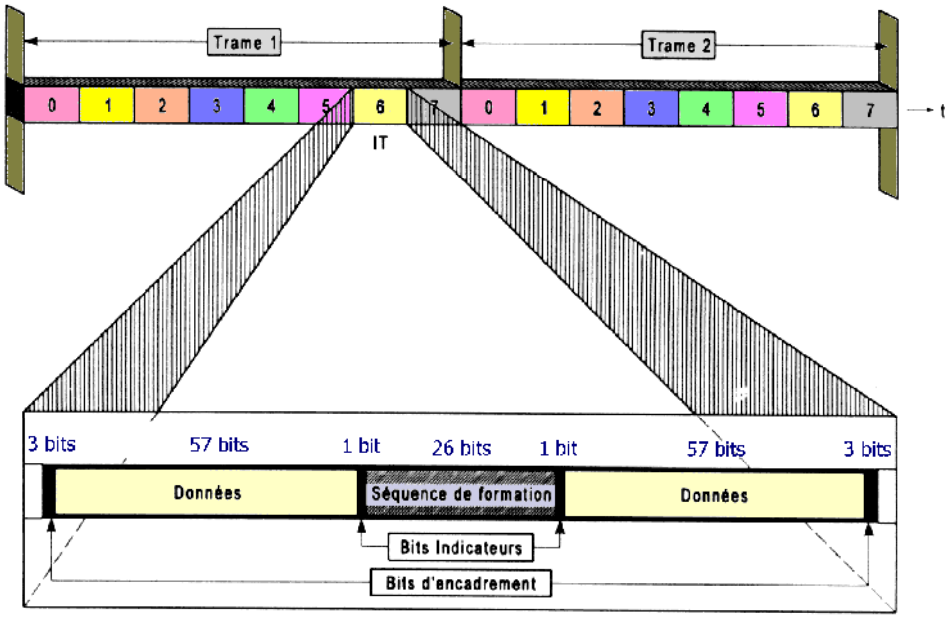


Fig.I.12 : Structure du signal émis dans un time slot.

IV.1.2.Les différents types de bursts :

1. Les bursts d'accès qui sont envoyés par les mobiles lorsqu'ils veulent entrer en contact avec le réseau.

2. Les bursts de synchronisation qui contiennent les informations sur la localisation et les fréquences utilisées.

3. Les bursts normaux qui transportent les messages.

4. Les bursts de correction de fréquence : La station de base envoie des données servant à prévenir des interférences possibles avec des fréquences voisines

5. Les bursts de bourrage (dummy packet) qui sont placés dans les espaces vides si aucune donnée ne doit être envoyée. Pour être précis, ce burst est composé de 2 salves de 58 bits préfixés interrompus par une séquence d'entraînement de
26 bits.

Tous les types de burst ont une forme semblable. Ils sont composés, dans l'ordre, de :

- bits d'en-tête (tail bit, TB), nécessaires à la synchronisation. Ils correspondent toujours au code 000 sauf pour les bursts d'accès.
- 148 bits utiles dont le format depend du type de burst.

- bits de fin, aussi appelés tail bit, terminés par une période temporelle de garde requise pour permettre à l'émetteur de réduire sa puissance de 70 [dB]. Elle sert aussi à compenser la durée de transmission qui est variable pour la réception d'un paquet au suivant si le mobile a bougé.

IV.2.Organisation des trames :

En veille ou en communication, un mobile travaille toujours avec plusieurs canaux logiques. Utiliser un canal physique pour de ces taches, ce serait gâcher de la ressource radio puisque les différents canaux logiques ne nécessitent pas un débit comparable à celui de la parole codée. Sur son canal physique, le mobile va donc trouver un multiplex de canaux logiques correspondant à son active.

La norme GSM impose l'organisation du transport des slots sous forme d'une structure à 4 niveaux hiérarchiques de trames :

La trame TDMA : 8 slots, t= 4,615 ms.

La multitrame : de 2 types possibles suivant le type de canaux à transporter. Multitrame à 26 : 26 trames TDMA, durée= 120 ms (canaux de trafic et de contrôle). Multitrame à 51 : 51 trames TDMA, durée=235,365 ms (canaux les canaux de contrôles).

La supertrame : 1326 trames TDMA ; TSUPERTRAME=6,12s

Dans chaque trame TDMA, on peut trouver des slots qui évoluent en multitrame à 51.La structure de supertrame permet d'homogénéiser i'organisation entre tous les slots d'une même trame TDMA. La supertrame se compose de 26 multitrames à 51 ou de 51 multitrames à 26.

L'hypertrame : 2048 supertrames ; TDurée =3h28min53s760ms

La structure de l'hypertrame dure 2048*26*51=2715648 trames TDMA. Chaque trame TDMA est repérée par un compteur FN dans l'hypertrame. Le compteur FN donne en quelque sorte la base de temps propre de la BTS.

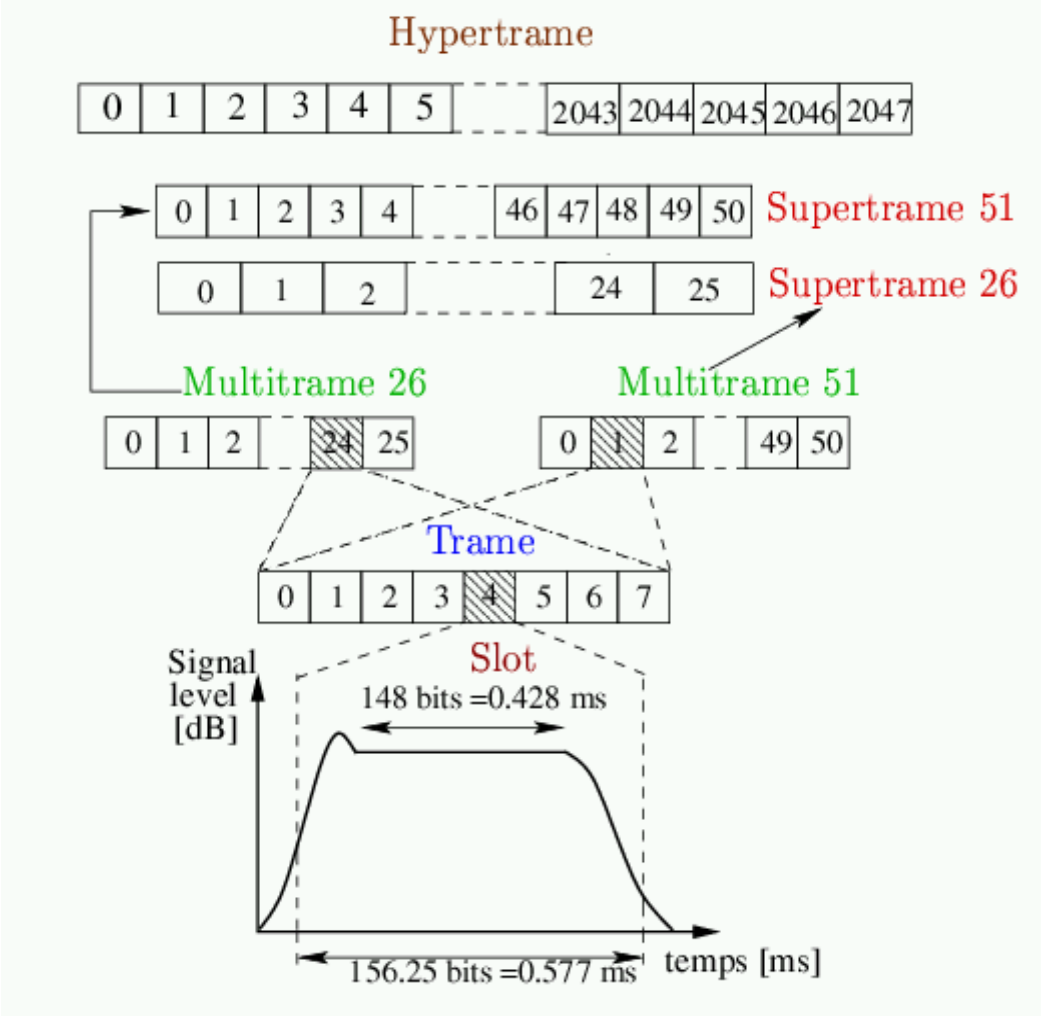


Fig.I.13: organisation des multiples de trames.

I. Introduction :

Tous les moyens de communication sont associés à un ensemble de risques.
La prise en compte de ces risques permet de mettre en œuvre des mesures de sécurité.
La téléphonie mobile GSM ne fait pas exception, et les risques menaçant ce réseau sont importants vu l'emploi d'un canal radio qui rend la communication vulnérable aux écoutes et aux utilisations frauduleuses.

Le système GSM a donc recours aux procédés suivants :

- authentification de chaque abonné avant de lui autoriser l'accès à un service.
- utilisation d'une identité temporaire.
- confidentialité de l'identité de l'utilisateur et des informations transmises.
- chiffrement des communications.

Gestion de sécurité du réseau et des appels :

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

II.1. Les systèmes cryptés :

II.1.1. Introduction :

Un système crypté est défini par deux transformations principales.
La première transformation correspond au cryptage qui est appliquée sur un item de données en clair et va générer un item correspondant (inintelligible) appelé texte crypté.
La seconde transformation appelée décryptage est appliquée au texte crypté et permet de retrouver le texte original. Une transformation de cryptage est définie par un

algorithme qui va utiliser en entré le texte original et une clé de décryptage pour retrouver le texte original à partir du texte crypté.

Il existe deux types de base de systèmes cryptographiques, les systèmes symétriques ou à clé privée et les systèmes asymétriques ou à clé publique.

GSM et GPRS sont des systèmes à clé privée.

II.1.2. Systèmes à clé secrète :

Les systèmes à clé secrète sont caractérisés par le fait que les clés utilisées pour le cryptage et le décryptage sont identiques.

Le système fonctionne de la façon suivante :

Si deux systèmes A et B décident de communiquer de façon sécurisée. Ils commencent par obtenir chacun une clé ; les clés doivent être gardées secrètes à l'exception de A et B. cela permet à A et B de protéger leurs messages envoyés en les cryptant à l'aide de la clé secrète.

Seules les parties concernées possèdent la clé permettant de décrypter les messages.

III. Les algorithmes utilisés dans la sécurité GSM :

Trois types d'algorithmes sont utilisés dans les protocoles de sécurité et confidentialité des données GSM :

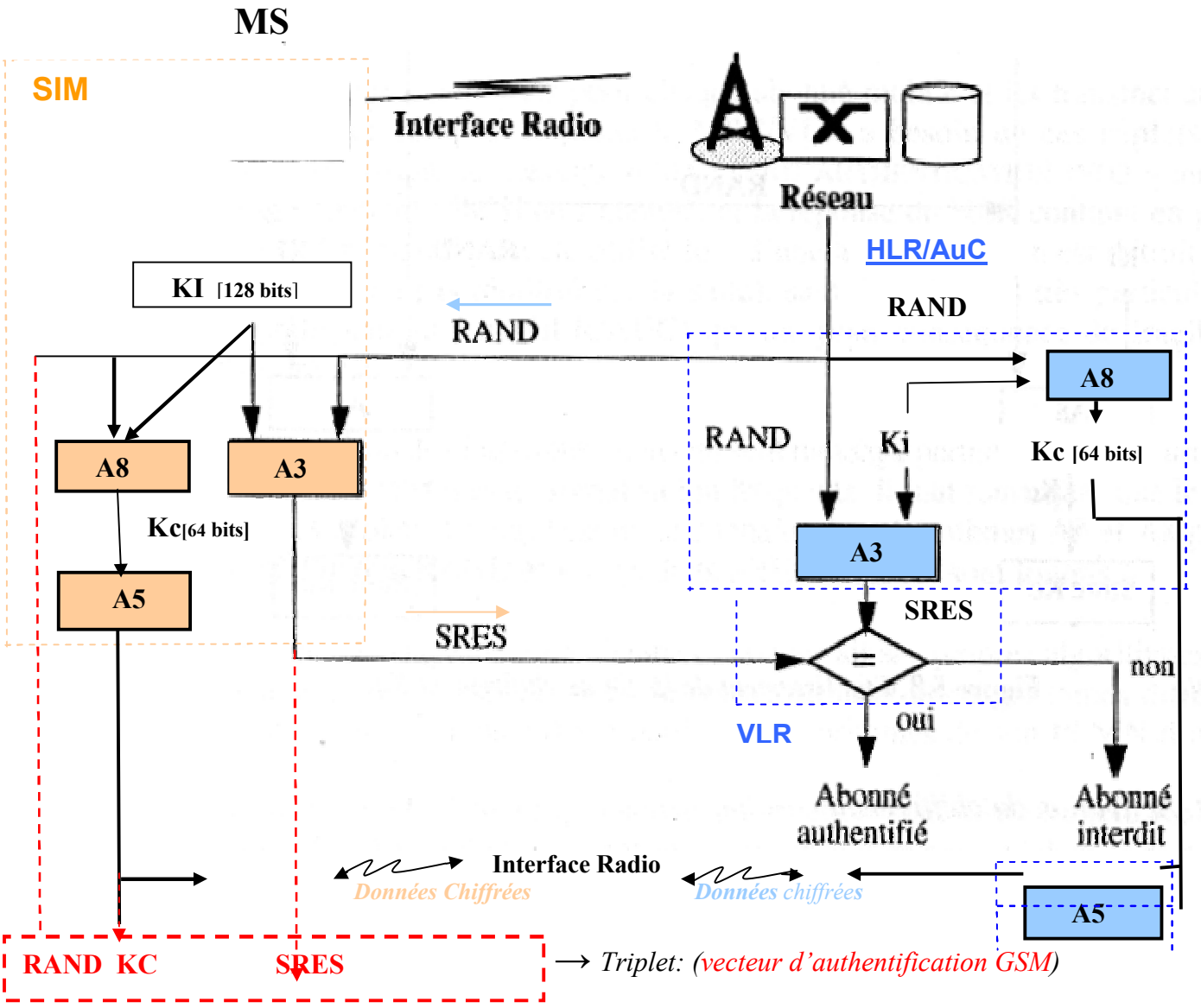


Fig. II.1 : Authenticité et sécurité GSM

III.1. Algorithme A3 :

Cet algorithme est utilisé pour l'authentification d'un utilisateur du réseau. A3 fourni une réponse SRES à partir d'un nombre aléatoire envoyé par le réseau. Pour la détermination de SRES, A3 utilise aussi la clé d'authentification Ki.

Du coté mobile, l'algorithme A3 est enregistré dans la carte SIM.

Du coté du réseau, il est obtenu dans le centre d'authentification (AuC) qui correspond juste à une subdivision du HLR.

Les deux paramètres utilisés par l'algorithme A3 ont les formats suivants :

Longueur de Ki : 128bits.

Longueur du nombre aléatoire (RAND) :128 bits.

Le résultat de l'algorithme (SRES) à une longueur de 32 bits.

III.2. Algorithmes A5 :

Cet algorithme est implémenté dans le mobile, il est utilisé dans les processus de cryptage et de décryptage.

Dans les systèmes TDMA, l'information est organisé en bloc de 114 bits, chaque bloc est incorporé dans un burst et transmis durant un time slot. Les slots d'un canal physique sont séparés par la durée d'une trame.

Pour le cryptage, l'algorithme A5 produit toute les 4.615ms une séquence de 114 bits de cryptage/décryptage (BLOCK) qui sont additionnés modulo 2 avec les 114 bits du texte en clair.

Le décryptage est accompli du coté du MS avec le premier bloc de 114 bits produit par l'algorithme A5 et l'encryptage est accompli avec le second bloc.

En conséquence, du coté du réseau le bloc1 est utilisé pour encrypter et le bloc2 pour décrypter. Ainsi A5produit 2 fois 114bits toute les 4.615ms.

Le cryptage démarre quand une réponse positive à l'authentification est reçue de la part du MS en utilisant la synchronisation pour le démarrage du cryptage qui a été sélectionnée dans le BSC.

Les deux paramètres d'entrée (N° de trame, Kc) et les deux paramètres de sortie (bloc1, bloc2) de l'algorithme A5 doivent avoir le format suivant :

Longueur de Kc : 64 bits.

Longueur de N° de trame : 22 bits.

Longueur du bloc1 : 114 bits.

Longueur du bloc2 : 114 bits.

L'algorithme A5 doit produire un bloc1 et bloc2 en un temps plus court que la durée d'une trame (4.615ms).

III.3. AlgorithmeA8 :

Du coté de la station mobile, l'algorithme A8 est contenu dans la carte SIM. Du coté du réseau, l'algorithme A8 est colocalisé avec A3.

Les deux paramètres en entrée (RAND, Ki) et le paramètre de sortie (Kc) de A8 doivent avoir les formats suivants :

Longueur de Ki : 128 bits.

Longueur du paramètre RAND : 128 bits.

Longueur de Kc : 64 bits.

IV. Numérotation liée à la sécurité/mobilité :

Le système GSM utilise quatre types d'adressages liés à l'abonné :

L'**IMSI** :(identité invariante de l'abonné), elle n'est connu qu'à l'intérieur du réseau GSM ; cette identité doit rester secrète autant que possible.

Le **TMSI** : c'est une identité temporaire utilisée pour identifier le mobile lors des interactions station mobile-réseau.

Le **MSISDN** : c'est le numéro de l'abonné, c'est le seul identifiant de l'abonné mobile connu à l'extérieur du réseau GSM.

Le **MSRN** : c'est un numéro attribué lors d'un établissement d'appel. Sa principale fonction est de permettre l'acheminement des appels par les commutateurs (MSC et GMSC).

IV.1. IMSI (International Mobile Subscriber Identirty) :

Chaque abonné dispose d'une identité internationale IMSI, unique pour tous les réseaux GSM et qui ne varie pas dans le temps.

On le transporte aussi rarement que possible sur l'interface radio pour des questions de sécurité et de confidentialité.

L'IMSI sert également au réseau à rechercher l'abonné dans les cas ou le TMSI n'est pas disponible.

L'IMSI est codé sur au plus 15 bits et comprend trois parties :

Mobile Country Code (MCC) : indicatif du pays domicile de l'abonné mobile.

Mobile Network Code (MNC) : indicatif du PLMN nominal de l'abonné mobile.

Mobile Subscriber Identification Number (MSIN) : numéro de l'abonné mobile à l'intérieur du réseau GSM.

Les deux champs MCC et MNC permettent de déterminer, de façon unique dans le monde, le PLMN de l'abonné. Les deux premiers chiffres du champ MSIN donnent

l'indicatif du HLR de l'abonné au sein de son PLMN. Les MSC/VLR sont donc capables à partir d'un IMSI quelconque d'adresser le HLR de l'abonné correspondant.

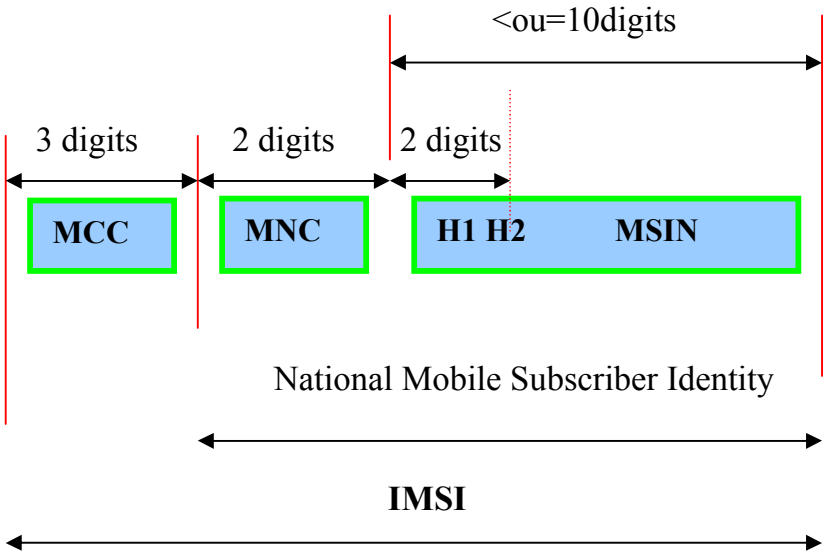


Fig. II. 2 : Composition de l'IMSI.

IV.2. TMSI (Temporary Mobile Station Identity) :

A l'intérieur d'une zone gérée par un VLR, un abonné dispose d'une identité temporaire, le TMSI attribuée au mobile de façon locale, c'est à dire uniquement pour la zone gérée par le VLR courant du mobile.

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

Le TMSI est utilisé pour identifier le mobile appelé ou appelant lors d'un établissement de communication. Plusieurs mobiles dépendant de VLR différents peuvent avoir le même TMSI. A chaque changement de VLR, un nouveau TMSI doit être attribué.

L'utilisation du TMSI est optionnelle ; en effet, la norme GSM prévoit la possibilité pour l'opérateur de n'avoir recours qu'à l'IMSI. Cependant pour les raisons de sécurité évoquées précédemment, il est préférable d'utiliser le TMSI.

La structure du TMSI est laissée libre à l'opérateur. Il est codé sur 4 octets, sa structure plus courte que l'IMSI permet de réduire la taille des messages d'appel sur la voie radio.

IV.3. MSISDN (Mobile Station ISDN Number):

Le MSISDN est le numéro que composera une personne désirant joindre un abonné GSM. Seul le HLR contient la table de correspondance entre le MSISDN et l'IMSI d'un abonné.

Il comprend les champs suivants :

Country Code (CC ou code pays) : indicatif du pays dans lequel l'abonné a souscrit son abonnement.

National Mobile Number : numéro national du mobile composé du National Destination Code(NDC) déterminant le PLMN particulier dans le pays et Subscriber Number (SN) attribué par l'opérateur.

Comme pour l'IMSI, le MSISDN permet à un PLMN de connaître le HLR de l'abonné à partir des premiers chiffres du champ SN.

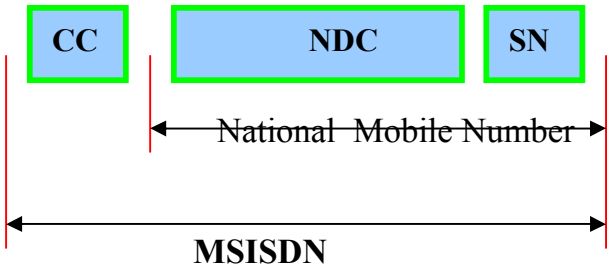


Fig. II. 3 : Structure du MSISDN.

IV.4. MSRN (Mobile Station Roaming Number):

Le MSRN a pour fonction de permettre le routage des appels entrants directement du commutateur passerelle (GMSC) vers le commutateur courant (MSC) de la station mobile.

Il est attribué par le VLR courant du mobile de façon temporaire et uniquement lors de l'établissement d'un appel à destination de la station mobile. Le MSRN a la même structure que le MSISDN.

IV.5. IMEI (International Mobile Equipement Identity) :

Tout terminal est référencé de manière unique par l'IMEI, qui est codé sur au plus 15 digits.

Il est composé des champs suivants :

Type Approval Code (TAC) : champ codé sur 6 digits fourni au constructeur lorsque le matériel a passé l'agrément.

Final Assembly Code (FAC) : champ codé sur 2 digits qui identifie l'usine de fabrication.

Serial Number (SNR) : champ codé sur 6 digits librement affecté par le constructeur.

Spare : digit réservé.

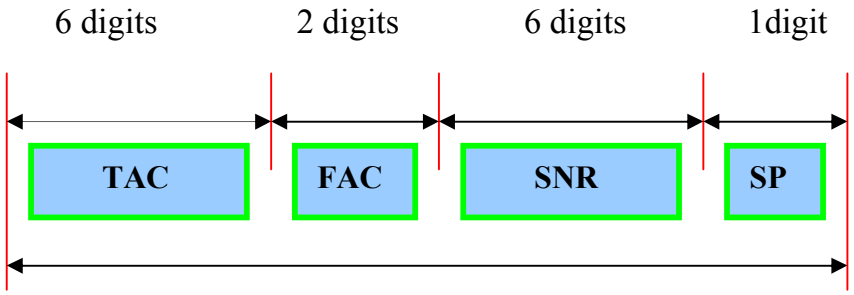


Fig. II. 4 : Composition de l'IMEI.

V. Principes généraux d'authentification et de chiffrement :

La sécurité pour les mobiles est assurée par la confidentialité des algorithmes décryptage du GSM. L'authentification et la confidentialité sont mises en place par les techniques de clés symétriques de chiffrement, ce qui est schématisé à la figure II.5.

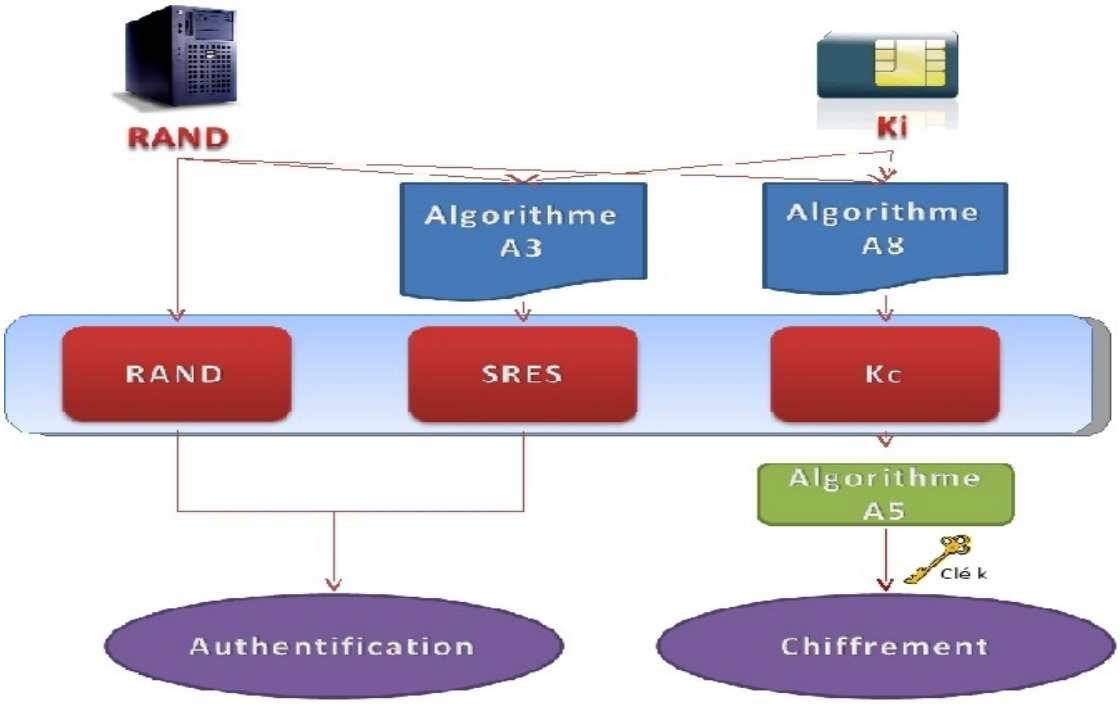


Fig. II. 5 : procédure d'authentification et de chiffrement

Pour les fonctions d'authentification et de chiffrement des informations transmises sur la voie radio, le GSM utilise des nombres aléatoires(RAND), une clé Ki pour l'authentification et la détermination de la clé de chiffrement.

A3, A8, A5 sont des fonctions spéciales dans le GSM. A3 fournissant un nombre SRES à partir de RAND et de ki, A8 donne la clé de chiffrement(Kc) à partir aussi de RAND et Ki, A5 est utilisée pour le chiffrement/déchiffrement des données à partir de Kc par le mobile et la station base.

SRES=A3 (ki, RAND)

Kc=A8 (Ki, RAND)

Le Kc ajouté à l'algorithme A5 réalise le chiffrement/déchiffrement des données, de la voix et les informations de signalisation dans l'interface radio.

Données Chiffrées=A5 (kc, Données)

Données=A5 (kc, Données Chiffrées)

V.1 .Protocole d'authentification :

L'Authentification GSM permet de vérifier que l'identité transmise par le mobile est correcte .Si la réponse émise (SRES) par le mobile est identique a celle générée par l'AUC, l'accès au réseau est accordé pour le MS, sinon l'accès est refusé
Le protocole d'authentification du GSM est montré ci-dessous (figure III.6).

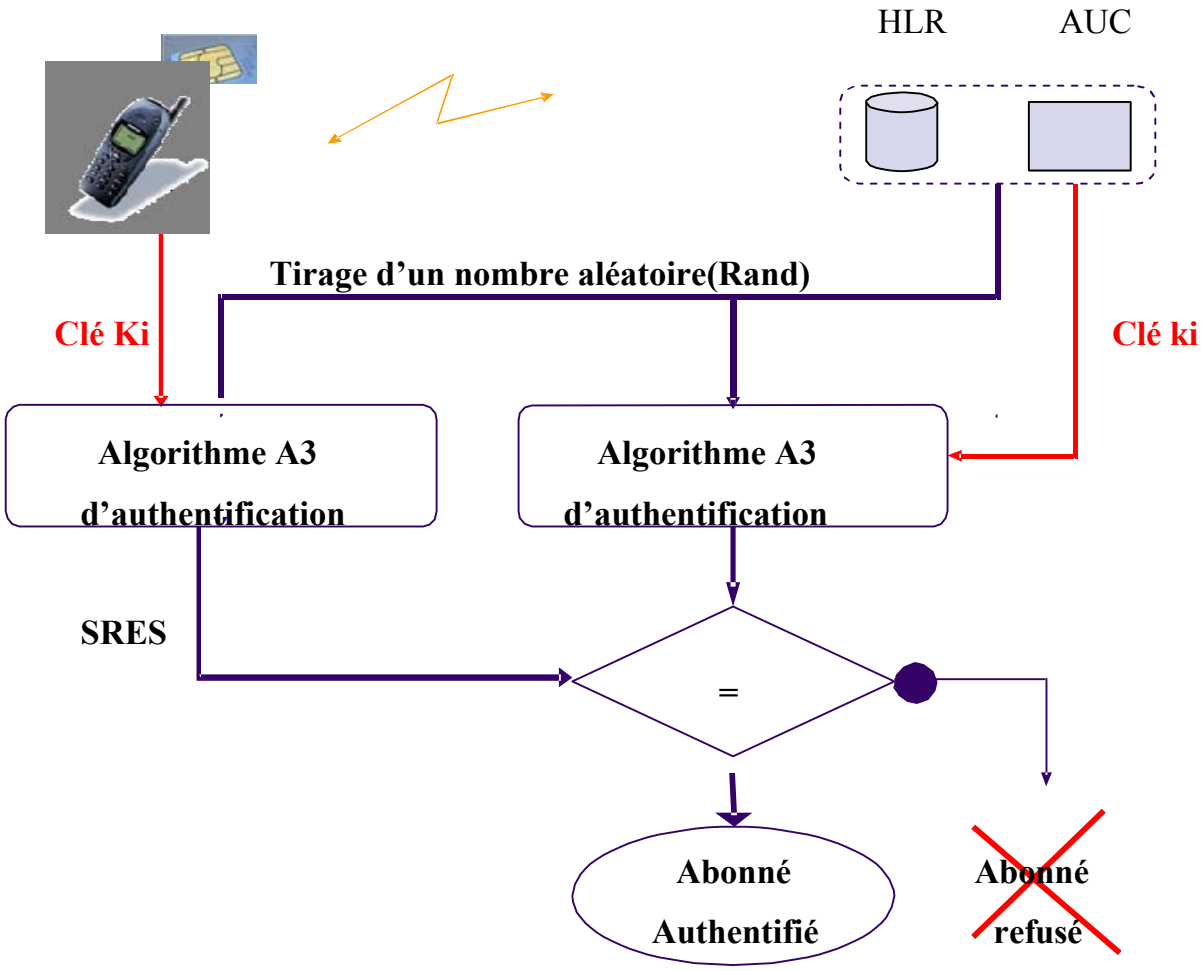


Fig. II. 6 : Authentification des abonnés

V.2 : Etablissement de la clé de chiffrement Kc :

Les informations transmises sur les canaux dédiés sont chiffrées grâce à la clé Kc calculée à partir du nombre aléatoire RAND et de l'algorithme A8 selon la figure II.6 :

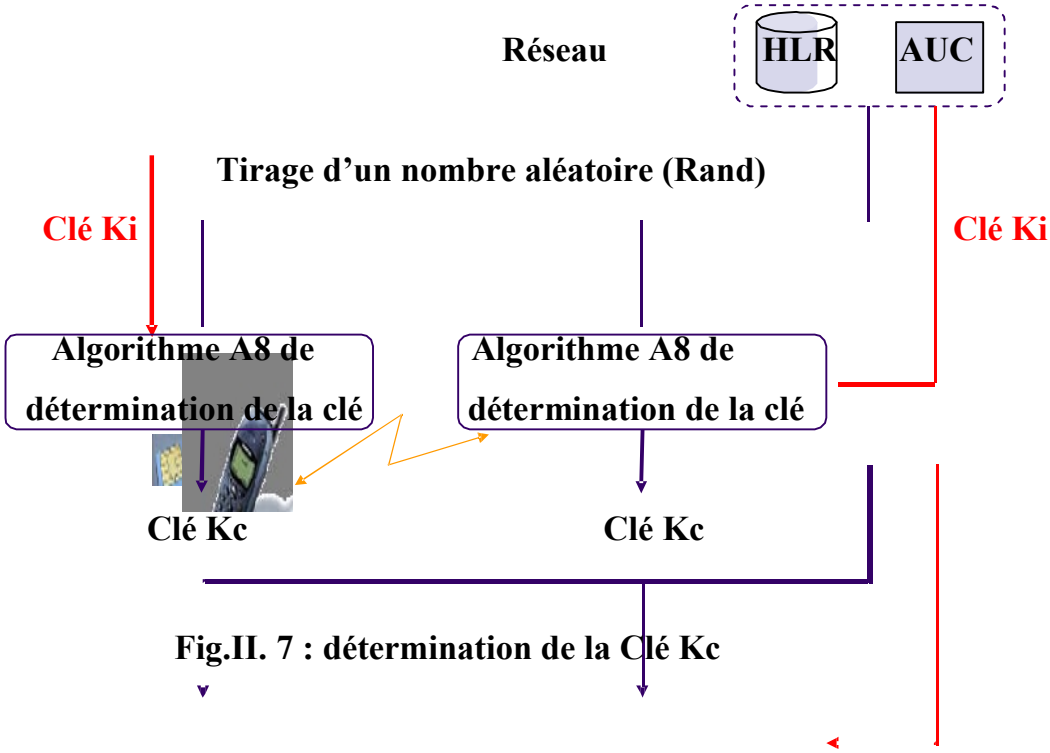
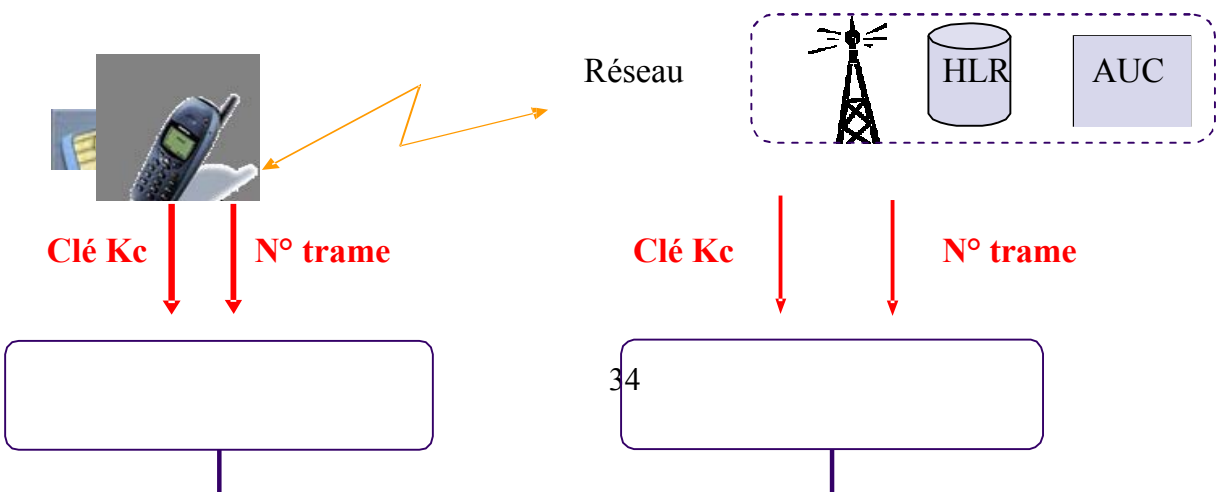


Fig.II. 7 : détermination de la Clé Kc

V.3 : Protocole de confidentialité des données :

La confidentialité des données permet d'interdire l'interception et le décodage des informations usager et de signalisation, par des personnes non autorisées.

La confidentialité des informations usager est obtenue grâce au chiffrement de celles-ci. Elle ne concerne que les informations transmises sur l'interface MS-BTS.



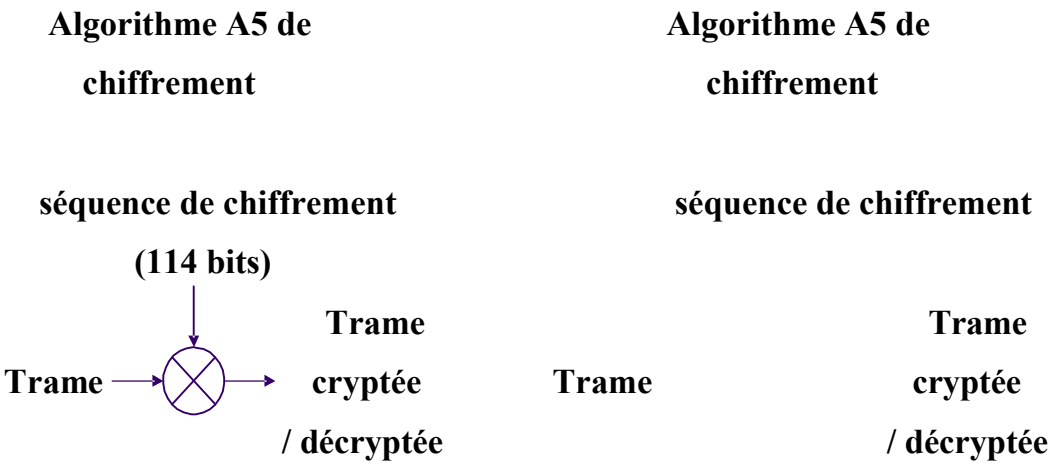


Fig. II. 8 : confidentialité des communications

VI. Les méthodes de transmission de données :

Les méthodes de transmission de données par le protocole GSM sont montrées aux figures II.9 et II.10 :

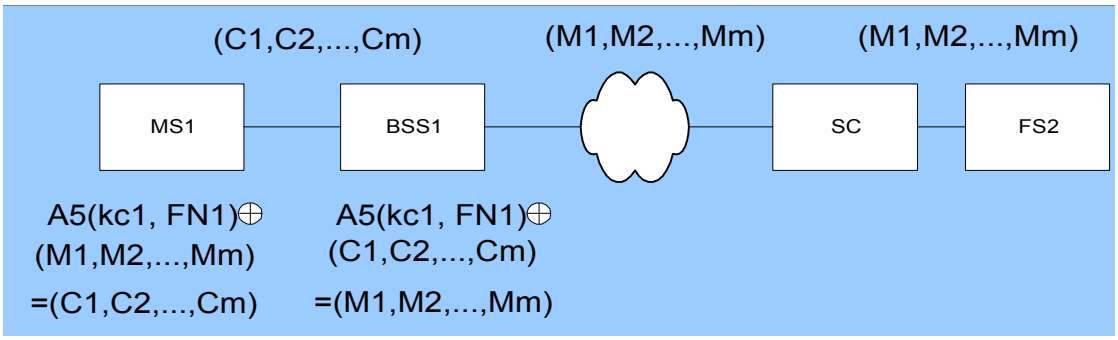


Fig II. 9 : méthode de transmission de données dans GSM MS-FS.

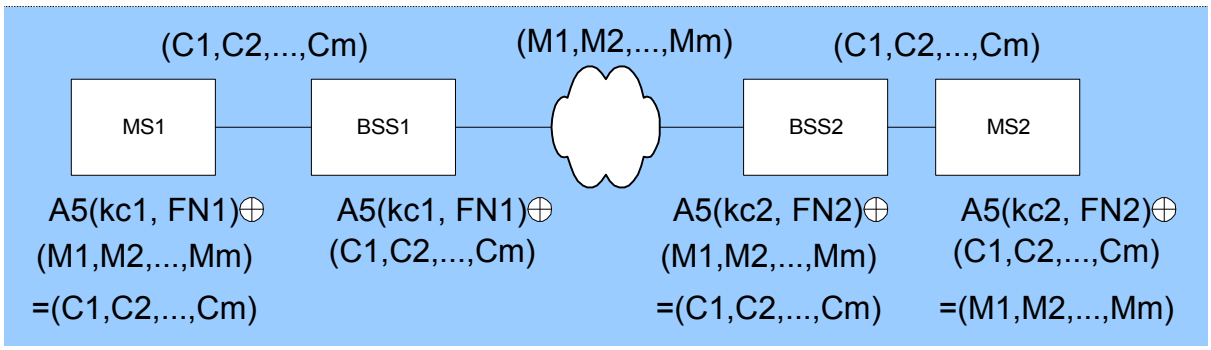


Fig. II.10 : méthode de transmission de données dans GSM MS-MS.

Sur la figure II.9, un appel est établi entre un mobile (MS1) et un fixe (FS2). MS1 fait le cryptage des informations en utilisant l'algorithme A5 et une clé kc1, puis passe par la voie radio. Le BSS1 va faire le décryptage. Alors il transmet les données sans aucune protection jusqu'au FS2.

Sur la figure II.10, un appel est établi entre deux mobiles (MS1 et MS2). MS1 fait le cryptage des informations en utilisant l'algorithme A5 et une clé kc1, puis passe par la voie radio. Le BSS1 va faire le décryptage, il transmet les informations sans protection à travers le réseau jusqu'au BSS2 qui fera le cryptage et le transmet à MS2, qui fait le décryptage pour récupérer les données en clair.

VII. Protocole de confidentialité de localisation :

Le mobile se déplace d'un endroit à l'autre et il peut accéder au réseau quelque soit l'endroit et le temps. La localisation du mobile est une information qu'on doit protéger. Le TMSI est utilisé pour protéger l'identité de l'utilisateur et éviter de transmettre l'IMSI sur la voie radio. Le réseau (au niveau d'un VLR) gère des bases de données et établit une correspondance entre IMSI et TMSI. L'IMSI est transmis lors de la mise sous tension du mobile, dans le cas où le TMSI serait perdu ou une panne produisant la perte des informations de l'abonné.

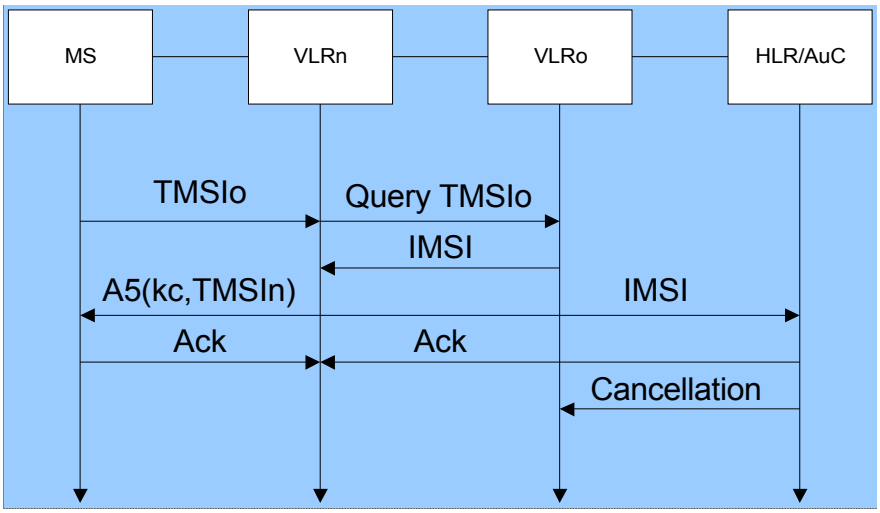


Fig. II.11 : protocole de mise à jour de localisation.

Le mobile transmet le TMSI ancien (TMSI-o) au nouveau VLR (VLRn). Le VLRn fait la mise à jour de la localisation, en demandant au VLR ancien (VLRo) le IMSI. Après que le VLRn a authentifié le MS.

Le VLR-n transmet le nouveau TMSI (TMSIn) au mobile en mode chiffré et le IMSI au HLR. Le HLR garde les informations courantes de la localisation du mobile dans sa base des données. Finalement, le HLR efface toutes les informations qui se réfèrent au VLRo.

I. Authentification:

L'authentification permet de vérifier l'identité transmise par le mobile (TMSI ou, par défaut, IMSI) afin de se prémunir des utilisations frauduleuses.
L'authentification de l'abonné peut être exigée par le réseau :

- avant une mise à jour de localisation
- avant l'établissement d'une communication (entrante ou sortante)
- avant l'activation/désactivation de certains services
- avant la mise en œuvre de la clé de chiffrement KC sur certains canaux dédiés

La procédure d'authentification comprend les étapes suivantes :

- Préalablement, le centre d'authentification AUC génère le triplet (RAND, Kc, SRES) en appliquant l'algorithme d'authentification A3, et à l'algorithme A8.

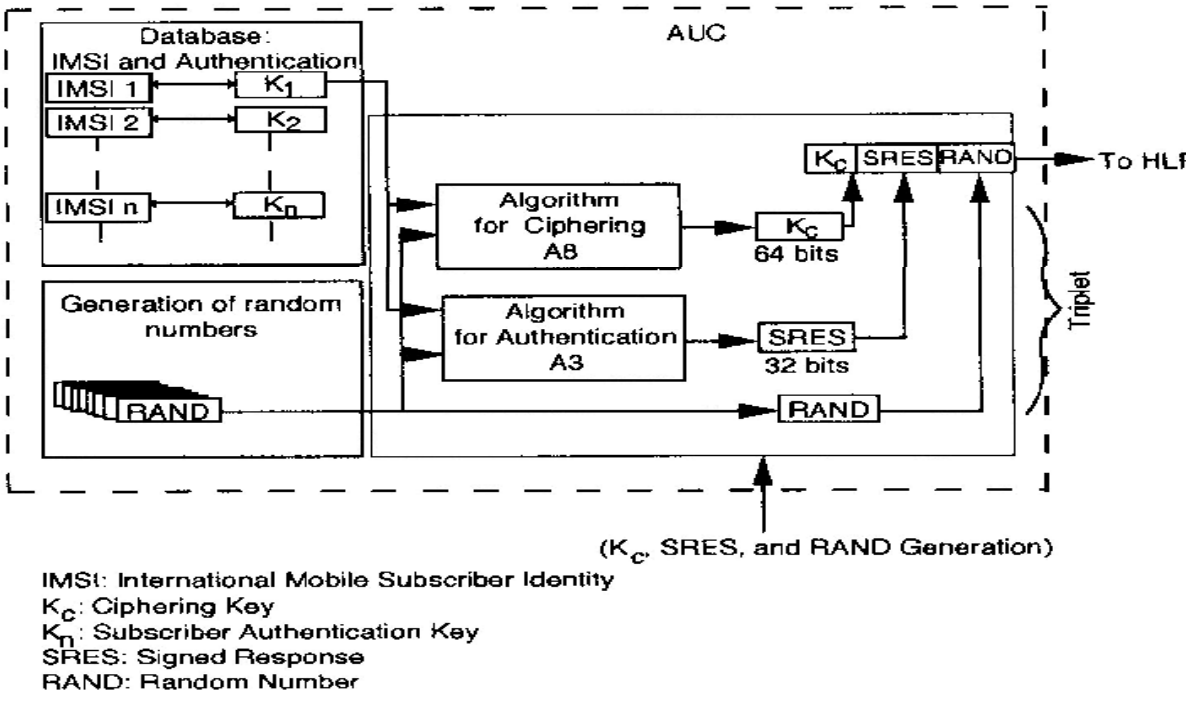


Fig.III.1 : La génération du triplet (RAND, KC, SRES) dans l'AUC.

- Le triplet est transféré de l'AUC vers le HLR sur ordre du MSC/VLR
- La carte SIM effectue un calcul cryptographique similaire a celui effectué dans l'AUC après avoir reçu le RAND du réseau.
- L'enregistreur VLR compare la réponse signée SRESc à celle contenue dans le triplet choisi, et, en cas d'égalité des réponses, la carte est authentifiée

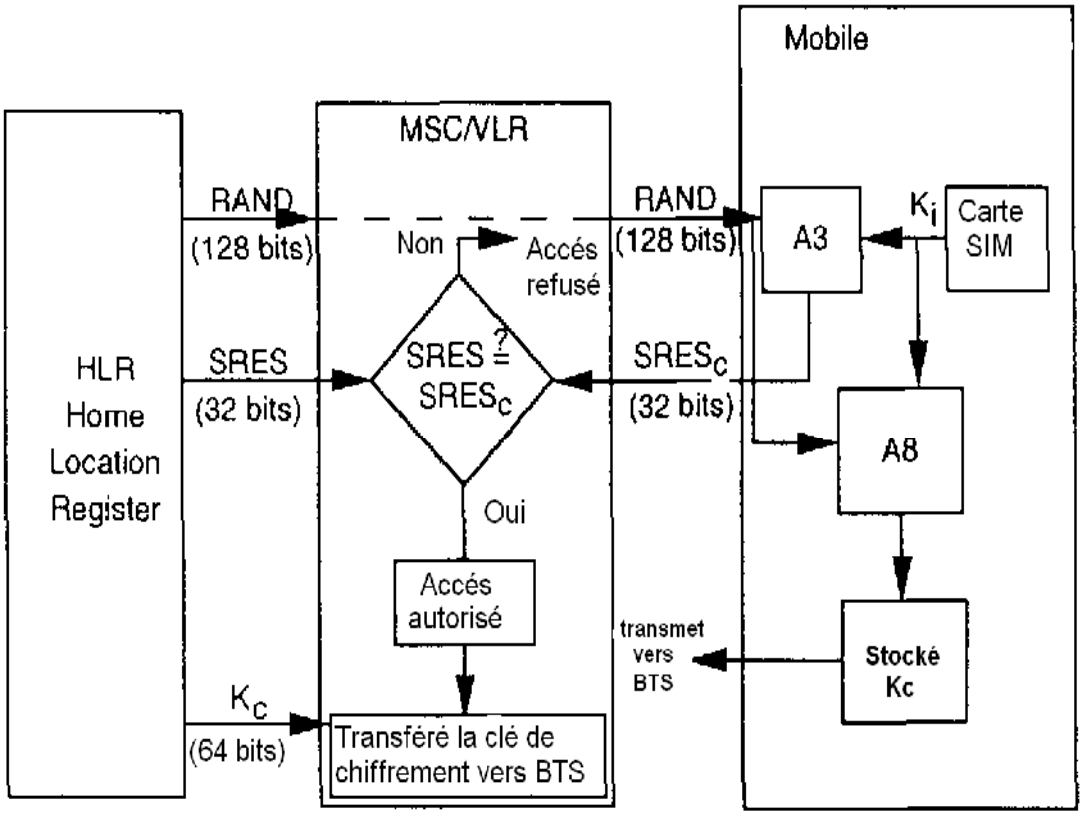


Fig.III.2 : Le processus d'authentification GSM

Si cette procédure d'authentification permet au réseau fixe d'authentifier la carte, elle ne permet pas en revanche à la carte SIM d'authentifier le réseau fixe. Aucune authentification mutuelle n'est prévue.

II. Le chiffrement :

Le chiffrement est réalisé via un chiffrement par flux, c'est à dire l'algorithme de chiffrement prend la clef secrète et un nombre appelé « *frames* » et génère un flux pseudo aléatoire de bits (keystream) qui sont ainsi XORé avec les bits définis en entrée pour obtenir le chiffrement, ou avec les bits reçus en sortie pour obtenir le déchiffrement.

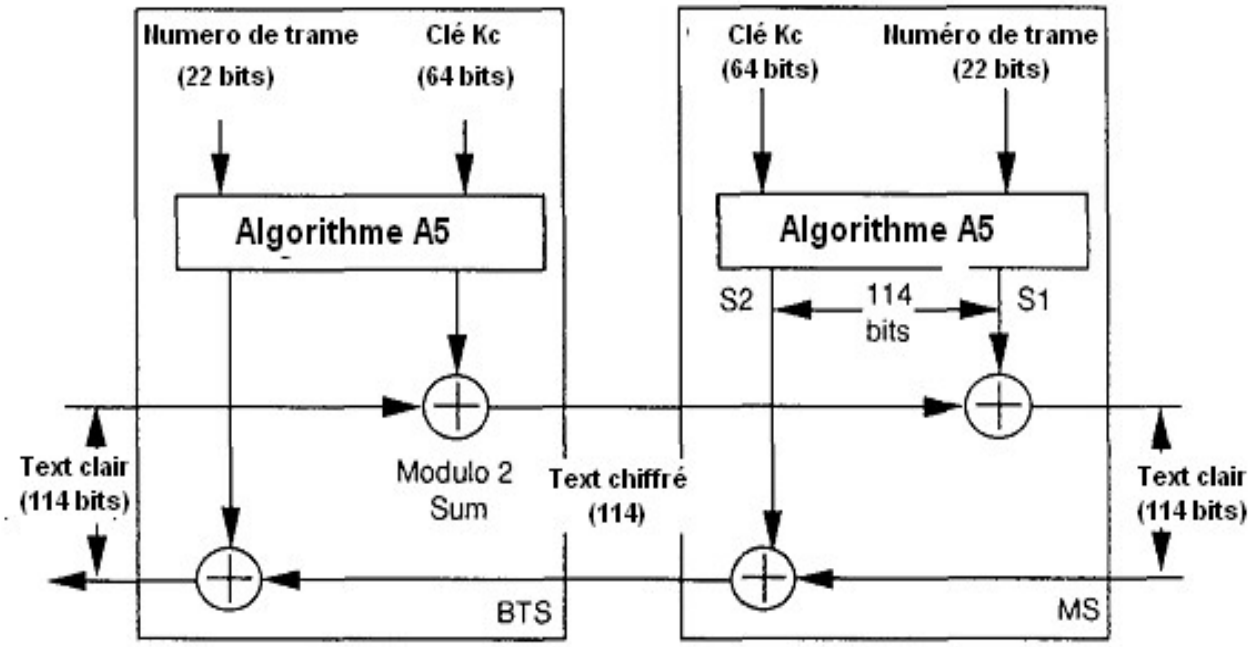


Fig.III.3 : chiffrement/déchiffrement par flux.

II.1.Le processus de chiffrement :

Le chiffrement commence au niveau du mobile après avoir reçu un message sur le canal DCCH par le MSC/VLR à travers la BTS. Le procède chiffrement/déchiffrement de données de l'utilisateur aura lieu dans la BTS après envoyé la Kc du MSC en passant par le BSC coté réseau et dans la carte SIM coté mobile comme le montre la Fig III.4 :

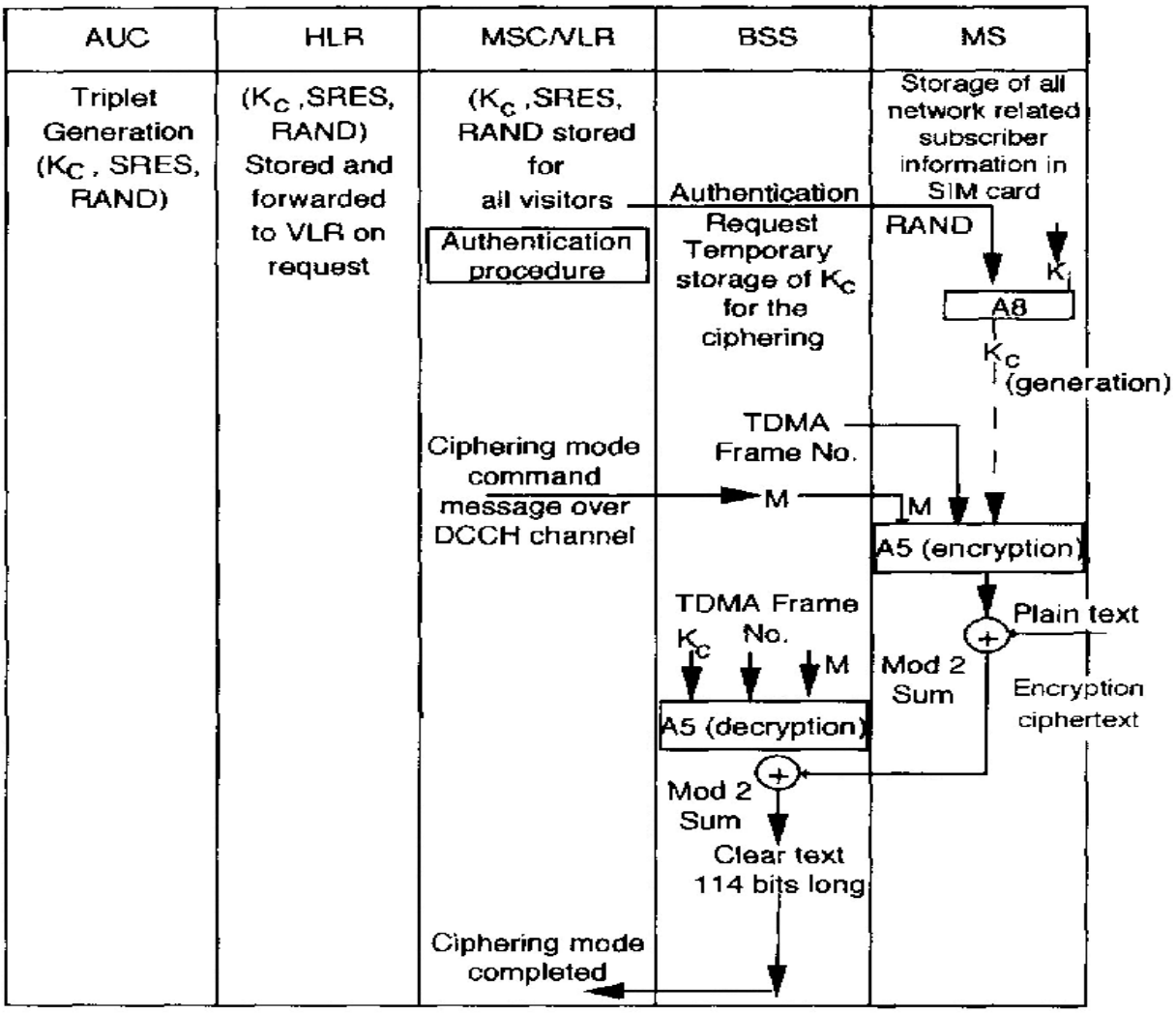


Fig.III.4 : Le processus de chiffrement/déchiffrement par séquence.

III. Les algorithmes de chiffrement :

L'algorithme principal à étudier est donc **A5**, cependant ces spécifications n'ont jamais été rendues publiques. Il existe différentes implémentations de cet algorithme **A5/1** et **A5/2**. Le design de c'est deux algorithmes a été obtenu grâce à du reverse engineering, en 1998 par Marc Briceno et Ian Goldberg.

III.1.L'algorithme A5/1 :

III.1.1.Description de l'algorithme A5/1:

A5/1 est en fait un générateur pseudo-aléatoire d'un flux de bits ; ce flux de bits est combiné par un ou exclusif avec les données à chiffrer. C'est le principe du One Time Pad, avec un masque pseudo-aléatoire et donc non aléatoire ; le déchiffrement se pratique de façon identique au chiffrement, par la génération du même flux, et un ou exclusif avec le texte chiffré.

A5/1 est constitué de trois LFSR (Linear Feedback Shift Registers, c'est-à-dire registres à décalage à rétroaction linéaire), de tailles respectives 19, 22et 23 bits, totalisant un état interne de 64 bits.

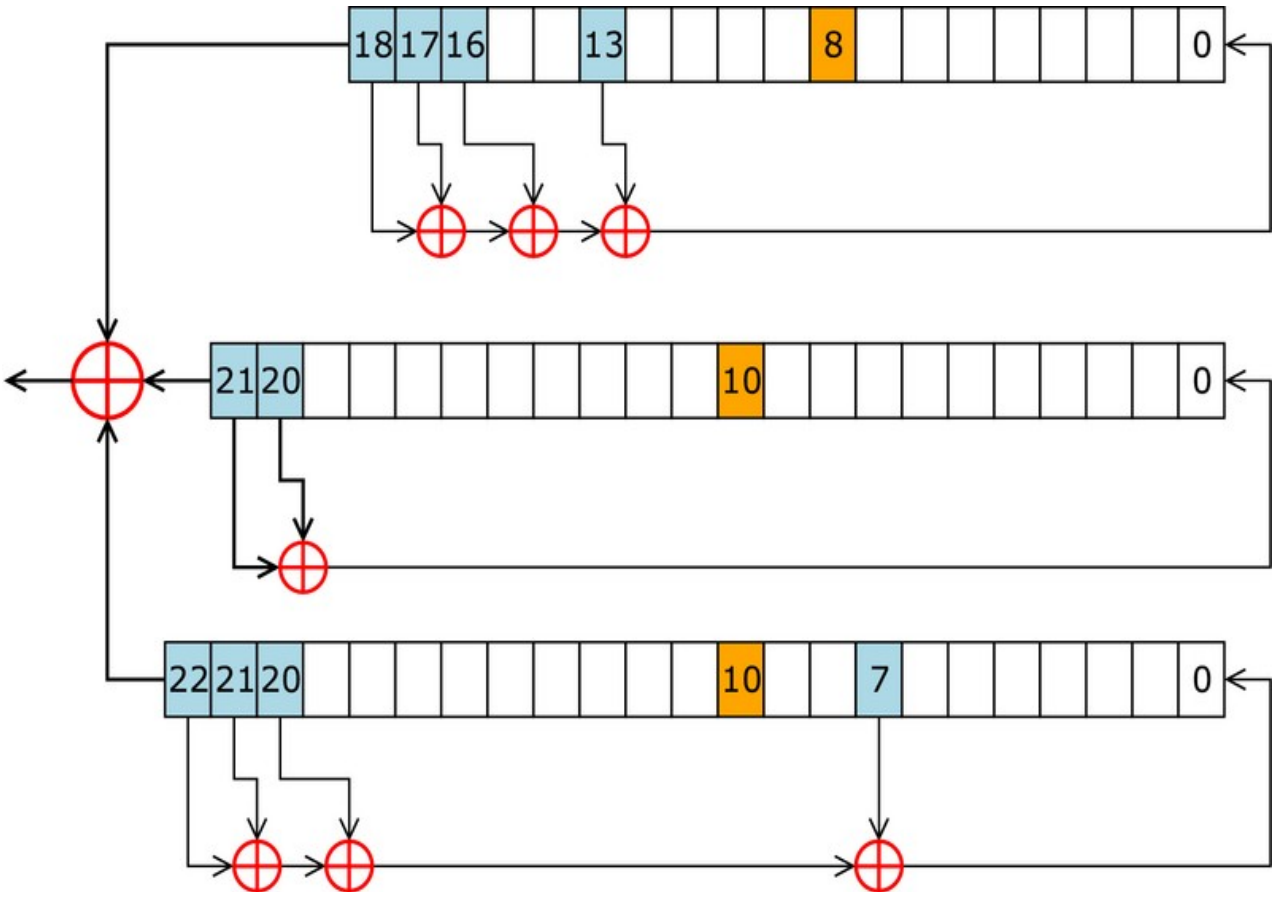


Fig.III.5. Registres à décalages deA5/1

Les trois LFSR ont pour polynômes de rebouclages les trois polynômes suivants :

$$P1=x19 \oplus x5 \oplus x2 \oplus x \oplus 1.$$

$$P2=x22 \oplus x \oplus 1.$$

$$P3=x23 \oplus x15 \oplus x2 \oplus x \oplus 1.$$

Ces trois polynômes sont primitifs et le degré de chacun est égal à la taille du registre correspondant. De plus, ces polynômes sont relativement « creux »,

c'est-à-dire que la fonction de rebouclage se calcule avec un nombre réduit de portes ou exclusif

III.1.2. Le mécanise de pointage :

Toute la force de **A5/1** réside dans son avancement sélectif de ces trois registres ; en effet, le mode d'opération de A5/1 s'effectue ainsi : à chaque cycle, un test est effectué pour chaque registre, test qui décide si le registre est avancé d'une unité ou pas. Pour ce test, un bit de chaque registre (respectivement, les bits 8, 10 et 10) est extrait, et la majorité de ces trois bits est calculée. Les registres dont le bit extrait est en accord avec cette majorité, sont décalés d'une unité. Ainsi, à chaque cycle, au moins deux des trois registres sont décalés. Une fois ces déplacements effectués, le bit terminal de chaque registre (respectivement, les bits 19, 22 et 23) est extrait, et le ou exclusif de ces trois bits est le bit de sortie d'**A5/1** pour ce cycle.

Une communication GSM est découpée en trames, c'est-à-dire des blocs de taille fixe; chaque trame est chiffrée indépendamment. Ce système permet de partager le même canal radio entre plusieurs communications, et autorise une synchronisation plus efficace entre les intervenants. Chaque trame est numérotée, en commençant à 0 ; ce numéro est un nombre binaire de 22 bits.

Chaque trame comporte deux champs de données de 114 bits ; chacun chiffre un des deux sens de la communication (car une communication téléphonique est bidirectionnelle)

III.1.3.Introduction de Kc et le numéro de trame :

Pour chaque trame, **A5/1** est réinitialisé ainsi :

- les trois registres sont initialisés à 0 ;
- la clé de session de 64 bits est rentrée, bit par bit, de la façon suivante : le bit est combiné par ou exclusif avec le bit 1 de chaque registre, puis les trois registres sont décalés d'une unité (le contrôle d'avancement est désactivé pendant cette procédure) ;
- le numéro de la trame est introduit de la même façon ;

- le contrôle d'avancement est alors activé ; **A5/1** tourne pendant 100 cycles à vide, c'est-à-dire que les 100 premiers bits de flux sont ignorés ;
- ensuite, **A5/1** produit les 228 bits nécessaires au chiffrement.

III.2.L'algorithme A5/2 :

III.2.1.Description de l'algorithme A5/2

. **A5/2** est composé de 4 registres LFSR respectivement de R1 :19bits, R2 :22bits, R3 :23bits et R4 :17 bits. Chaque registre possède sa propre source de données et sa fonction de sortie et leurs polynômes irréductibles sont respectivement :

P1=x19 $\oplus$x5 $\oplus$x2 $\oplus$x $\oplus$1.

P2=x22 $\oplus$x $\oplus$1.

P3=x23 $\oplus$x15 $\oplus$x2 $\oplus$x $\oplus$1.

P4= x17 $\oplus$x5 $\oplus$1.

Quand R4 est pointé, le XOR de R4 (17-1=16) et R4 (17-5-1=11) est calculé, puis le registre est décalé d'un bit vers la droite, et la valeur du XOR est placé dans R4.

Donc à chaque étape les différents registres sont pointés de la même façon que R4. Un bit de sortie est alors mis en place à la sortie de **A5/2**. Après l'initialisation, 100 bits de sortie sont jetés, et les 228 bits suivants sont utilisés pour la clef de chiffrement.

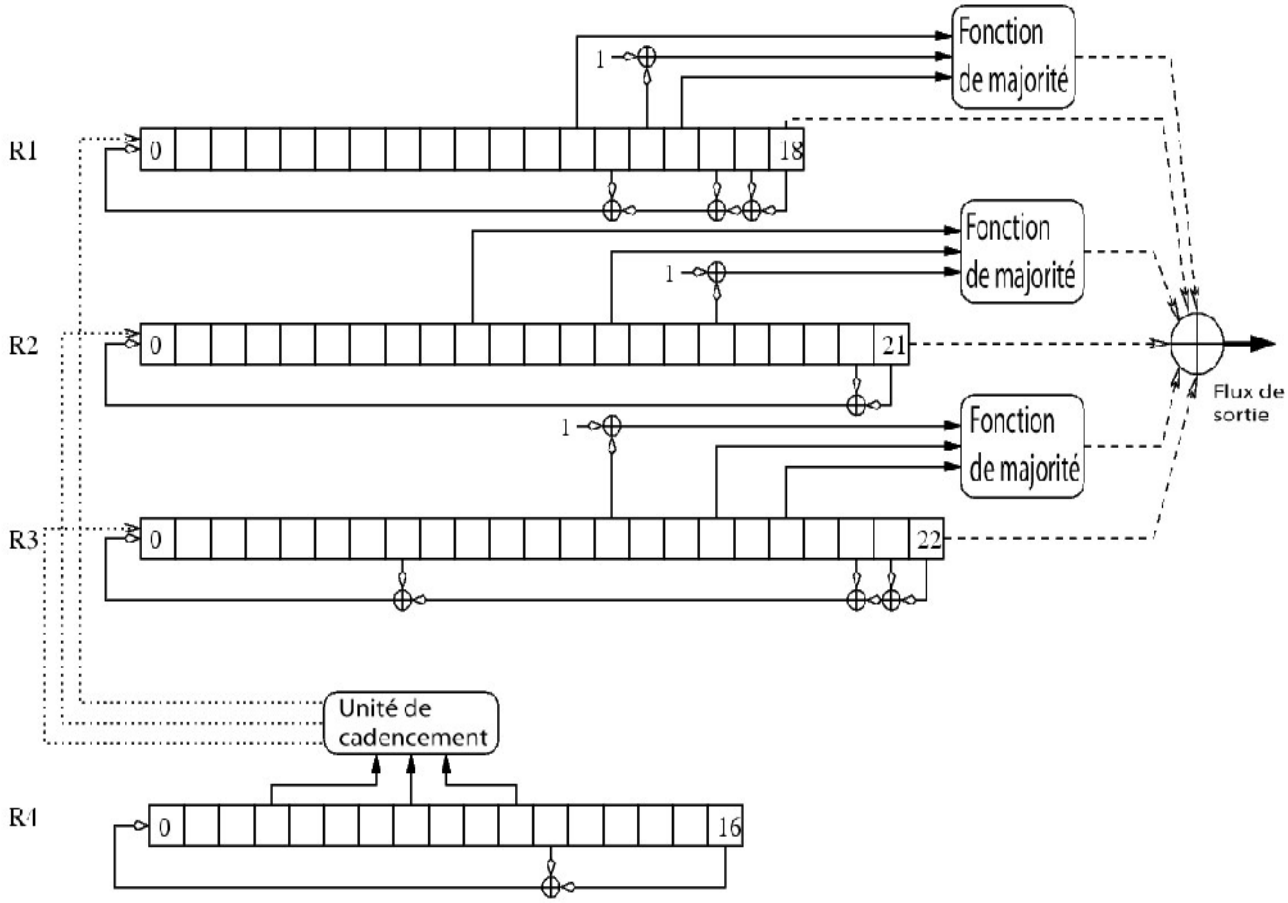


Fig.III.6. Registres à décalages de A5/2

III.2.2.Le mécanise de pointage

Après que le premier pointage ait été réalisé, le 1er bit de sortie est prêt à la sortie de **A5/2**. Le mécanisme de pointage se déroule comme suit : R4 vérifie le pointage des autres registres, après la vérification les registres exécutent les bits d'entrée de l'unité de pointage (Clocking unit) R4 [3], R4 [7] et R4 [10].

R1 est pointé ssi R4 [10] est conforme à la majorité,

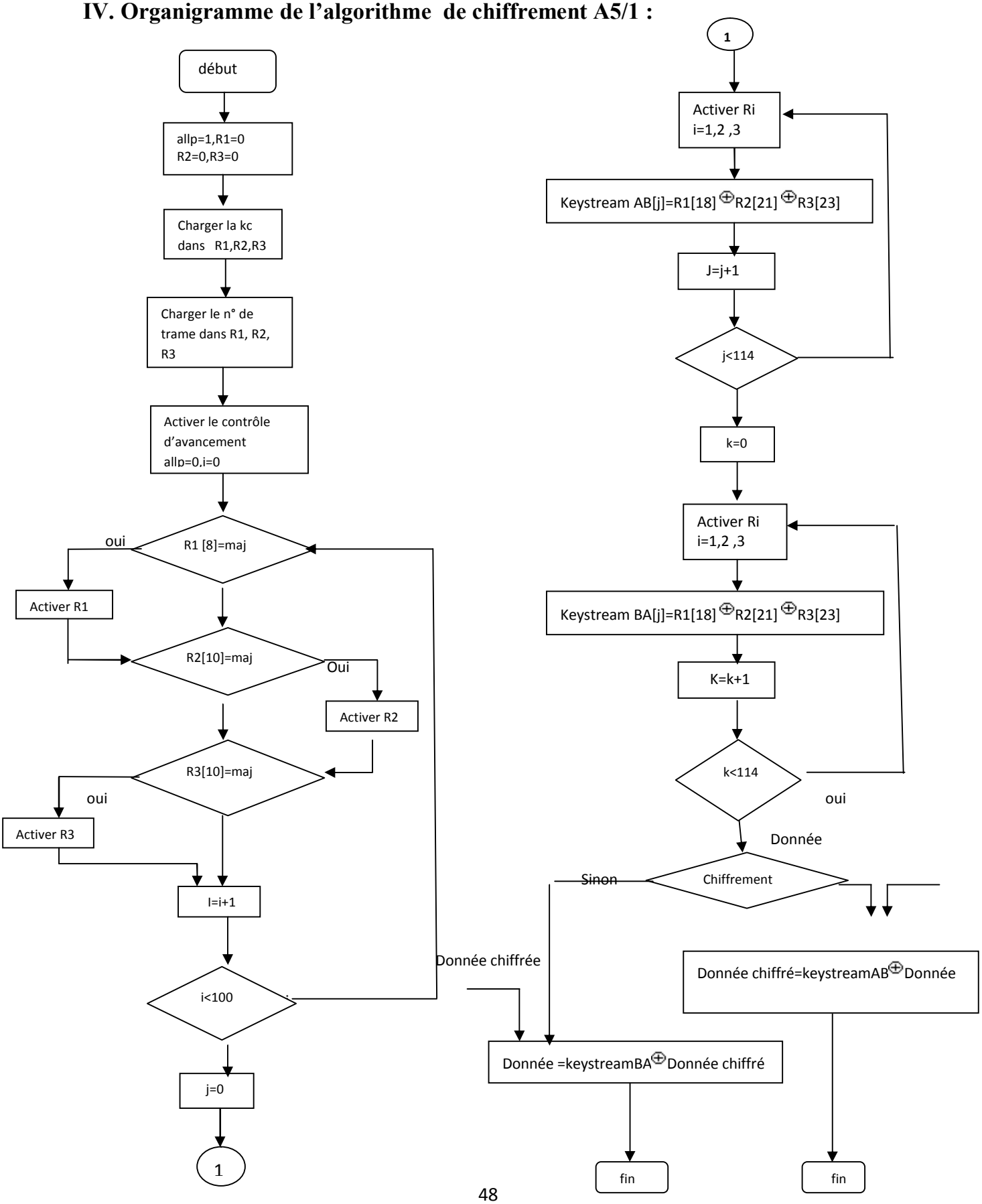
R2 est pointé ssi R4 [3] est conforme à la majorité.

R3 est pointé ssi R4 [7] est conforme à la majorité.

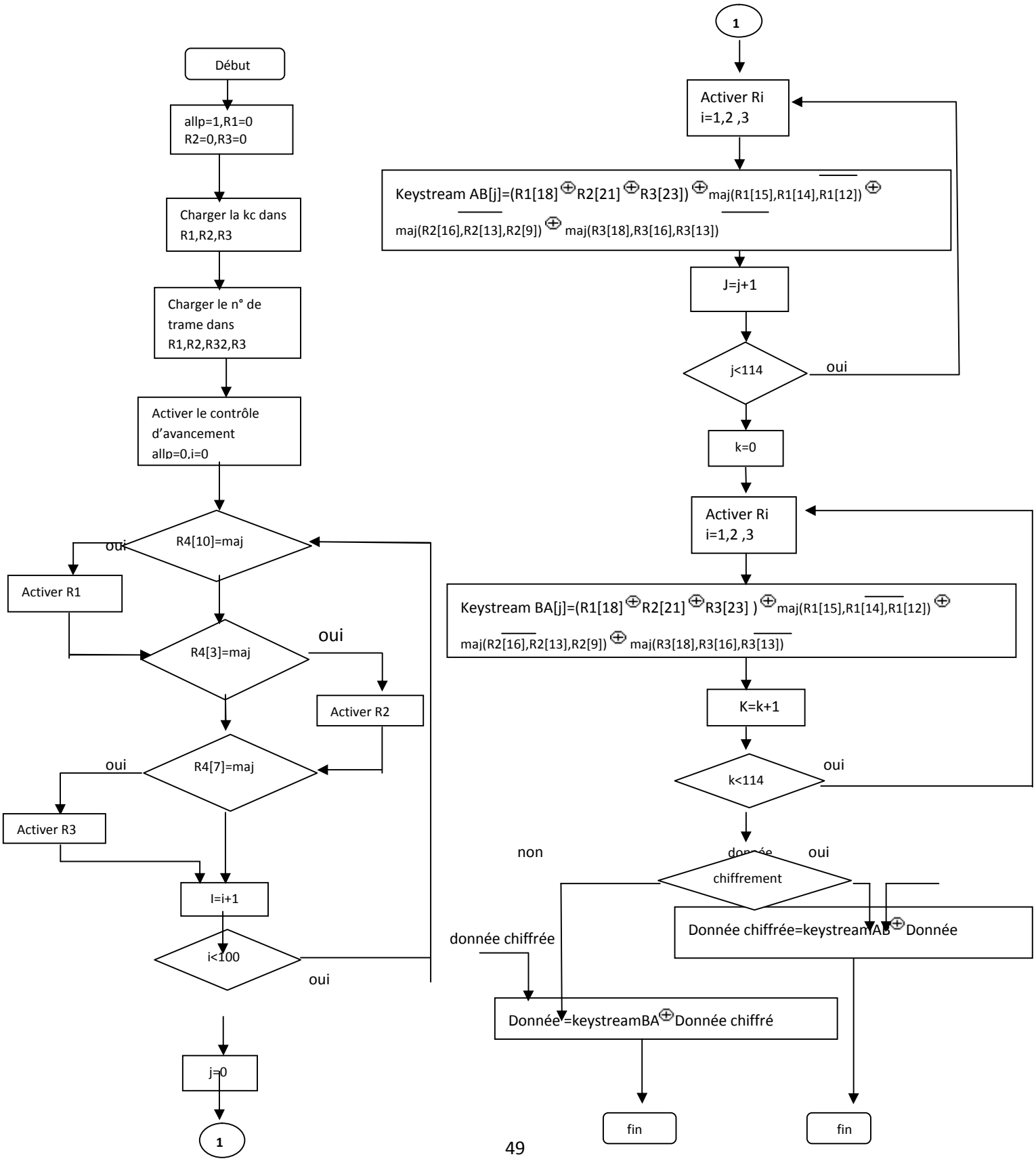
III.2.3.La génération de la séquence de chiffrement (keystream)

Une fois que le pointage est réalisé, un bit de sortie est calculé de la manière suivante : Dans chaque registre la majorité de deux bits et le complément d'un troisième est calculé ; les résultats et le bit le plus à droite de chaque registre sont ensuite XORé afin d'obtenir la sortie (Fig .III.6). **A5/2** produit 228 bits de la clef de chiffrement. Le premier bloc de 114 bits est utilisé pour chiffrer le lien du réseau de communication vers l'utilisateur, et le second block réalise le chiffrement inverse que le premier. Le chiffrement est réalisé grace à un simple XOR du message avec la clef de chiffrement.

IV. Organigramme de l'algorithme de chiffrement A5/1 :



V. Organigramme de l'algorithme de chiffrement A5/2 :



I. Introduction :

Dans le chapitre précédent, nous avons présenté l'architecture et le fonctionnement de l'algorithme de chiffrement A5. A présent, nous allons effectuer son implémentation et son interface montrant l'étape de chiffrement/déchiffrement. Pour ce faire, nous devons au préalable décrire l'environnement de développement intégré Builder C++ sous Windows, en utilisant le langage de programmation c++.

I.1.Description du système d'exploitation Windows :

Le système d'exploitation Windows est un environnement graphique organisé en fenêtres. Il offre à l'utilisateur une interface graphique multifenêtrage et une gestion multitâches, qui facilite le travail des développeurs.

I.2.Description du l'environnement de développement Builder c++:

Suite au succès de Delphi lancé en 1995, Borland a repris sa philosophie, l'interface des applications et la bibliothèque des composants visuels de ce dernier pour l'adapter depuis le langage Pascal Objet vers C++.

Builder C++ permet de réaliser de façon très simple l'interface des applications et de relier aisément le code utilisateur aux événements Windows en utilisant un ensemble de composants visuels prêts à l'emploi.

Il est doté d'outils de base de données utilisés pour développer de plus puissantes applications et cela grâce aux contrôles orientés données. Ces derniers permettent de voir les données pendant la conception de l'application.

II. Interface graphique de l'application :

II.1. fenêtre principale :

La fenêtre principale de notre application est donnée par la figure suivante :

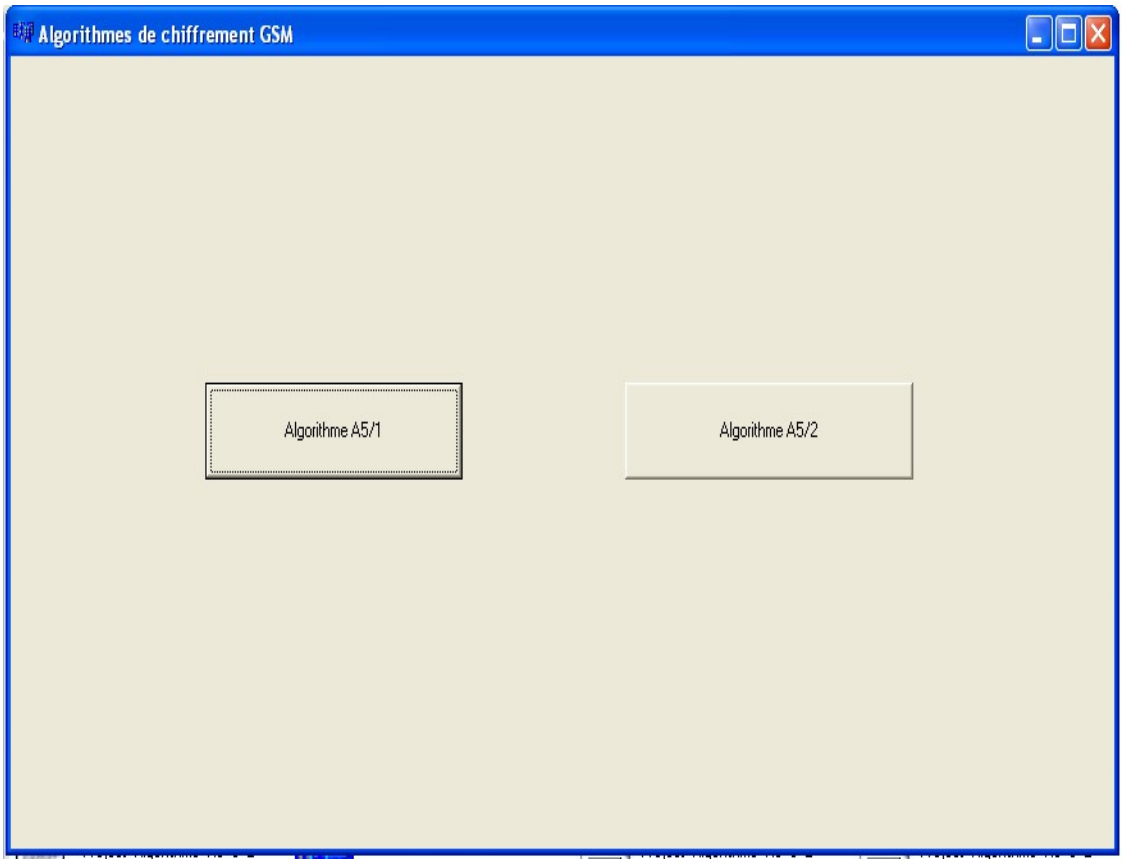


Fig.IV.1 : Fenêtre principale.

Cette fenêtre, nous permet d'accéder aux services offerts par l'application. Elle est constituée de :

-Une barre de titre qui contient le titre de l'application et les boutons *Réduire, Agrandir* et *Fermer.*

-Deux boutons raccourcis pour le choix de l'algorithme de chiffrement, soit algorithme A5/1 ou bien algorithme A5/2.

II.2.Les Interfaces des algorithmes A5/1 et A5/2 :

La fenêtre principale nous permet d'accéder aux intefaces des algorithmes de chiffrement A5/1 et A5/2, en appuyant respectivement sur les boutons [Algorithme A5/1] et [Algorithme A5/2].

Ces deux iterfaces sont constituées de :

- Une barre de titre qui contient le titre de l'application (AlgorithmeA5/1) et *Réduire, Agrandir* et *Fermer.*
- Quatre cases pour introduire :
    - La clé de chiffrement Kc.
    - Le numéro de trame.
    - La trame (texte en clair).
    - La trame chiffrée
- Un bouton [Chiffrer] pour chiffrer la trame.
- Un bouton [Déchiffrer] pour déchiffrer la trame chiffrée.
- Un bouton [Retour menu] pour retourner à la fenêtre principale de l'application.

II.2.1.L'interface de l'algorithme de chiffrement A5/1 :

L'interface de l'algorithme A5/1 de notre application est donnée par la figure suivante :

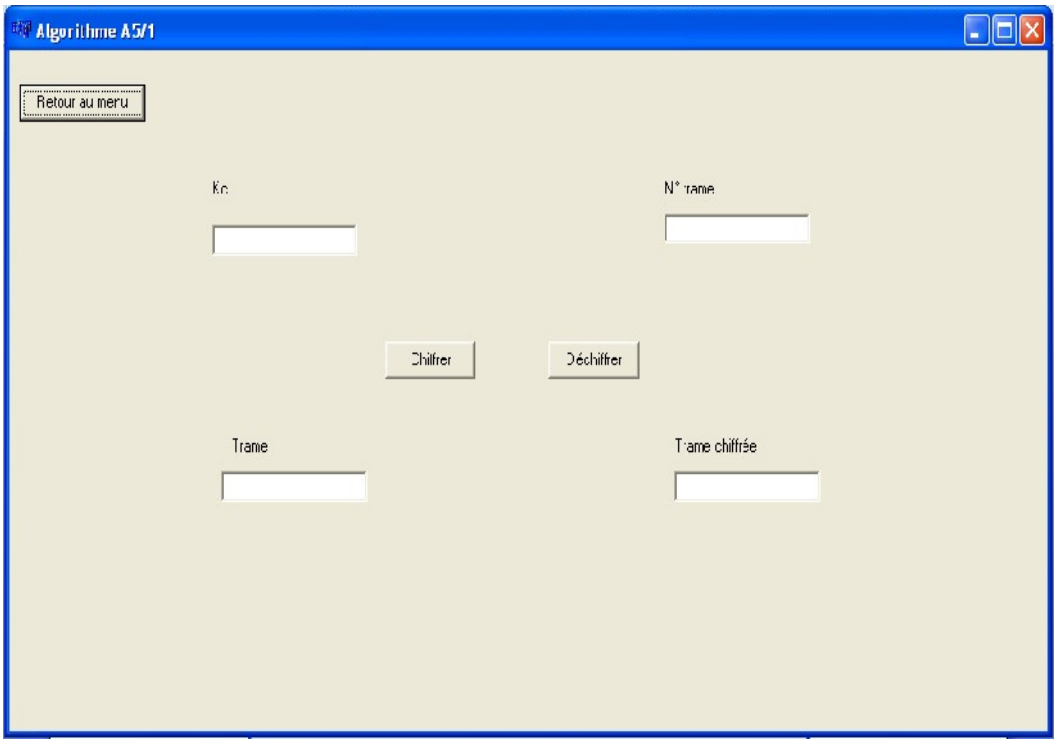


Fig.IV.2 : L'interface de A5/1

II.2.2.L'interface de l'algorithme de chiffrement A5/2 :

L'interface de l'algorithme A5/2 de notre application est donnée par la figure suivante :

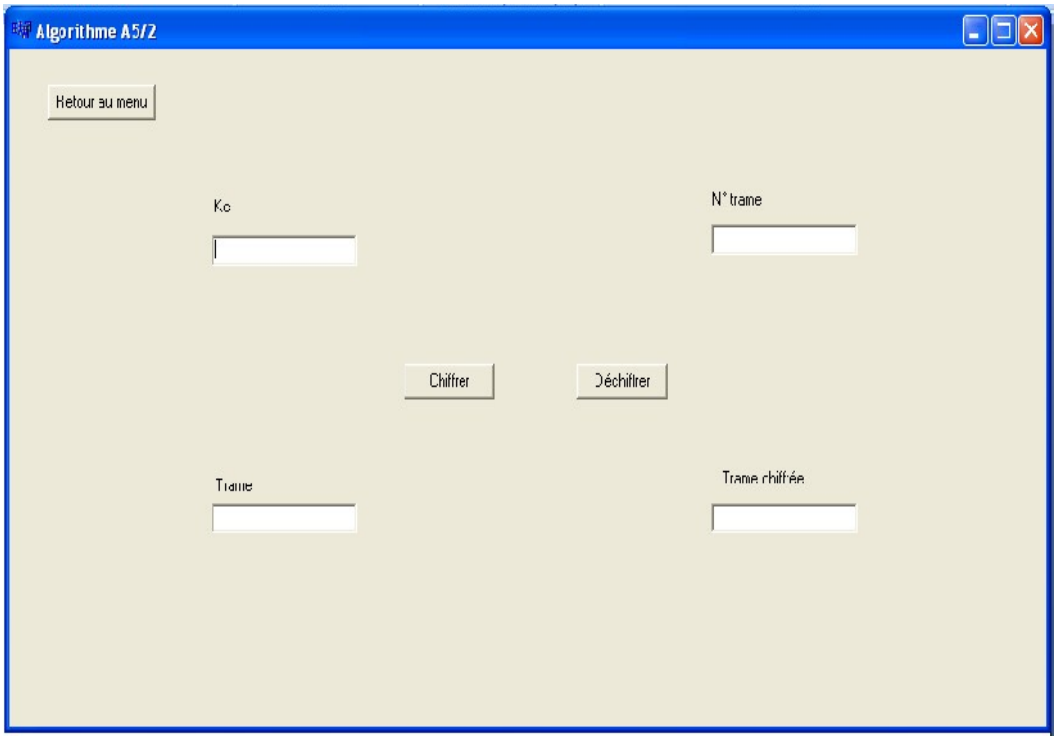


Fig.IV.3 : L'interface de A5/2

III. Exemple de chiffrement/déchiffrement par l'algorithme A5/1 :

En introduisant sur l'interface de l'algorithme A5/1:

- la clé Kc: ABCDDCBA
- le numéro de trame: 100
- la trame: l'électronicien

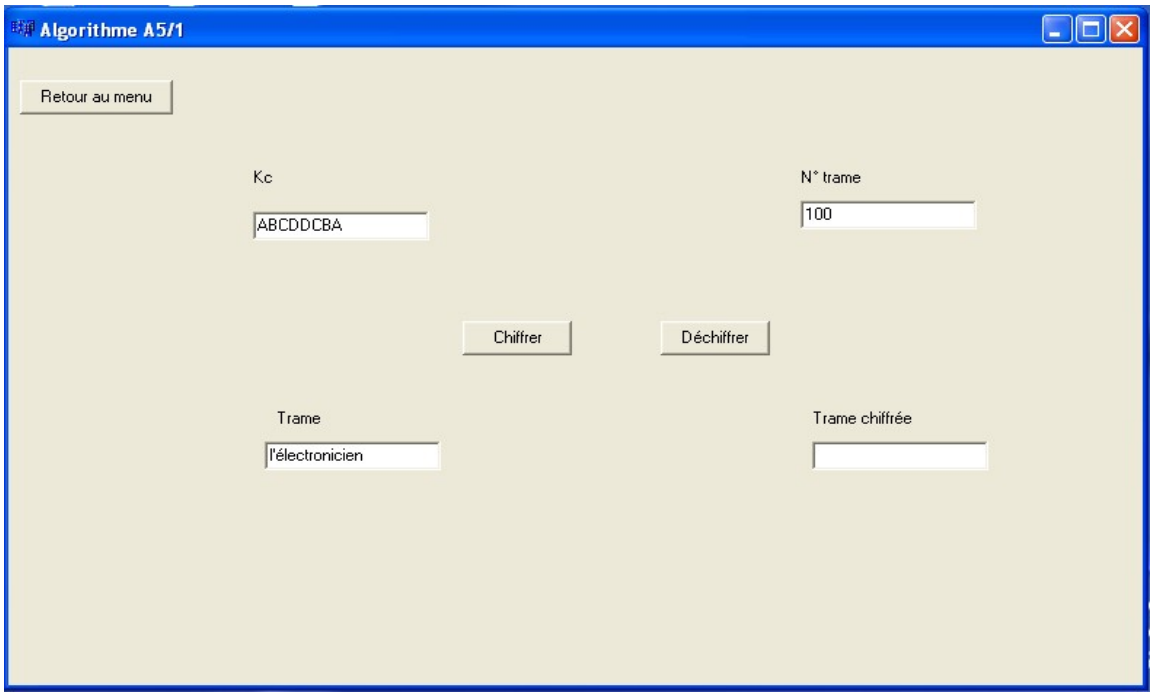


Fig.IV.4 : L'interface de l'algorithme A5/1 avant le chiffrement

En appuyant sur le bouton « chiffrer », on aura la « trame chiffrée ».

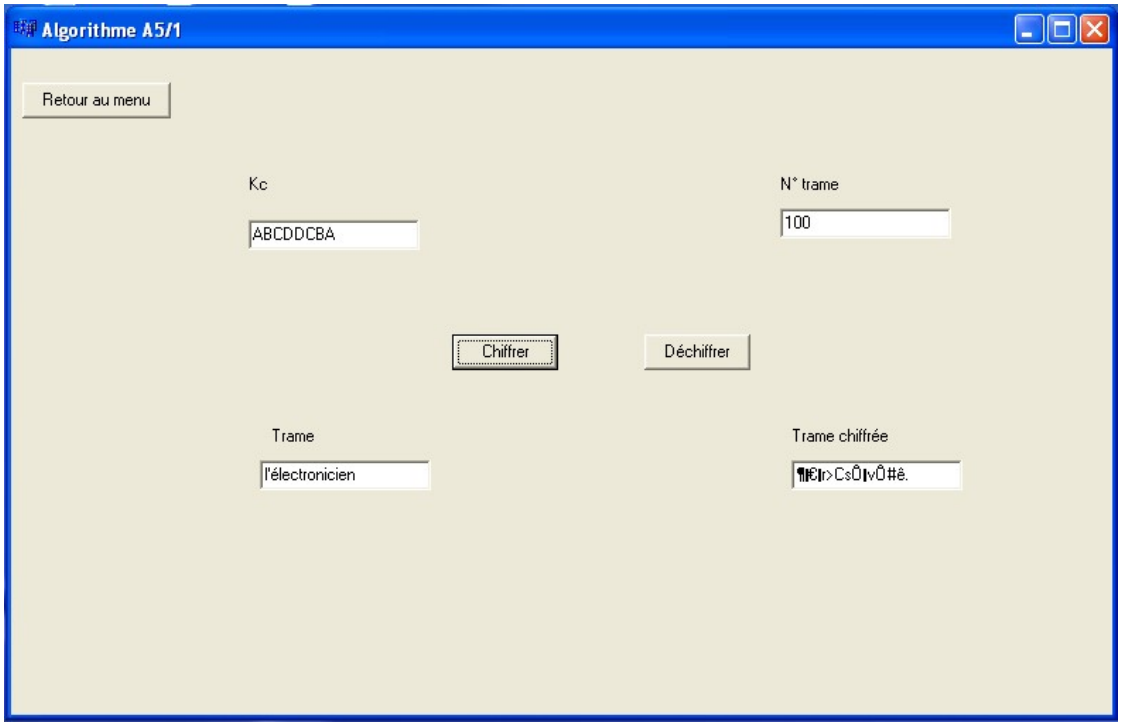


Fig.IV.5 : Fenêtre de l'algorithme A5/1 après le chiffrement

A partir de la trame chiffrée, en appuyant sur le bouton déchiffrer on récupère la trame initiale.

GLOSSAIRE

A3 : Algorithme de mise en œuvre dans la procédure d'authentification.

A5 : Algorithme de chiffrement/ déchiffrement de l'ensemble des informations transmises via l'interface radio.

A8 : Algorithme de génération de la clé Kc.

AUC (Authentification Center) :

Centre d'authentification des abonnés d'un réseau GSM.

BSC (Base Station Controller) :

Contrôleur de la station base.

BSS (Base Station Sub-system):

Sous- système radio composé d'un BSC et d'une BTS.

BTS (Base Transceiver Station) :

Equipement composé des l'émetteurs et récepteurs radio constituant l'interface entre le BSC et les mobiles.

FDMA (Frequency Division Multiple Access):

Technique de transmission permettant de transmettre plusieurs flux simultanés par répartition de fréquence.

FN (Frame Number) :

Numéro de la trame courant dans l'hypertrame définie pour une BTS.

HLR (Home Location Register) :

Enregistreur de localisation nominal. Base de données contenant les localisations d'abonnés du réseau GSM.

IMEI (International Mobile Equipement Identity) :

Identité internationale spécifique d'un terminal.

IMSI (International Mobile Subscriber Identity) :

Identité internationale d'un abonné inscrit dans la carte SIM.

Kc : Clé de chiffrement.

Ki : Clé d'authentification.

ME (Mobile Equipement) :

Le terminal mobile.

MS (Mobile Station) :

Terminal GSM muni de la carté SIM et susceptible de fonctionner sur un réseau.

MSC :(Mobile- services Switching Center):

Commutateur fixe adapté GSM permettant de gérer les appels.

RAND : Nombre aléatoire émis par le réseau vers le MS pour l'authentification.

SIM (Subscriber Identity Module) :

Carte s'insérant dans un terminal GSM et contenant toutes les informations d'abonnement.

SRES *(Signed Response):*

Résultat de l'authentification calculé à partir du RAND en appliquant l'algorithme A3.

TDMA (Time Division Multiple Access):

Technique de transmission permettant de transmettre plusieurs flux simultanés par répartition de temps.

TMSI (Temporary Mobile Identity) :

Identité temporaire attribuée par le réseau à une MS et utilisée pour les transactions sur l'interface radio.

VLR (Visitor Location Register) :

Enregistreur de localisation des visiteurs

GPRS (General Packet Radio Service):

Système réseau transférant les données en paquets, il offre une meilleur sécurité et permet l'utilisation d'Internet via le mobile (consultation d'email, surfer sur le net…).

UMTS (Universal Mobile Telecommunications System) :

désigne une technologie permettant des améliorations substantielles par rapport au GSM.

Conclusion générale

Le réseau GSM a révolutionné le monde à plus d'un trait par l'introduction de la mobilité et le passage de l'analogique au numérique par rapport au réseau fixe.

Le groupement GSM a élaboré des procédes permettant de proteger les données transmises via l'interface radio, contre les menaces externes :

- Authentification de chaque abonné en utilisant l'algorithme A3.
- Chiffrement des communications par l'algorithme A5.

Toutefois le GSM n'offre pas de sécurité de bout en bout, il comporte une étape intermediaire (en BTS) dont les données sont déchiffrées ; les algorithmes de chiffrement sont cassables ainsi que la ressource radio est menacée par des brouillages et d'interceptions.

L'avénement du GPRS et l'UMTS ont permet l'introduction de services supplimentaires(navigation sur internet, la visotéléphonie…), l'accroit du taux de transfret des données respectivement : 171,1kb/s et 2Mb/s par rapport au GSM, ainsi que des procédes de sécurite plus efficaces en l'encurrence pour l'UMTS :

- Authentification : mutuelle et l'algorithme dépond de l'opérateur.
- Confidentialité :

  Nouvel algorithme de chiffrement par bloc :KASUMI.

  Clé de chiffrement plus longue : 128 bit.

En fin, nous pensons avoir atteint les objectifs fixés au départ et nous esperons que ce travail sera d'un grand interét pour toute personne qui le consultera.

Bibliographie

[1].Asha Mehrotra **« GSM system engineering »** Artech House, Inc. Boston London , édition **1997**

[2]. Thèse d'Ingénieur par Harchaoui Sofiane et Beladjal Oussalem**« *La sécurité dans les réseaux sans files*»** Université Mouloud Mammeri de Tizi Ouzou promotion **2004-2005**.

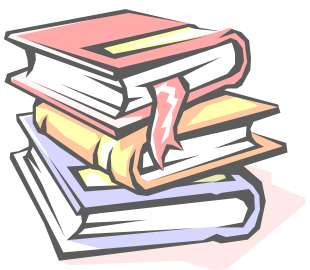
[3]. Thèse d'Ingénieur par Hassina Chaouche et Djamila Kadouche **« Sécurité réseaux »** Université Mouloud Mammeri de Tizi Ouzou promotion **2003**.

[4].Thése Doctorat Paris 7 par Thomas Pornin« **Implantation et optimisation des primitives cryptographique »** Département d'Informatique de l'École Normale Supérieure,45 rue d'Ulm, 75005 PARIS, promotion **2001**

[5]. Thèse d'Ingénieur par Ilan NACMIAS «**Cryptanalyse instantané de texte chiffré via l'utilisation de l'algorithme de communication GSM. (D'après un document de Elad BARKAN, et Eli BIHAM) »** Ecole Supérieur d'Informatique Paris, promotion SUPINFO **2005**

[6] http://www.cryptome.org/gsm-a512.htm .

[7] http://www.rocq.inria.fr/canteaut/.htm



ANNEXE

Acheminement des appels :

En GSM, trois types d'appels peuvent se présentés :

- Appel d'un mobile vers un mobile.
- Appel d'un mobile vers le réseau fixe.
- Appel d'un abonné du réseau fixe vers le réseau GSM.

Nous nous intéresserons au deux derniers cas.

a) : Appel d'un mobile vers le réseau fixe. (appel sortant)

L'abonné compose le numéro de son correspondant qui se trouve dans le réseau fixe, sa demande passe tout d'abord par la BTS de la cellule où il se situe en utilisant le canal d'accès aléatoire(RACH), le BSC reçoit les signalisations venant de la BTS et les transmit au MSC ainsi il répond sur le canal d'allocation des ressources (AGCH). Après l'établissement de liaisons de signalisation entre Le MSC et la MS, cette dernière envoie une demande de l'établissement d'un appel au MSC/VLR en utilisant le canal SDCCH. Le MSC/VLR vérifiera les droits de l'abonné, si l'abonné rempli les conditions, le MSC/VLR transmit l'appel au réseau public et demande au BSC d'allouer un canal TCH pour la communication.

b) : Appel d'un abonné de réseau fixe vers le réseau GSM (appel entrant).

L'abonné de réseau fixe compose le numéro MSISDN de son correspondant (numéro d'appel de MS), ce numéro est analysé dans le central de PSTN qui détermine qu'il s'agit d'un appel à destination d'un l'abonné d'un réseau GSM. Une liaison s'établie avec le commutateur passerelle GMSC, ce dernier analyse le numéro formé(MSISDN) et interroge le HLR qui le transpose en IMSI. Le HLR détermine également le MSC/VLR dont la MS se trouve, ainsi que son état (libre, occupée, éteinte).

Le MSC/VLR envoie le numéro de roaming de station mobile MSRN au HLR qui le transmit à son tour au GMSC, ce dernier achemine l'appel directement à destination de MSC/VLR qui sait dans quelle zone de localisation LA la station mobile se trouve ; un

message de recherche (paging message) est envoyé au BSC qui contrôle cette zone LA.

Le BSC diffuse le message de recherche vers les différentes BTS de LA, qui diffusent a leurs tour ce message sur le canal logique PCH sur l'interface radio. Lorsque la station mobile détecte le message (paging), elle envoie une demande de canal de signalisation SDCCH et le BSC répond à la demande en utilisant le canal AGCH. Un canal de trafic TCH est alloué a la MS et le SDCCH est libéré, le mobile sonne et la communication s'établie lorsque l'abonné répond.

NB : lorsque il s'agit d'un appel de mobile vers un autre mobile les procédures d'établissement de l'appel restent les mêmes que précédemment sauf que le GMSC au lieu d'être connecter a un central PSTN, il est connecté à un autre MSC/VL où l'appel arrive.

La mobilité:

La mobilité dans le réseau GSM est définie comme un service qui permet au usagers de services télécoms (émission/réception) sur une zone de couverture.
Cette mobilité permet aussi de poursuivre une communication tout en se déplaçant ; elle est assurée par trois mécanismes qui sont :

- Le mécanisme de transfert inter/intra-cellulaire (**HANDOVER**)
- Le mécanisme de sélection/reséléction de cellules.
- Le mécanisme de gestion de la localisation.

Le HANDOVER :

Le HANDOVER est le processus par lequel une communication établie est maintenue alors que le mobile se déplace à travers le réseau cellulaire ce qui implique que la communication puisse passer d'un canal physique à un autre canal physique avec le minimum d'interruptions (au moyenne < 10 ms).

Le HANDOVER est un transfert inter-cellulaire ; en cas de petites cellules les HANDOVER peuvent se multiplier et entraîner une charge grandissante pour le réseau .

Il existe aussi un type de HANDOVER intra-cellulaire imposé par la qualité de service de la communication.

le modèle OSI (Open System International) :

C'est la base de référence pour tout système de communication, il a été mis au point par l'Organisation Internationale des Standards, il a pour but d'assurer une compatibilité entre les réseaux propriétaires et que la communication entre tous les réseaux soit possible et efficace.

Le modèle OSI est composé de sept couches, chacune d'entre elles a sa propre fonction, les protocoles utilisés dans chacune des couches collaborent pour assurer une communication efficace. Les trois premières couches appelées couches utilisateurs et les trois dernières appelées couches de traitement.

couche	nom	
1	Application	Couches utilisateurs
2	Présentation	
3	Session	
4	Transport	
5	Réseau	Couches de traitement
6	Liaison	
7	Physique	

La cryptologie : est la science des messages secrets, c'est un outil primordial de la sécurité. Ce mot est un anglicisme et il inclus la cryptographie ainsi que la cryptanalyse.

La cryptanalyse : est la technique qui permet de déduire le texte en clair à partir d'un texte chiffré, sans en connaître la clef.

La cryptographie : est l'ensemble des techniques de chiffrement, ou ensemble des méthodes utilisées pour cacher le sens d'un message. Le terme est souvent appliqué

dans un sens plus général pour signifier la science des messages secret, et est employé comme synonyme de cryptologie..

Un algorithme : est une séquence d'opérations visant à la résolution d'un problème en un temps fini (mentionner la condition d'arrêt).

Chiffrer : Transformation d'un texte, dans le but d'en cacher le sens. (~Coder=crypter).

Déchiffrer : Transformer un message chiffré en un message clair conforme à l'original. Ce terme s'applique en principe au destinataire qui connaît la clef nécessaire pour obtenir le texte en clair, mais on l'utilise dans le cas d'un intercepteur ennemi qui opère le déchiffrement par la cryptanalyse. (~Décoder=décrypter).

Texte clair et texte chiffré : respectivement texte avant sa présentation à l'algorithme de chiffrement, et résultat du texte après chiffrement.

LFSR : ***Linear Feedback Shift Register*** (Registre de Changement de Réactions Linéaire). Un registre à décalage dont l'entrée des données est produite comme XOR ou XNOR de deux éléments ou plus dans la chaîne de registre ~ Système de Chiffrement.

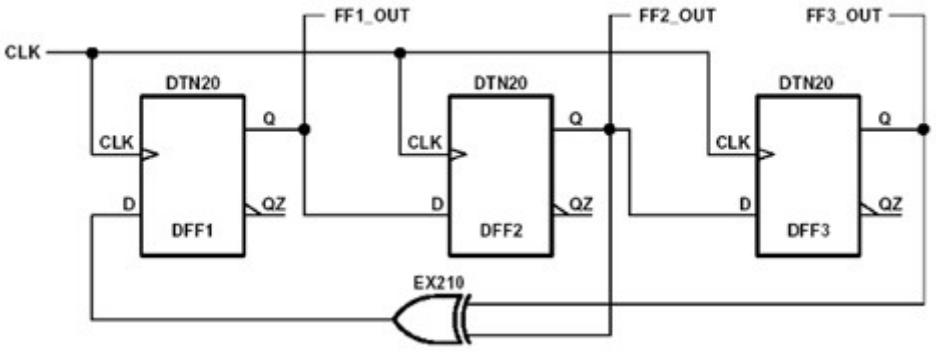


Fig : schèma d'un LFSR