NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

AUTHENTICATION AND SECURITY IN GSM

Graduation Project
EE- 400

GHASSAN A. EL_TAHA

Supervisor: PROF. FAKHREDDIN MAMEDOV

Nicosia – 2003

TABLE OF CONTENTS

AKNOWLEDGMENT

I would first like to sincerely and especially thank my supervisor Prof. Dr. Fakhreddin Mamedove who gave me from his precious time and consolation. Without her guidance providing a spur to my confidence, I am sure I would not have been able to produce what I finally did.

To whom I can not imagine myself to be without their guidance and continuous support ,to my parents who helped me to know myself ,know my own abilities ,take advantage of it. to my family especially my brother TAHA who helped me in the preparation of this research.

My research led me to so many different people, friends, and materials, that I do not know who to thank first. I will start with khaled almasri, Muhammad Qunj, malath al aghaa, Computer Engineer Ahmad El_Taha.

For taking the time from his time commitments and consulting me by telephone or face to face, I largely appreciated the help of hani jaber.

My appreciation also goes to Dr.s and assistants at the Department of Electrical and Electronic Engineering who provided me with needed knowledge to reach my present stage.

ABBREVIATION

ISDN	Integrated Services Digital Network
GSM	Global System for Mobile communications
CEPT	Conference of European Posts and Telecommunications
JDC	Japanese Digital Cellular
PDC	Personal Digital Cellular
DCS	Digital Cellular System
NADC	North American Digital Cellular
TACS	Total Access Communication System
AMPS	American Mobile Phone System
NMT	Nordic Mobile Telephony
MoU	Initial Memorandum of Understanding
ETSI	European Telecommunications Standards Institute
CEPT	Conference of European Posts and Telecommunications
BTS	Base Transceiver Station or Base Station
BSC	Base Station Controller
PIN	Personal Identification Number
IMSI	International Mobile Subscriber Identity SIM Subscriber Identity Module
OSS	Operation and Support Subsystem
NSS	Network and Switching Subsystem
BSS	Base Station Subsystem
MS	Mobile Station
PCS	Personal Communications Systems
LA	Location Area
CGI	Cell Global Identity number
GIWU	GSM Interworking Unit
OSS	Operation and Support Subsystem
IMEI	International Mobile Equipment Identity
EIR	Equipment Identity Register
AuC	Authentication Center
HLR	Home Location Register
GMSC	Gateway Mobile services Switching Center
MSC	Mobile services Switching Center
PSTN	Public Switched Telecommunications Network
MSRN	Mobile Station Roaming Number
OAM	Operation, Administration and Maintenance
CM	Communication Management
MM	Mobility Management
RR	Radio Resources management
LAI	Location Area Identity
PN	pseudo-noise
XOR	exclusive or
LFSR	Linear feedback shift register
CFB	cipher feedback
CBC	cipher block chaining

ECB	electronic code book
FACCH	Fast Associated Control Channel
CCH	control channel
TCH	traffic channel
TDMA	time division multiplexing access
FDMA	frequency division multiplexing acess
RPE-LTP	Regular Pulse Excitation Long-Term Prediction
TMSI	Temporary Mobile Subscriber Identity
RSA	Rivest-Shamir-Adleman
CRHF	Collision resistant hash function
DSA	Digital Signature Algorithm
NIST	National Institutes of Standards and Technology
SHA	Secure hash algorithm
OWHF	One-way hash function
MDC	Modification Detection Codes
MAC	Message Authentication Code
DES	Data Encryption Standard
MIPS	Million Instructions Per Second
MDS	Maximum Distance Separable
GPS	global positioning system
RAND	random number
OMS	Operation and Maintenance Subsystem
A5	ciphering algorithm
A3	authentication algorithm
A8	ciphering key generating algorithm
Kc	a temporary, randomly generated ciphering key
ESN	Electronic Serial Number
Ki	individual subscriber authentication key
3DES	a variant of DES, Triple-DES
SS7	Signaling System 7 is used in most intelligent networks as a signaling protocol. SS7 is defined by ITU-T.
VLR	Visitor Location Register. The VLR stores triples generated by the HLR when the subscriber is not in his home network. The VLR then provides the MSCs with these triples when necessary.
SRES	The secret session key used to encrypt over-the-air traffic between the BTS and the MS. The Kc is generated after every authentication initialized by the MSC. The Kc is calculated from the Ki and from the random challenge sent by the MSC with the A8 algorithm. The MS and the HLR both calculate the Kc independently of each other. The Kc is never transmitted over-the-air.
ISAAC	Internet Security, Applications, Authentication and Cryptography. A small research group in the Computer Science Division at the University of California, Berkeley. http://www.isaac.cs.berkeley.edu/
COMP128	A one-way function that is currently used in most GSM networks for A3 and A8. Unfortunately the

	COMP128 algorithm is broken so that it gives away information about its arguments when queried appropriately. This is an undesired and unacceptable side effect in a one-way function.
BTS	Base Transceiver Station, a base station the MS communicates with.

ABSTRACT

Since the date where GSM standards where commercially introduced to the public, number of subscribers to GSM services are still increasing every day. This increase is due to good services GSM provides to the public, these services meets the needs of the people since it provides to be in touch with the world around at any time and at any place, also subscribers can reach any other subscriber at any time and place in the world. Nowadays the GSM service is sufficient to every single person in this whole wide world, a subscriber only needs a good mobile station and a subscriber identity given by local GSM network.

This huge number of subscribers assures that GSM is the best cellular system exists although there are many cellular systems were developed after1991.

Security of each subscriber, so his speech never be intercepted or no one would clone his identity and calls in his account, was one of the biggest problems security doers face, and especially with that huge number of subscribers. That's what I tried to present in this project.

INTRODUCTION

GSM is the most widely used cellular mobile phone system in the world with over 100 million GSM subscribers. GSM was one of the first digital mobile phone systems to follow the analog era. Widely known problems with GSM's analog counter parts were the possibility of phone fraud through cloning phones and thus calling in someone else's expense, and the possibility of someone intercepting the phone call over the air and eavesdropping on the discussion. The GSM system was supposed to correct these problems by implementing strong authentication between the MS and the MSC, as well as implementing strong data encryption for the over-the-air transmission channel between the MS and the BTS.

The GSM specifications were designed by the GSM Consortium in secrecy and were distributed only on a need-to-know basis to hardware and software manufacturers and to GSM network operators. The specifications were never exposed to the public, thus preventing the open science community around the world from studying the enclosed authentication and enciphering algorithms as well as the whole GSM security model. The GSM Consortium relied on Security by Obscurity, i.e. the algorithms would be harder to crack if they were not publicly available. According to the open scientific community, one of the basic requirements for secure cryptographic algorithms is that the security of the crypto system lies solely on the key. This is known as Kerckhoffs' assumption. The algorithm in question should be publicly available, so that the algorithm is exposed to the scrutiny of the public. According to the general opinion no single entity can employ enough experts to compete with the open scientific community in crypt analyzing an algorithm. Thus, the algorithms designed and implemented in secrecy will probably be somehow cryptographically weak and contain design faults.

Eventually, the GSM algorithms leaked out and have been studied extensively ever since by the open scientific community. Interesting facts have been discovered since then, during the cryptanalysis of the A3, A5 and A8 algorithms.

In this project I will attempt to clarify to which extent is GSM network is secure. This subject will be discussed in four chapters as follows:

The first chapter shows an overview GSM including history, system, architecture, functions, radio interface.

The second chapter presents an overview of cryptography in general including cryptography of the voice signals. Including encryption, symmetric algorithm,

asymmetric algorithm, design principles for cryptographic algorithms, importance of key lengths, hash functions, and introducing some structures of famous algorithms.

Third chapter discuses GSM security features, identifying used algorithms possible attacks on GSM security model and possible improvements concluding the level of security of GSM

Fourth chapter is concerned with authentication mechanism, signature, cloning and fraud causes and some cloning attacks.

Conclusion answers the question: Is GSM network secure or not? And sums up the whole project and emphasizes the future of the GSM security.

I. OVERVIEW OF GSM

The Global System for Mobile communications is a digital cellular communications system. It was developed in order to create a common European mobile telephone standard but it has been rapidly accepted worldwide. The GSM standard was designed to be a secure mobile phone system with strong subscriber authentication and over-the-air transmission encryption. The security model and algorithms were developed in secrecy and were never published.

1.1 History of the cellular mobile radio and GSM

The idea of cell-based mobile radio systems appeared at Bell Laboratories (in USA) in the early 1970s. However, mobile cellular systems were not introduced for commercial use until the 1980s. During the early 1980s, analog cellular telephone systems experienced a very rapid growth in Europe, particularly in Scandinavia and the United Kingdom. Today cellular systems still represent one of the fastest growing telecommunications systems.

But in the beginnings of cellular systems, each country developed its own system, which was an undesirable situation for the following reasons:
The equipment was limited to operate only within the boundaries of each country.
The market for each mobile equipment was limited.

In order to overcome these problems, the Conference of European Posts and Telecommunications (CEPT) formed, in 1982, the Groupe Spécial Mobile (GSM) in order to develop a pan-European mobile cellular radio system (the GSM acronym became later the acronym for Global System for Mobile communications). The standardized system had to meet certain criteria:

- Spectrum efficiency
- International roaming
- Low mobile and base stations costs
- Good subjective voice quality
- Compatibility with other systems such as ISDN (Integrated Services Digital Network)
- Ability to support new services

Unlike the existing cellular systems, which were developed using an analog technology, the GSM system was developed using a digital technology. The reasons for this choice are explained in section 3.

In 1989 the responsibility for the GSM specifications passed from the CEPT to the European Telecommunications Standards Institute (ETSI). The aim of the GSM specifications is to describe the functionality and the interface for each component of the system, and to provide guidance on the design of the system. These specifications will then standardize the system in order to guarantee the proper interworking between the different elements of the GSM system. In 1990, the phase I of the GSM specifications were published but the commercial use of GSM did not start until mid-1991.

The most important events in the development of the GSM system are presented in the table1.

Table 1.1 Events in the development of GSM

Year	Events
1982	CEPT establishes a GSM group in order to develop the standards for a pan-European cellular mobile system
1985	Adoption of a list of recommendations to be generated by the group
1986	Field tests were performed in order to test the different radio techniques proposed for the air interface
1987	TDMA is chosen as access method (in fact, it will be used with FDMA) Initial Memorandum of Understanding (MoU) signed by telecommunication operators (representing 12 countries)
1988	Validation of the GSM system
1989	The responsibility of the GSM specifications is passed to the ETSI
1990	Appearance of the phase 1 of the GSM specifications
1991	Commercial launch of the GSM service
1992	Enlargement of the countries that signed the GSM- MoU> Coverage of larger cities/airports
1993	Coverage of main roads GSM services start outside Europe
1995	Phase 2 of the GSM specifications Coverage of rural areas

From the evolution of GSM, it is clear that GSM is not anymore only a European standard. GSM networks are operational or planned in over 80 countries around the world. The rapid and increasing acceptance of the GSM system is illustrated with the following figures:

1,3 million GSM subscribers worldwide in the beginning of 1994.

Over 5 million GSM subscribers worldwide in the beginning of 1995.

Over 10 million GSM subscribers only in Europe by December 1995.

Since the appearance of GSM, other digital mobile systems have been developed. The table 2 charts the different mobile cellular systems developed since the commercial launch of cellular systems.

Table 1.2 Mobile cellular systems

Year	Mobile Cellular System
1981	Nordic Mobile Telephony (NMT), 450>
1983	American Mobile Phone System (AMPS)
1985	Total Access Communication System (TACS) Radiocom 2000 C-Netz
1986	Nordic Mobile Telephony (NMT), 900>
1991	Global System for Mobile communications> North American Digital Cellular (NADC)
1992	Digital Cellular System (DCS) 1800
1994	Personal Digital Cellular (PDC) or Japanese Digital Cellular (JDC)
1995	Personal Communications Systems (PCS) 1900- Canada>
1996	PCS-United States of America>

1.2 Cellular systems

1.2.1 The cellular structure

In a cellular system, the covering area of an operator is divided into cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power.

The concept of cellular systems is the use of low power transmitters in order to enable the efficient reuse of the frequencies. In fact, if the transmitters used are very powerful, the frequencies can not be reused for hundred of kilometers as they are limited to the covering area of the transmitter.

The frequency band allocated to a cellular mobile radio system is distributed over a group of cells and this distribution is repeated in all the covering area of an operator. The whole number of radio channels available can then be used in each group of cells that form the covering area of an operator. Frequencies used in a cell will be reused several cells away. The distance between the cells using the same frequency must be sufficient to avoid interference. The frequency reuse will increase considerably the capacity in number of users.

In order to work properly, a cellular system must verify the following two main conditions:

The power level of a transmitter within a single cell must be limited in order to reduce the interference with the transmitters of neighboring cells. The interference will not produce any damage to the system if a distance of about 2.5 to 3 times the diameter of a cell is reserved between transmitters. The receiver filters must also be very performing.

Neighboring cells can not share the same channels. In order to reduce the interference, the frequencies must be reused only within a certain pattern.

In order to exchange the information needed to maintain the communication links within the cellular network, several radio channels are reserved for the signaling information.

1.2.2 Cluster

The cells are grouped into clusters. The number of cells in a cluster must be determined so that the cluster can be repeated continuously within the covering area of an operator. The typical clusters contain 4, 7, 12 or 21 cells. The number of cells in each cluster is very important. The smaller the number of cells per cluster is, the bigger the number of channels per cell will be. The capacity of each cell will be therefore increased. However a balance must be found in order to avoid the interference that could occur between neighboring clusters. This interference is produced by the small size of the clusters (the size of the cluster is defined by the number of cells per cluster). The total number of channels per cell depends on the number of available channels and the type of cluster used.

1.3 The GSM network

1.3.1 Architecture of the GSM network

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts:

- The Mobile Station (MS).
- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).
- The Operation and Support Subsystem (OSS).

The architecture of the GSM network is presented in figure 1.3

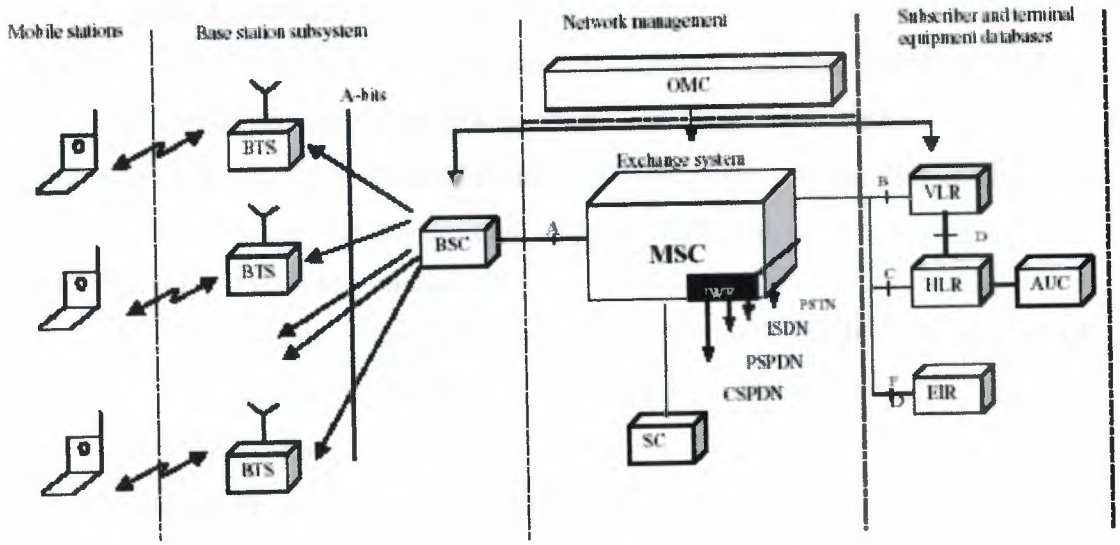

Figure 1.3 Architecture of the GSM network

1.3.1.1 Mobile Station

A Mobile Station consists of two main elements:

- The mobile equipment or terminal.
- The Subscriber Identity Module (SIM).

1) The Terminal

There are different types of terminals distinguished principally by their power and application:

The `fixed' terminals are the ones installed in cars. Their maximum allowed output power is 20 W.

The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.

The handheld terminals have experienced the biggest success thanks to the weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows to decrease the maximum allowed power to 0.8 W.

2) The SIM

The SIM is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational.

The SIM card is protected by a four-digit Personal Identification Number (PIN).In order to identify the subscriber to the system; the SIM card contains some parameters of the user such as its International Mobile Subscriber Identity (IMSI).

Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using its SIM card.

1.3.1.2 The Base Station Subsystem

The BSS connects the Mobile Station and the NSS. It is in charge of the transmission and reception. The BSS can be divided into two parts:

- The Base Station Controller (BSC).
- The Base Transceiver Station (BTS) or Base Station.

1) The Base Transceiver Station

The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell.

2) The Base Station Controller

The BSC controls a group of BTS and manages their radio resources. A BSC is principally in charge of handovers, frequency hopping, exchange functions and control of the radio frequency power levels of the BTSs.

1.3.1.3 The Network and Switching Subsystem

Its main role is to manage the communications between the mobile users and other users, such as mobile users, ISDN users, fixed telephony users, etc. It also includes data bases needed in order to store information about the subscribers and to

manage their mobility. The different components of the NSS are described below.

1) The Mobile services Switching Center (MSC)

It is the central component of the NSS. The MSC performs the switching functions of the network. It also provides connection to other networks.

2) The Gateway Mobile services Switching Center (GMSC)

A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user. The GMSC is often implemented in the same machines as the MSC.

3) Home Location Register (HLR)

The HLR is considered as a very important database that stores information of the subscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers and the services to which they have access. The location of the subscriber corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal.

4) Visitor Location Register (VLR)

The VLR contains information from a subscriber's HLR necessary in order to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough information in order to assure the subscribed services without needing to ask the HLR each time a communication is established.

The VLR is always implemented together with a MSC; so the area under control of the MSC is also the area under control of the VLR.

5) The Authentication Center (AuC)

The AuC register is used for security purposes. It provides the parameters needed for authentication and encryption functions. These parameters help to verify the user's identity.

6) The Equipment Identity Register (EIR)

The EIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a list of all valid terminals. A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g. a terminal which does not respect the specifications concerning the output RF power).

7) The GSM Interworking Unit (GIWU)

The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

1.3.1.4 The Operation and Support Subsystem (OSS)

The OSS is connected to the different components of the NSS and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS.

However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transferred to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

1.3.2 The geographical areas of the GSM network

The figure 2 presents the different areas that form a GSM network.

As it has already been explained a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. A group of location areas under the control of the same MSC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the area served by one network operator.

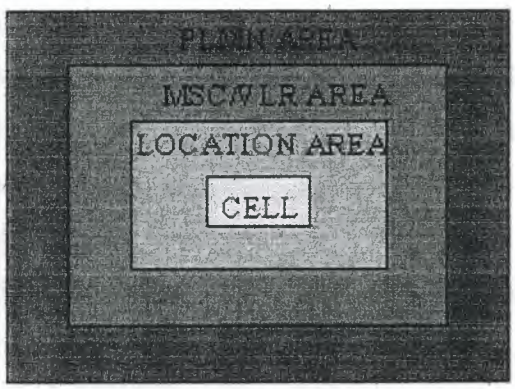

Figure 1.4 GSM network areas

1.3.3 The GSM functions

In this paragraph, the description of the GSM network is focused on the different functions to fulfill by the network and not on its physical components. In GSM, five main functions can be defined:

- Transmission.
- Radio Resources management (RR).
- Mobility Management (MM).
- Communication Management (CM).
- Operation, Administration and Maintenance (OAM).

1.3.3.1 Transmission

The transmission function includes two sub-functions:

The first one is related to the means needed for the transmission of user information.

The second one is related to the means needed for the transmission of signaling information.

Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network. Some of the most important aspects of the transmission are described in section 5.

1.3.3.3 Mobility Management

The MM function is in charge of all the aspects related with the mobility of the user, specially the location management and the authentication and security.

1) Location management

When a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.

The mobile station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different PLMN. This location updating message is sent to the new MSC/VLR, which gives the location information to the subscriber's HLR. If the mobile station is authorized in the new

MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR.

A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

2) Location updating and call routing

The MSC provides the interface between the GSM mobile network and the public fixed network. From the fixed network's point of view, the MSC is just another switching node. However, switching is a little more complicated in a mobile network since the MSC has to know where the mobile is currently roaming - and in GSM it could even be roaming in another country. The way GSM accomplishes location updating and call routing to the mobile is by using two location registers: the Home Location Register (HLR) and the Visitor Location Register (VLR).

Location updating is initiated by the mobile when, by monitoring the Broadcast Control Channel, it notices that the location area broadcast is not the same as the one previously stored in the mobile's memory. An update request and the IMSI or previous TMSI is sent to the new VLR via the new MSC. A Mobile Station Roaming Number (MSRN) is allocated and sent to the mobile's HLR (which always keeps the most current location) by the new VLR. The MSRN is a regular telephone number that routes the call to the new VLR and is subsequently translated to the TMSI of the mobile. The HLR sends back the necessary call control parameters, and also sends a cancel message to the old VLR, so that the previous MSRN can be reallocated. Finally, a new TMSI is allocated and sent to the mobile, to identify it in future paging or call initiation requests.

With the above location updating procedure, call routing to a roaming mobile is easily performed. A call from a fixed network (Public Switched Telecommunications Network or Integrated Services Digital Network) is placed to a mobile subscriber. Using the Mobile Subscriber's telephone number (MSISDN, the ISDN numbering plan specified in the ITUT E.164 recommendation), the call is routed through the fixed land network to a gateway MSC for the GSM network (an MSC that interfaces with the fixed land network, thus requiring an echo canceller). The gateway MSC uses the MSISDN to query the Home Location Register, which returns the current roaming number (MSRN). The MSRN is used by the gateway MSC to route the call to the current MSC

(which is usually coupled with the VLR). The VLR then converts the roaming number to the mobile's TMSI, and a paging call is broadcast by the cells under the control of the current BSC to inform the mobile.

3) Handover

Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. There are four different types of handover in the GSM system, which involve transferring a call between

- channels (time slots) in the same cell,
- cells (Base Transceiver Stations) under the control of the same (BSC),
- cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC)
- cells under the control of different MSCs.

The first two types of handover, called internal handovers, involve only one (BSC). To save signaling bandwidth, they are managed by the BSC without involving the (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. Note that call control, such as provision of supplementary services and requests for further handoffs, is handled by the original MSC.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, and is used by the handover algorithm.

The algorithm for when a handover decision should be taken is not specified in the GSM recommendations. There are two basic algorithms used, both closely tied in with power control. This is because the BSC usually does not know whether the poor signal quality is due to multipath fading or to the mobile having moved to another cell. This is especially true in small urban cells.

The 'minimum acceptable performance' algorithm gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased. If further power increases do not improve the

signal, then a handover is considered. This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.

The 'power budget' method uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level. It thus gives precedence to handover over power control. It avoids the 'smeared' cell boundary problem and reduces cochannel interference, but it is quite complicated.

4) Authentication and security

The authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number generated by the AuC. If the two computed SRES are the same, the subscriber is authenticated. The different services to which the subscriber has access are also checked.

Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network.

In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure.
Enciphering is another option to guarantee a very strong security

1.4 The GSM Radio Interface

The radio interface is the interface between the mobile stations and the fixed infrastructure. It is one of the most important interfaces of the GSM system.
One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the radio interface must be completely defined.

The spectrum efficiency depends on the radio interface and the transmission, more particularly in aspects such as the capacity of the system and the techniques used in order to decrease the interference and to improve the frequency reuse scheme. The specification of the radio interface has then an important influence on the spectrum efficiency.

1.4.1 From source information to radio waves

If the source of information is data and not speech, the speech coding will not be performed.

1.4.1.1 Speech coding

The transmission of speech is, at the moment, the most important service of a mobile cellular system. The GSM speech codec, which will transform the analog signal (voice) into a digital representation, has to meet the following criteria:

- A good speech quality, at least as good as the one obtained with previous cellular systems.
- To reduce the redundancy in the sounds of the voice. This reduction is essential due to the limited capacity of transmission of a radio channel.
- The speech codec must not be very complex because complexity is equivalent to high costs.

The final choice for the GSM speech codec is a codec named RPE-LTP (Regular Pulse Excitation Long-Term Prediction). This codec uses the information from previous samples (this information does not change very quickly) in order to predict the current sample. The speech signal is divided into blocks of 20 ms These blocks are then passed to the speech codec, which has a rate of 13 kbps, in order to obtain blocks of 260 bits.

1.4.1.2 Channel coding

Channel coding adds redundancy bits to the original information in order to detect and correct, if possible, errors occurred during the transmission.

1) Channel coding for the GSM data TCH channels

The channel coding is performed using two codes: a block code and a convolutional code.

The block code corresponds to the block code defined in the GSM Recommendations 05.03. The block code receives an input block of 240 bits and adds four zero tail bits at the end of the input block. The output of the block code is consequently a block of 244 bits.

A convolutional code adds redundancy bits in order to protect the information. A convolutional encoder contains memory. This property differentiates a convolutional code from a block code. A convolutional code can be defined by three variables: n, k and K. The value n corresponds to the number of bits at the output of the encoder, k to the number of bits at the input of the block and K to the memory of the encoder. The ratio, R, of the code is defined as follows: $R = k/n$. Let's consider a convolutional code

with the following values: k is equal to 1, n to 2 and K to 5. This convolutional code uses then a rate of R = 1/2 and a delay of K = 5, which means that it will add a redundant bit for each input bit. The convolutional code uses 5 consecutive bits in order to compute the redundancy bit. As the convolutional code is a 1/2 rate convolutional code, a block of 488 bits is generated. These 488 bits are punctured in order to produce a block of 456 bits. Thirty two bits, obtained as follows, are not transmitted :

C (11 + 15 j) for j = 0, 1, ..., 31

The block of 456 bits produced by the convolutional code is then passed to the interleaver.

2) Channel coding for the GSM speech channels

Before applying the channel coding, the 260 bits of a GSM speech frame are divided in three different classes according to their function and importance. The most important class is the class Ia containing 50 bits. Next in importance is the class Ib, which contains 132 bits. The least important is the class II, which contains the remaining 78 bits. The different classes are coded differently. First of all, the class Ia bits are block-coded. Three parity bits, used for error detection, are added to the 50 class Ia bits. The resultant 53 bits are added to the class Ib bits. Four zero bits are added to this block of 185 bits (50+3+132). A convolutional code, with r = 1/2 and K = 5, is then applied, obtaining an output block of 378 bits. The class II bits are added, without any protection, to the output block of the convolutional coder. An output block of 456 bits is finally obtained.

3) Channel coding for the GSM control channels

In GSM the signaling information is just contained in 184 bits. Forty parity bits, obtained using a fire code, and four zero bits are added to the 184 bits before applying the convolutional code (r = 1/2 and K = 5). The output of the convolutional code is then a block of 456 bits, which does not need to be punctured.

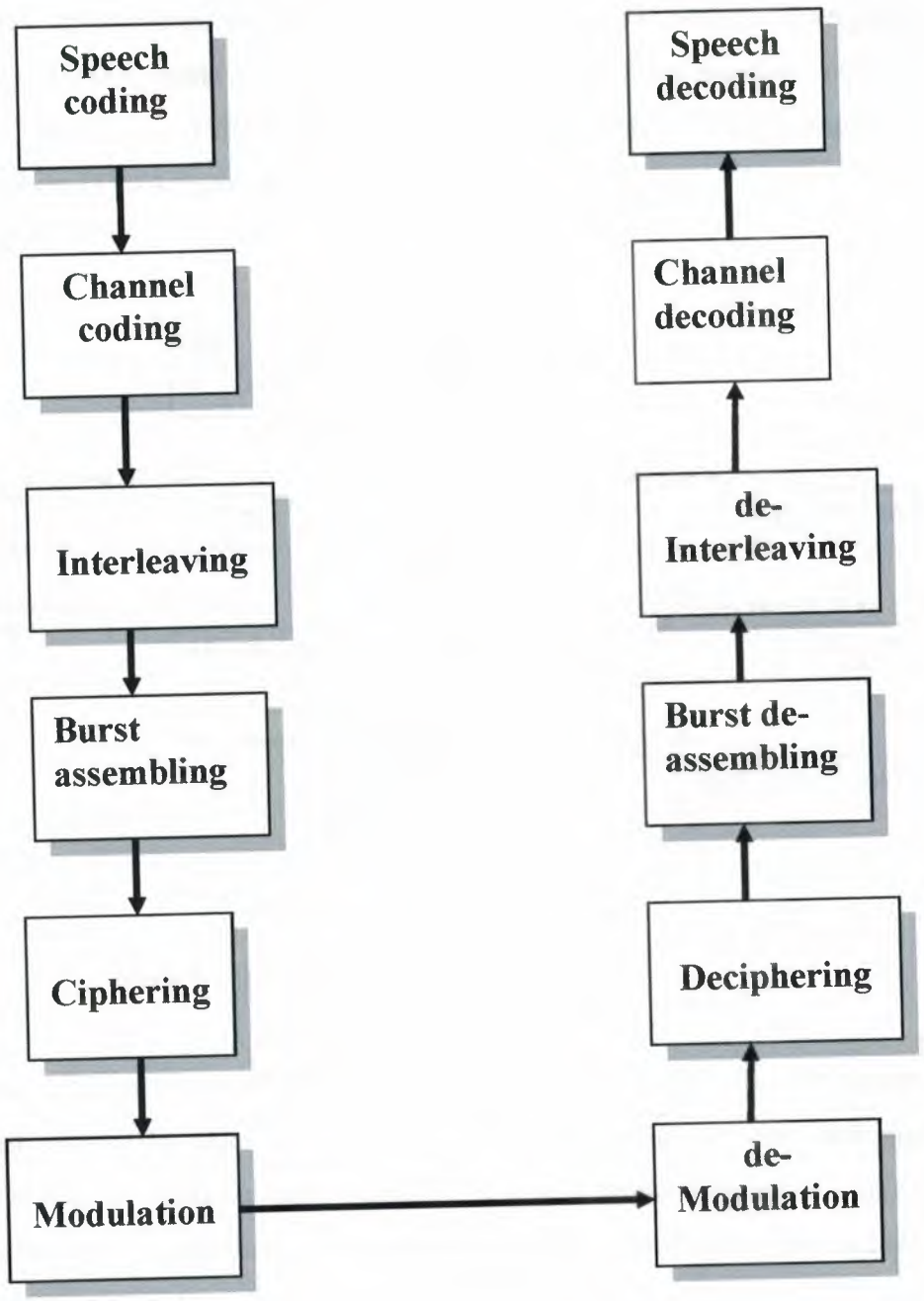

Figure 1.5 From speech source to radio waves

1.4.1.3 TDMA Frame Structures, Channel Types, and Burst Types

The 200 kHz channels in each band are further subdivided into 577 ms timeslots, with 8 timeslots comprising a TDMA frame of 4.6 ms. Either 26 or 51 TDMA frames are grouped into multiframes (120 or 235 ms), depending on whether the channel is for traffic or control data. Either 51 or 26 of the multiframes (again depending on the channel type) make up one super frame (6.12 s). A hyper frame is

composed of 2048 super frames, for a total duration of 3 hours, 28 minutes, 53 seconds, and 760 ms. The TDMA frame structure has an associated 22-bit sequence number which uniquely identifies a TDMA frame within a given hyper frame. Figure 1 illustrates the various TDMA frame structures.

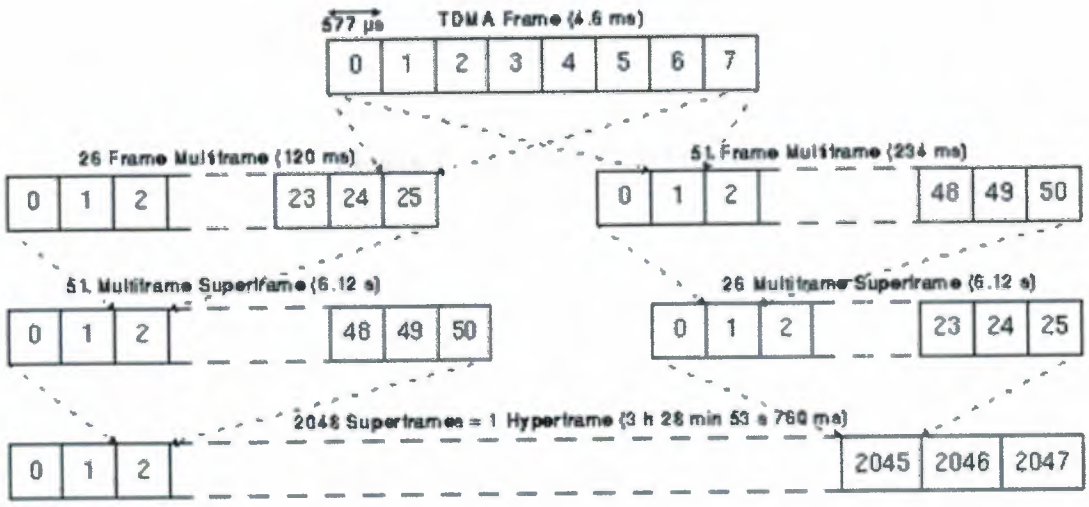

Figure 1.6 TDMA Frame Structure

The various logical channels which are mapped onto the TDMA frame structure may be grouped into traffic channels (TCHs) used to carry voice or user data, and control channels (CCHs) used to carry signaling and synchronization data. Control channels are further divided into broadcast control channels, common control channels, and dedicated control channels.

Each timeslot within a TDMA frame contains modulated data referred to as a "burst". There are five burst types (normal, frequency correction, synchronization, dummy, and access bursts), with the normal burst being discussed in detail here. The bit rate of the radio channel is 270.833 kbit/sec, which corresponds to a timeslot duration of 156.25 bits. The normal burst is composed of a 3-bit start sequence, 116 bits of payload, a 26-bit training sequence used to help counter the effects of multipath interference, a 3-bit stop sequence required by the channel coder, and a guard period (8.25 bit durations) which is a "cushion" to allow for different arrival times of bursts in adjacent timeslots from geographically disperse MSs. Two bits from the 116-bit payload are used by the

Fast Associated Control Channel (FACCH) to signal that a given burst has been borrowed, leaving a total of 114 bits of payload. Figure 2 illustrates the structure of the normal burst.

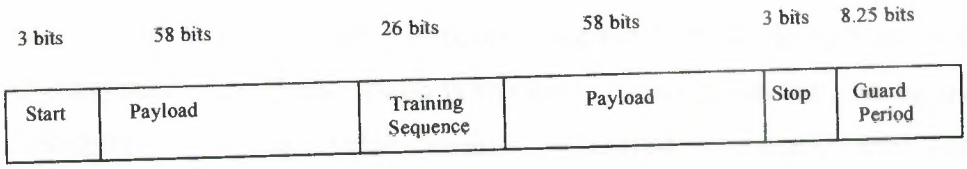

Figure 1.7 Normal Burst Structure

II. OVERVIEW OF CRYPTOGRAPHY

2.1 Introduction:

People mean different things when they talk about cryptography. Children play with toy ciphers and secret languages. However, these have little to do with real security and strong encryption. Strong encryption is the kind of encryption that can be used to protect information of real value against organized criminals, multinational corporations, and major governments. Strong encryption used to be only military business; however, in the information society it has become one of the central tools for maintaining privacyand confidentiality. As we move into an information society, the technological means for global surveillance of millions of individual people are becoming available to major governments. Cryptography has become one of the main tools for privacy, trust, access control, electronic payments, corporate security, and countless other fields.

Cryptography is no longer a military thing that should not be messed with. It is time to make full use of the advantages it provides for the modern society.

2.2 Encryption:

Encryption is the transformation of data (radio wave) into a form of radio wave unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.

In a multi-user setting, encryption allows secure communication over an insecure channel. The general scenario is as follows: A sends a message to B so that no one else besides B can read it. A encrypts the message (plaintext), with an encryption key; the encrypted message (ciphertext), is sent to B. B decrypts the ciphertext with the decryption key and reads the message. An attacker, C, may either try to obtain the secret key or to recover the plaintext without using the secret key. In a secure cryptosystem, the plaintext cannot be recovered from the ciphertext except by using the decryption

A method of encryption and decryption is called a cipher. Some cryptographic methods rely on the secrecy of the algorithms; such algorithms are only of historical interest and are not adequate for real-world needs. All modern algorithms use a key to control encryption and decryption; a message can be decrypted only if the key matches

the encryption key.

There are two classes of key-based encryption algorithms, symmetric (or secret-key) and asymmetric (or public-key) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

Asymmetric algorithms (also called public-key algorithms or generally public-key cryptography) permit the encryption key to be public (it can even be published in a newspaper), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the public key and the decryption key the private key or secret key.

2.3 Symmetric algorithm (Private Key Algorithms):

The most ancient and basic problem of cryptography is secure communication over an insecure channel A wants to send to B a secret message over the air that may be intercepted by an adversary. The traditional solution to this problem is called private key encryption. In private key encryption, A and B agree on a pair of encryption and decryption algorithms E and D, and an additional piece of information S to be kept secret. We shall refer to S as the shared secret key. The adversary may know the encryption and decryption algorithms E and D which are being used, but does not know S.

In a symmetric cryptosystem, a single key serves as both the encryption and decryption keys. For a good encryption algorithm, the security of the data rests with the security of the key, which introduces the problem of key management for symmetric algorithms.

Symmetric encryption algorithms may be further divided into block ciphers and stream ciphers.

2.3.1 Block ciphers

Symmetric-key block ciphers are the most prominent and important elements in many cryptographic systems. Individually, they provide confidentiality. As a fundamental building block, their versatility allows construction of pseudorandom number generators, stream ciphers, MACs, and hash functions. They serve as a central component in message authentication techniques, data integrity mechanisms, entity authentication protocols, and (symmetric-key) digital signature schemes. No block cipher is ideally suited for all applications, even one offering a high level of security. This is a result of inevitable tradeoffs required in practical applications, including those arising from, for example, speed requirements and memory limitations (e.g., code size, data size, cache memory), constraints imposed by implementation platforms (e.g., hardware, software, chip cards), and differing tolerances of applications to properties of various modes of operation. In addition, efficiency must typically be traded off against security.

Block ciphers encrypt or decrypt data in blocks or groups of bits. DES uses a 56_bit key and processes data in 64-bits blocks, producing 64-bits of input, and vice-versa. Block algorithms are further characterized by their mode of operation, such as electronic code book (ECB), cipher block chaining (CBC) and cipher feedback (CFB). CBC and CFB are examples of modes of operation where the encryption of successive blocks is dependent on the output of one or more previous encryptions. These modes are desirable because they break up the one-to-one correspondence between ciphertext blocks and plaintext blocks (as in ECB mode). Block ciphers may even be implemented as a component of a stream cipher.

2.3.2 Stream ciphers:

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation, which varies with time. By contrast, block ciphers tend to simultaneously encrypt groups of characters of a plaintext message using a fixed encryption transformation. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in GSM), when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.

Stream ciphers operate on a bit-by- bit basis, producing a single encrypted bit for a single plaintext bit. Stream ciphers are commonly implemented as the exclusive or (XOR) of the data stream with the keystream. The security of a stream cipher is determined by the properties of the keystream. A completely random keystream would effectively implement an unbreakable one-time pad encryption, and a deterministic keystream with a short period would provide very little security.

Linear feedback shift registers (LFSRs) are a key component of many stream ciphers. LFSRs are implemented as a shift register where the vacant bit created by the shifting is a function of the previous states. With the correct choice of feedback taps, LFSRs can function as pseudorandom number generators. The statistical properties of LFSRs, such as the autocorrelation function and power spectral density, make them useful for other applications such as pseudo-noise (PN) sequence generators in direct sequence spread spectrum communications and for distance measurement in systems such as the global positioning system (GPS). LFSRs have the additional advantage of being easily implemented in hardware.

The maximal length sequence (or m-sequence) is equal to 2n-1 where n is the degree of the shift register. An example of a maximal length LFSR is shown below in Figure. This LFSR will generate the periodic m-sequence consisting of the following states (1111, 0111, 1011, 0101 1010, 1101, 0110, 0011, 1001, 0100, 0010, 0001, 1000, 1100, and 1110).

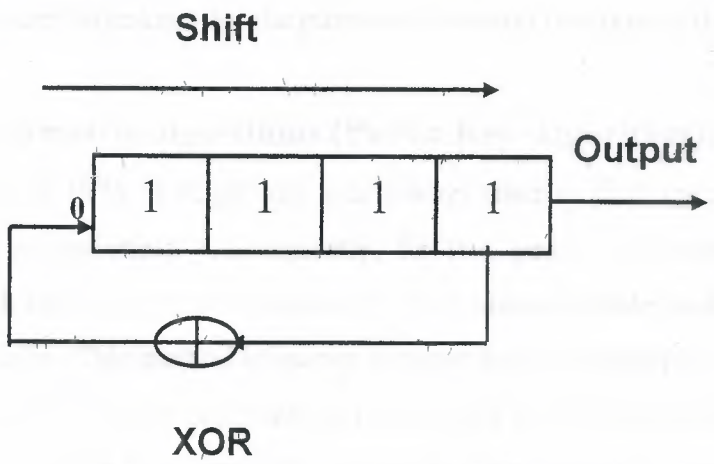

Figure 2.1 Four-Stage Linear Feedback Shift Register

In order to form an m-sequence, the feedback taps of an LFSR must correspond to a primitive polynomial modulo 2 of degree. A number of stream cipher designs consist of multiple LFSRs with various interconnections and clocking schemes. The

GSM A5 algorithm, used to encrypt voice and signaling data in GSM is a stream cipher based to encrypt voice and signaling data in GSM is a stream cipher based on three clock-controlled LFSRs.

2.3.3 Advantages of symmetric-key cryptography

Symmetric-key ciphers can be designed to have high rates of data throughput. Keys for symmetric-key ciphers are relatively short.

Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators, hash functions, and computationally efficient digital signature schemes, to name just a few.

Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyze, but on their own weak, can be used to construct strong product ciphers.

2.3.4 Disadvantages of symmetric-key cryptography

In a two-party communication, the key must remain secret at both ends. In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP.

In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently and perhaps for each communication session.

Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP.

2.4 Asymmetric algorithms (Public Key Algorithm):

Until 1976, a single key was always used to both encode the message and to decode the ciphertext. Consequently, for two people to communicate securely, they must both have a copy of the same key. This raises extreme problems in transferring the key securely.. This method is known as secret-key cryptography

In 1976, a new approach was developed by Whitfield Diffie - called Public Key Cryptography. In this approach each person has two keys, which they generate with special software at the same time. They keys related - but not in any way which can be computed externally. One - the private key - is kept secret. The other - the public key - can be given freely to anyone. Something encrypted with the private key can only be

decrypted with the public key. Something encrypted with the public key can only be decrypted with the private key.

This means that someone can send me a message without the need for me to get a secret key to them - they simply encrypt with my public key. This utterly changes the usefulness of cryptography - previously physical couriers were needed to transport the single keys to both end of an anticipated communication path - no electronic path could be trusted with the key. Public key cryptography, when properly implemented and used, enables people to communicate in secrecy, and to sign documents, with what is in all practical terms absolute security - without ever having to exchange something like a single symmetric key which must be kept from prying eyes.

2.4.1 Advantages of public-key cryptography

Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed). The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an *offline* manner, as opposed to in real time.

Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).

Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

2.4.2 Disadvantages of public-key encryption

Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best-known symmetric-key schemes. Key sizes are typically much larger than those required for symmetric-key encryption, and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.

No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.

2.5 Design principles for cryptographic algorithms

Designing a slow and secure algorithm is easy for someone who understands the current designs and their strengths and weaknesses. For example, composition constructions exist which are at least as secure as each of the building blocks. If on the other hand the performance has to be pushed to the limits, a thorough analysis has to be combined with a good understanding of the limitations of the processor or technology in which the system has to be implemented. While it is clear that the performance of primitives depends on the implementation details, even for a given environment, very little is known on which structures provide the best security (for a given number of instructions per encrypted or hashed byte). Key issues are clearly the use of memory and the amount of parallelism. This section summarizes the different design aspects:

– Global structure and number of rounds;
– Non-linearity;
– Diffusion;
– Key schedule.

2.5.1 Global structure and number of rounds

Hash functions and block ciphers operate on relatively large inputs (64 . . . 256 bits). These primitives are designed based on a principle proposed by Shannon: nonlinear substitutions are alternated with mixing functions. The result of the combination is that "any significant statistics from the encryption algorithm must be of a highly involved and very sensitive type—the redundancy has been both diffused and confused by the mixing transformation." In the seventies a round transformation was used, consisting of small non-linear components and a transposition (or bit permutation). The strength of a cryptographic primitive can be obtained by repeating this simple transformation. For a block cipher, the secret key has to be introduced in every round as well.

If every input bit is treated in a similar way, one can speak of a uniform transformation. An example of such a network is given in Figure 2.2.

A disadvantage of this approach is that the inverse function (which is required for decryption in case of a block cipher in ECB or CBC-mode) may be different from the function itself. This can be a problem for hardware and smart card applications. Subhash is a hash function using this approach. A different approach consists of dividing the input into two halves, and applying a non-linear function only to the right

half. The result is added into the left half and subsequently left and right half are swapped. Ciphers following this approach are called Feistel ciphers (see also Figure 2.3). Since the nonlinear part requires most of the computation, two rounds of a Feistel cipher require about the same effort as a uniform transformation. The output of one nonlinear function is input directly to the next one, which decreases the amount of parallelism but increases the propagation of local changes. Due to the special structure of the round function, the nonlinear function itself need not be invertible, and the round function is an involution. Since DES is a Feistel cipher, more cryptanalytic experience is available on Feistel ciphers than on any other general structure. Other Feistel ciphers are FEAL, Blowfish, Khufu, LOKI91, CAST, and MISTY1.

The approach of a Feistel cipher can be further extended by dividing the input into more parts (ciphers constructed in this way have been called general unbalanced Feistel networks). This may lead to a faster propagation of changes, but could reduce parallelism (depending on the nature of the nonlinear functions).

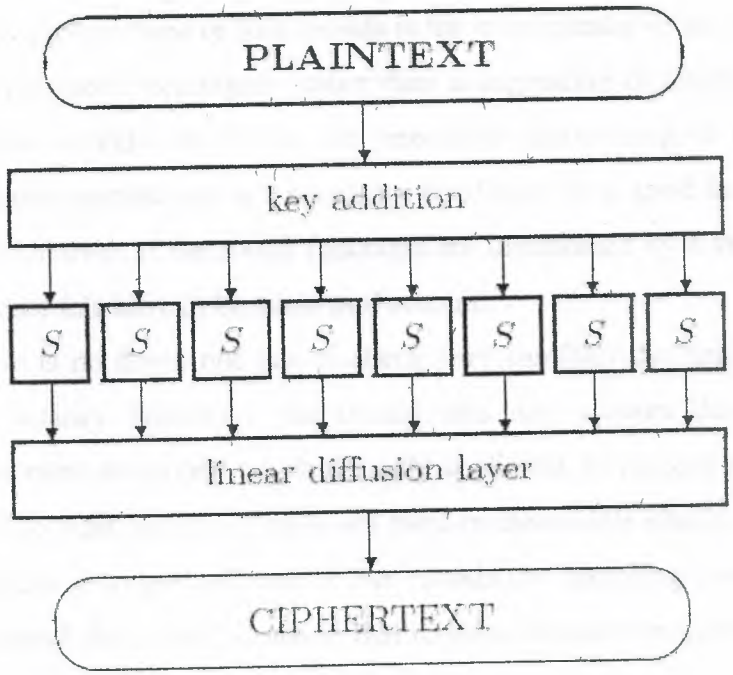

Figure 2.2 One round of SHARK,

Other variants and extensions of uniform transformations and Feistel ciphers have been proposed. RC5 is almost a Feistel cipher, since a part of the left half influences the transformation of the right half. MISTY2 is a Feistel variant which increases parallelism: by moving the nonlinear function to a different place, its input in

the next round is already known before its output in the current round is calculated, so that calculations for two consecutive rounds can be carried out at the same time. IDEA is a also a variant: a function is computed of the sum of the two halves, and the result is added to the two halves (such that their sum remains a constant).

The main conclusion which can be drawn from this section is that for the time being no conclusion can be drawn on which global structure is best. Different approaches have advantages and disadvantages, and it seems not very likely that clear winners will emerge in the near future.

Numbers of rounds most block ciphers and hash functions obtain their strength from repeating a number of identical rounds (one exception is CAST: some members of this cipher family have different rounds).

While this provides some theoretical support for the Feistel structure, this work has been misinterpreted by others with regard to its impact on practical ciphers. For example, this research is orthogonal to the issue whether one should have many simple rounds or only three or four more complex rounds. The fact that most proofs seem to achieve their limit at three or four rounds is the consequence of the shortcomings of the model and the proof techniques, rather than a suggestion that ciphers with fewer but more complex rounds are better. An important shortcoming is that while being a pseudo-random permutation is a necessary condition for a good block cipher, it is not sufficient. Moreover, if the round functions are instantiated by a smaller block cipher, other attack models have to be taken into account.

There is no doubt one has to check very carefully the resistance to linear and differential attacks. However, one should take into account that several dedicated attacks have been developed which are only applicable to ciphers with a small number of rounds. The most general of these are meet-in-the-middle attacks. Another trick used in these attacks is to peel off one or two rounds (by searching over part of the round keys), and attack the 'weak' structure that remains. Attacks on ciphers with few rounds include:

- Meet-in-the middle attacks exploiting the key schedule
- Key recovery attacks on 4 or 5 rounds of ladder-DES
- Higher order differentials (up to 6–8 rounds);
- Interpolation attacks (for ciphers with S-boxes with a simple algebraic structure)
- Attacks on Feistel ciphers with non-subjective round functions (up to 8 rounds)

- Structure attacks, which exploit the structure of a uniform round transformation

2.5.2Nonlinearity

A nonlinear component is essential to every strong cryptographic primitive. The goal of the designer is to build a 'large' nonlinear primitive from smaller ones. The design approaches differ in the choice of the basic nonlinear component.

A straightforward way to implement simple nonlinear functions is lookup tables or S-boxes. The DES uses eight different S-boxes with 6 input bits and 4 output bits; the total size of 256 bytes was clearly dictated by hardware constraints of the mid 1970's.

For modern processors with 32-bit or 64-bit words, S-boxes with more output bits can provide higher efficiency. An important concern is that the S-boxes should fit in the fast cache memory. Snefru was the first cipher to use 8 to 32 S-boxes;
It has the Feistel structure. E denotes the linear expansion of the 32 input bits to 48 input bits, © denotes the bitwise exor with the round key, S is the nonlinear substitution and P is the bit permutation.

2.5.3 Diffusion

In order to restrict the complexity of the implementation, nonlinear operations can only be applied to small parts of the block. Several techniques are used to spread local changes.

Linear transformations are very well suited for this purpose. The simplest solution is a bit permutation (or transposition), as is used by DES, or a rotation. An alternative is to add the output of several S-boxes. More general linear transformations are the pseudo-Hadamard transform, and the 10 diffusion operation based on MDS (Maximum Distance Separable) linear codes.

Some cryptographic primitives have no separate diffusion operation, but combine linear and nonlinear operations in such a way that changes are spread quickly through the block.

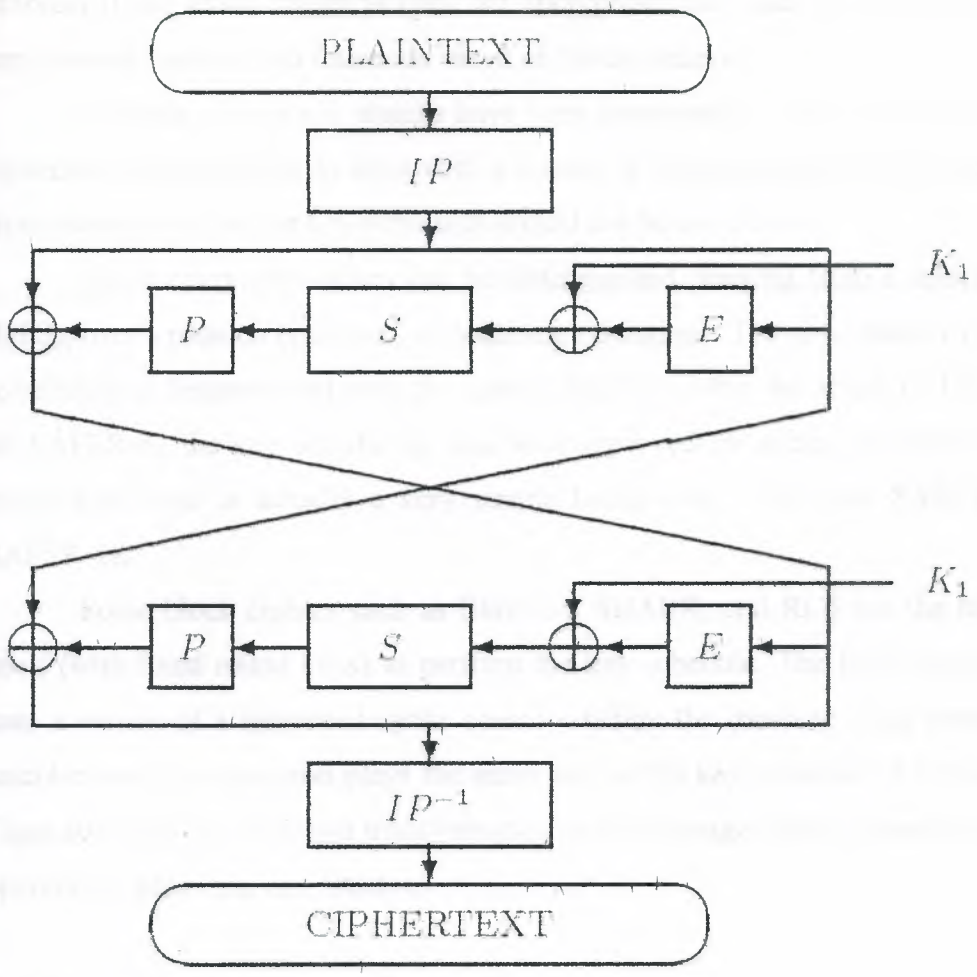

Figure 2.2 Two rounds of the DES, the most famous block cipher.

2.5.4 Key schedule

The key schedule is an important component of a block cipher; it computes the round keys from the external key. For many applications, the key schedule should not be too slow: some applications require very fast key schedules. Examples are constructions for hash functions based on a block cipher, and banking applications which use a new session key per transaction. On the other hand, enumerating the key space should not be too easy in order to frustrate an exhaustive key search. Large key dependent S-boxes (as found in Blowfish and Khufu) do not foster a quick key change.

One issue is the existence of weak keys, i.e., keys for which the block cipher is more vulnerable. Weak keys have been identified for DES. Ideally, such keys should not exist. If they form only a sparse subset of the key space, they pose no security

problem if the block cipher is used for encryption; they can be a problem for other applications such as hash functions based on block ciphers.

Recently related key attacks have been developed, in which an attacker obtains ciphertext corresponding to keys with a known or chosen relation. The lesson learned from these attacks is that key schedules should not be too simple.

Again many approaches can be distinguished, varying from a selection of bits (DES), over a rotation operation, to nonlinear operations. The importance of a good key scheduling is demonstrated with the case of SAFER. After the attack of L.R. Knudsen on SAFER-K, the key scheduling has been improved by adding a parity byte to the round keys (this is actually a very simple linear code). The new SAFER is called SAFER-SK.

Some block ciphers such as Blowfish, SHARK, and RC5 use the block cipher itself (with fixed round keys) to perform the key schedule. The hash function SHA-1 uses a variant of a shortened cyclic code to diffuse the message input throughout the calculations (this operation plays the same role as the key schedule of a block cipher). Tiger also applies a diffusion transformation to the message input; it consists of Boolean operations, additions, and rotations.

2.6 What Do Security Rests On?

If anyone tries to sell you - or even give you - a cryptosystem based on a secret algorithm, or one that has not been subject to years of scrutiny by the cryptographic community, don't take it!

Only after years of such scrutiny can confidence be gained that the cryptographic algorithms used - or the entire cryptosystem - is without easily exploitable flaws.

Assuming a cryptosystem is sound and is properly used, the security of the communications which depend on it relies on only two things: the secrecy of the decryption key and the difficulty of finding that key without knowing it.

So we know that security of a cryptosystem rests on the secrecy of the key and not the secrecy of the algorithm

2.7 Key lengths and security

Each key is a long number - say 1024 binary bits, or around 300 decimal places. The keys are typically converted to and from text and stored. The text representation of the 1024 bit key. Using existing search techniques, with a 100 MIPS (Million Instructions Per Second) computer - roughly equivalent to a 200 MHz Pentium - it would take 28,000 billion years to find the right key to decrypt a message which had been encrypted with a key of this length.

The keys used for public key cryptography are not quite as simple as a standard symmetrical key - which can have any value at all. Each key of the public/private key-pair is the product (multiplication) of two prime numbers. A prime number is one such as 3, 7, 19 etc which has no factors other than one and itself. So a 1024 bit public or private key is a number which is one 512 bit prime number multiplied by another 512 bit prime number. Only some numbers are prime numbers, so it is not true to say every possible number between 0 and 2 to the 1024th power could be a key. This makes a search for the correct key easier, so public key cryptography needs to use keys of a longer length than would be required for symmetric key cryptography in order to attain the same degree of security.

In fact the 1024 bit length of the public/private key pairs used by PGP is equivalent to about a 96 bit symmetrical key. I don't have figures for how long the mythical US$1billion dollar cracking machine would take to find a key with this length, but an 80 bit symmetrical key would take it 7 years on average and a 112 bit key 10,000 million years.

Cryptography is an arcane field, so detailed discussion of the security of key lengths is out of place here. However three things are worth noting. Firstly, the only successful attempt at finding a key for the 429 bit RSA129 public key algorithm took the equivalent of 46 years of 100 MIPS computer time. This was close to what had been predicted theoretically.

The recent finding of a 128 bit symmetrical key as used by Netscape (US version) in a far shorter time than expected was a result of a poor key generation technique which the researchers exploited. The original Netscape implementation (which has since been fixed) was only capable of producing a tiny subset of the possible key range, so the researchers only needed to search within this subset.

The third thing which is worth noting is that current US export restrictions inhibit Netscape from exporting software which uses a symmetrical key length longer than 40 bits - and this is nowhere near long enough for the serious security it is supposed to provide. In symmetrical cryptography, as used in this aspect of Netscape, any key within the 40 bit range can be a key - a million, million, million, million keys. This is feasible to search with lots of computers or with specialized hardware.

A popular key length is 56 bits - as used with the established DES (Data Encryption Standard). it is estimated that a system to find a 56 bit DES key in 3.5 hours could be built for $1M in 1995. For 56-bit keys, these numbers (costs) are within the budgets of most large companies and many criminal organizations. The military budgets of most large industrialized countries can afford to break 64-bit keys. Breaking an 80-bit key is still beyond the realm of possibility, but if current trends continue that will change in only 30 years.

When a search for a key is successful, the enormous effort results in finding just one key to decrypt any message made with just one corresponding encryption key - this does not constitute "cracking" an algorithm. To do that would require finding a fault in the algorithm - something which enabled the key to be found without having to test every possible key.

Cryptographers are generally a cautious bunch - many having been humbled when their own published algorithms are show by their colleagues to contain fatal flaws. In this field the word "strong" generally has a special meaning. "Strong" means that no known methods exist to break the cryptosystem unless anything less than astronomical time- scales or expenditures are allowed. It is never true to say that a cryptosystem is uncrackable because given a few billion, billion years, the key to decrypt a message can certainly be found. Generally "Strong" means "To all intents and purposes uncrackable - with existing technology and knowledge."

For users of cryptography, the word "strong" means that the chances of a cryptosystem's ciphertext or digital signatures being decoded or forged by anyone who does not possess the private key, are so small as to be not worth considering.

The ideal form or cryptography is "strong public key" cryptography - because it does not require the exchange of secret keys. Symmetric cryptography, whether for encryption or signatures, has no advantage over public key cryptography of similar security except for the two following considerations:

The keys used by public key cryptography need to be somewhat (6 to 30 times) longer than the equivalent symmetrical key for a given level of security. For instance a 128 bit key for symmetrical cryptography is as secure as a 2304 bit key for public key cryptography.

Public key cryptographic algorithms are a lot more complicated than symmetrical algorithms and therefore run a lot slower on a given computer.

The first of these points is hardly ever an issue. It is hard to imagine the key length becoming a problem due to storage or communication delays, even with present day communications and technologies, as long as it is below around 10 to 50 Kbytes - 80,000 to 400,000 bits.

The second point is a much more serious matter. In fact for encryption of communications and data storage, pure public key cryptography is almost never used on its own - because of the excessive time which would be required to compute the encryption and decryption operations.

Almost all encryption application programs - such as PGP - use a fast symmetric algorithm to encrypt the file or data stream. PGP uses the IDEA algorithm with a 128 bit key. For each session, or each file, the software generates a random 128 bit symmetric key - the session key - and encrypts the plaintext with it to form the main body of ciphertext. In the final output file, or at the start of the communication session, the program also sends this session key - encrypted using strong public key cryptography. This encryption of the session key is all that the 1024 bit (PGP also does shorter keys) public/private key pair is used for.

Since the session key is very short, it is computationally easy to encrypt it with the slow public key algorithms - PGP uses the industry standard RSA algorithm. The security of the whole system then depends on a chain of two cryptographic processes - and an attacker could be expected to exploit the weakest link. Not only is the randomness and length of the public/private key pair an issue, so to is the randomness and length of the symmetric session key. Assuming the software does not enable the session key to escape from the computer or be recorded at the end of the session, and then the secrecy of that key should not be a problem.

Communication with "Strong symmetric" cryptography can never be as secure as with "strong public key" cryptography for the simple reason that with symmetric cryptography, the decryption key (the same as the encryption key) must leave the site of the person who encrypted the communication so that the receiver can decrypt it. Once

that copy has left that person's possession, they can never be absolutely sure what has become of it. With public key cryptography, the decryption key is the private key of the person who receives the communication. This need never leave their possession - so (barring ESP and otherworldly events) its security and the secrecy of the communication can be, for all practical purposes, absolute.

2.8 Hash Functions

An essential element of most authentication and digital-signature schemes is a hash function. A hash function accepts a variable-size message M as input and produces a fixed-size tag H (M), sometimes called a message digest, as output. Typically, a hash code is generated for a message, encrypted, and sent with the message. The receiver computes a new hash code for the incoming message, decrypts the hash code that accompanies the message, and compares them. If the message has been altered in transit, there will be a mismatch.

2.8.1Classification of Hash Functions

At the highest level, hash functions can be classified as:

- Unkeyed hash functions: The input to these hash functions is a single parameter, i.e., the message.
- Keyed hash functions: These hash functions take two parameters as input, the message and a secret key.

2.8.2 Basic Properties

Any hash function should have the following basic properties:

1) Compression: The hash function should be able to accept any arbitrary length message as input and generate a fixed length output.

2) Ease of computation: The hash should be easy to compute.

2.8.3 Functional Classification

1) Message Authentication Codes (MACs)

The purpose of a MAC is to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity. MACs have two functionally distinct parameters, a message input and a secret key; they are a subclass of keyed hash functions

2) Modification Detection Codes (MDCs)

MDCs are also known as manipulation detection codes, and less commonly as message integrity codes (MICs), the purpose of an MDC is to provide a representative image or hash of a message, satisfying additional properties as refined below. The end goal is to facilitate, in conjunction with additional mechanisms, data integrity assurances as required by specific applications. MDCs are a subclass of unkeyed hash functions, and themselves may be further classified:

- One-way hash functions (OWHFs): for these, finding an input which hashes to a pre-specified hash-value is difficult; one-way hash functions produce a fixed-length output given an arbitrary input. Secure one-way hash functions are designed such that it is computationally unfeasible to determine the input given the hash value, or to determine two unique inputs that hash to the same value. Examples of one-way hash functions include MD5, which produces a 128-bit hash value, and the Secure Hash Algorithm (SHA) developed by the National Institutes of Standards and Technology (NIST), which produces a 160-bit output.

  A typical application of a one-way hash function is to compute a "message digest" which enables the receiver to verify the authenticity of the data by duplicating the computation and comparing the results. A hash function output encrypted with a public key algorithm forms the basis for digital signatures, such as NIST's Digital Signature Algorithm (DSA).

  A key-dependent one-way hash function requires a key to compute and verify the hash value. This is useful for authentication purposes, where a sender and receiver may use a key-dependent hash function in a challenge-response scheme. A key-dependent one-way hash function may be implemented by simply appending the key to the message and computing the hash value. Another approach is to use a block cipher in cipher feedback (CFB) mode, with the output being the last encrypted block (recall that in CFB mode a given block's output is dependent on the output of previous blocks). The A3 and A8 algorithms of GSM are key- dependent one-way hash functions. The GSM A3 and A8 algorithms are similar in functionality and are commonly implemented as a single algorithm called COMP128.

- Collision resistant hash functions (CRHFs): for these, finding any two inputs having the same hash-value is difficult.

Three potential properties are listed for an Unkeyed hash function h with inputs x, x' and outputs y, y':

1. 1st-preimage resistance: for essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output, i.e., to find any preimage x' such that h (x') = y when given any y for which a corresponding input is not known.
2. 2nd-preimage resistance - it is computationally infeasible to find any second input which has the same output as any specified input, i.e., given x, to find a 2nd-preimage x' ? x such that h (x) = h (x').
3. collision resistance - it is computationally infeasible to find any two distinct inputs x and x' which hash to the same output, such that h(x) = h(x')

2.9 Some famous Algorithms

the following algorithms are widely used in the main structure of the keys used for encryption of data.

2.9.1 RSA

The most commonly used public key algorithm. It can be used both for encryption and for digital signatures. The security of RSA is generally considered equivalent to factoring, although this has not been proved.

RSA computation takes place with integers modulo n = p * q, for two large secret primes p, q. To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the ciphertext $c = m^e \pmod n$ computes the multiplicative reverse $d = e^{-1} \pmod{(p-1)*(q-1)}$ (we require that e is selected suitably for it to exist) and obtains $c^d = m^{e*d} = m \pmod n$. The private key consists of n, p, q, e, d (where p and q can be forgotten); the public key contains only of n, e. The problem for the attacker is that computing the reverse d of e is assumed to be no easier than factorizing n. More details are available in many sources.

The key size (the size of the modulus) should be greater than 1024 bits (i.e. it should be of magnitude 10^{300}) for a reasonable margin of security. Keys of size, say, 2048 bits should give security for decades. Dramatic advances in factoring large integers would make RSA vulnerable, but other attacks against specific variants are also known. Good implementations use redundancy (or padding with specific structure) in order to avoid attacks using the multiplicative structure of the ciphertext. RSA is

vulnerable to chosen plaintext attacks and hardware and fault attacks. Also important attacks against very small exponents exist, as well as against partially revealed factorization of the modulus.

The proper implementation of the RSA algorithm with redundancy is well explained in the PKCS standards. They give detailed explanations about how to implement encryption and digital signatures, as well as formats to store the keys. The plain RSA algorithm should not be used in any application. It is recommended that implementations follow the standard as this has also the additional benefit of inter-operability with most major protocols.

RSA is currently the most important public key algorithm. It was patented in the United States (the patent expired in the year 2000).

2.9.2 DES:

The Data Encryption Standard (DES) is an algorithm developed in the mid-1970s. It was turned into a standard by the US (NIST), and was also adopted by several other governments worldwide. It was and still is widely used, especially in the financial industry.

DES is a block cipher with 64-bit block size. It uses 56-bit keys. This makes it suspectible to exhaustive key search with modern computers and special-purpose hardware. DES is still strong enough to keep most random hackers and individuals out, but it is easily breakable with special hardware by government, criminal organizations, or major corporations. DES is getting too weak, and should not be used in new applications.

A variant of DES, Triple-DES (also 3DES) is based on using DES three times (normally in an encrypt-decrypt-encrypt sequence with three different, unrelated keys). The Triple-DES is arguably much stronger than (single) DES; however, it is rather slow compared to some new block ciphers.

Nevertheless, even though DES seems to be of little interest for applications of today there are many reasons for considering it still important. It was the first block cipher which was widely deployed in the public sector. Thus it played an important role in making strong cryptography available to the public. Also, the design was exceptionally good for a cipher that was meant to be used only a few years. DES proved to be a very strong cipher and it took over a decade for any interesting crypt analytical attacks against it to develop (not to underestimate the pioneering efforts that lead to this

breakthrough). The development of differential cryptanalysis and linear cryptanalysis opened ways to really understand the design of block ciphers.

Although at the time of DES's introduction its design philosophy was held secret, it did not discourage its analysis - to the contrary. Some information has been published about its design, and one of the original designers, Don Coppersmith, has commented that they discovered ideas similar to differential cryptanalysis already while designing DES in 1974. However, it was just matter of time that these fundamental ideas were re-discovered.

Even today, when DES is no longer considered a practical solution, it is often used to describe new crypt analytical techniques. It is remarkable that even today, there are no crypt analytical techniques that would completely break DES in a structural way, indeed, and the only real weakness known is the short key size (and perhaps the small block size).

2.9.3 CBC

A ciphertext block is obtained by first XORing the plaintext block with the previous ciphertext block, and encrypting the resulting value. This way leading blocks influence all trailing blocks, which increases the number of plaintext bits one ciphertext bit depends on, but also leads to synchronization problems if one block is lost.

2.9.4 CFB

The kth ciphertext block is obtained by encrypting the (k-1)th ciphertext block and XORing the result onto the plaintext. Interestingly, an CFB feedback loop can also be used as a pseudo-random number generator if one simply feeds one block of true random data with trailing blocks of zeroes into the encryption routine (although the expected period of this PRNG would be only about 2n/2 where n is the block size of the cipher).

III SECURITY AND INTERCEPTION IN GSM

3.1 Description of GSM Security Features

Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The MS identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically (i.e. during hand-offs) for additional security.

The security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, and A8) are present in the GSM network as well. The Authentication Center (AuC), part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the TMSI, the Location Area Identity (LAI), and the individual subscriber authentication key (Ki) for each user. In order for the authentication and security mechanisms to function, all three elements (SIM, handset, and GSM network) are required. This distribution of security credentials and encryption algorithms provides an additional measure of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud.

Figure 3.1 demonstrates the distribution of security information among the three system elements, the SIM, the MS, and the GSM network. Within the GSM network, the security information is further distributed among the authentication center (AuC),

the home location register (HLR) and the visitor location register (VLR). The AuC is responsible for generating the sets of RAND, SRES, and Kc which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.

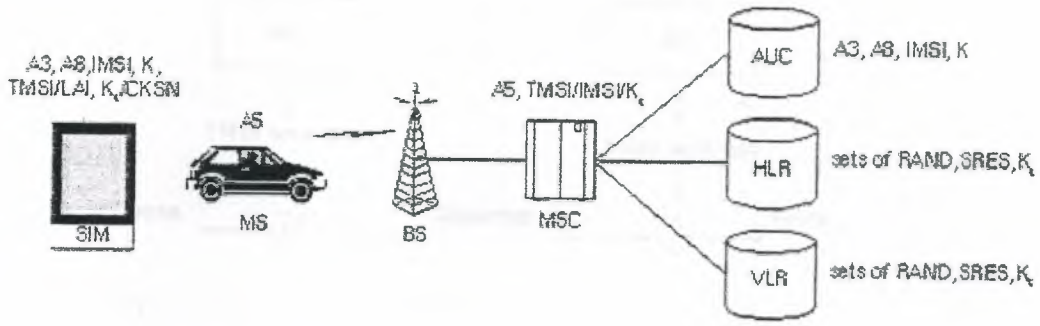

Figure 3.1 Distribution of Security Features in the GSM Network

3.1.1 GSM Security Model:

When a MS first signs on to a network, the HLR provides the MSC with five triples containing a RAND, a SRES to that particular RAND based on the Ki and a Kc based again on the same Ki. Each of the triples is used for one authentication of the specific MS. When all triples have been used the HLR provides a new set of five triples for the MSC

The MS then generates a Session Key, Kc, with the A8 algorithm using, again, the Challenge from the MSC and the Ki from the SIM. The BTS, which is used to communicate with the MS, receives the same Kc from the MSC, which has received it in the triple from the HLR. Now the over-the-air communication channel between the BTS and MS can be encrypted.

Each frame in the over-the-air traffic is encrypted with a different keystream. This keystream is generated with the A5 algorithm. The A5 algorithm is initialized with the Kc and the number of the frame to be encrypted, thus generating a different keystream for every frame. This means that one call can be decrypted when the attacker knows the Kc and the frame numbers. The frame numbers are generated implicitly, which means that anybody can find out the frame number at hand. The same Kc is used as long as the MSC does not authenticate the MS again, in which case a new Kc is generated. In practice, the same Kc may be in use for days. The MS authentication is an

optional procedure in the beginning of a call, but it is usually not performed. Thus, the Kc is not changed during calls Figure 3.2

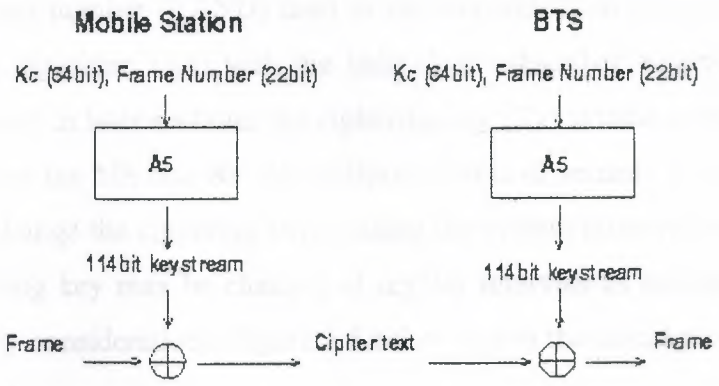

Figure 3.2 Frame encryption and decryption

Only the over-the-air traffic is encrypted in a GSM network. Once the frames have been received by the BTS, it decrypts them and sends them in plaintext to the operator's backbone network

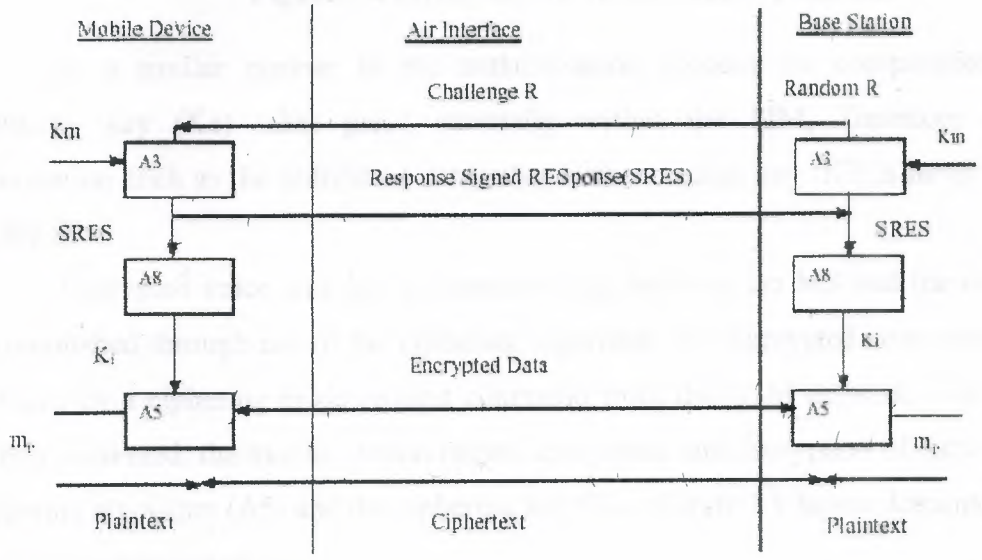

Figure 3.3 shows main parts of security model which is described above

3.1.2 Signaling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) which is used to produce the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). As will be shown in later sections, the ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations. Figure 3.4 below shows the calculation of the ciphering key (Kc).

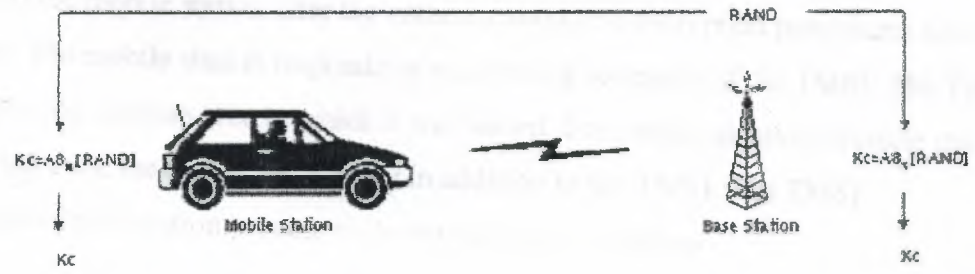

Figure 3.4 Ciphering Key Generation Mechanism

In a similar manner to the authentication process the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished through use of the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc). Figure 3.5 below demonstrates the encryption mechanism.

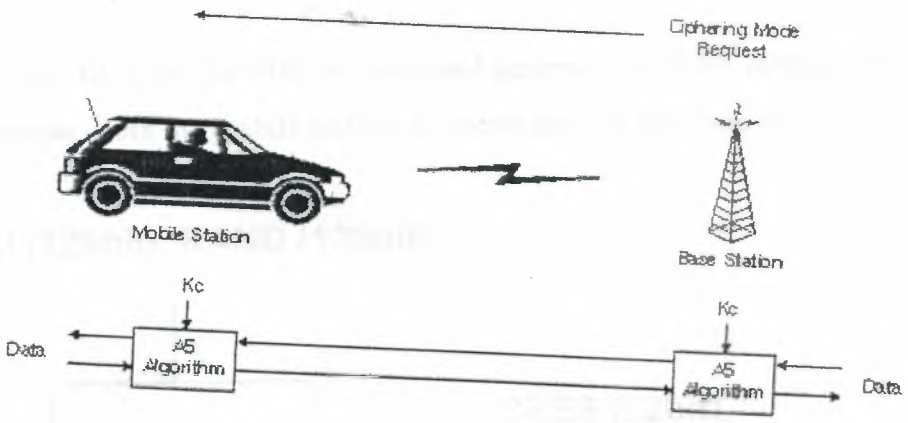

Figure 3.5 Ciphering Mode Initiation Mechanism

3.1.3 Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the (TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the (LAI) is necessary in addition to the TMSI. The TMSI allocation/reallocation process is shown in Figure 3.6 below

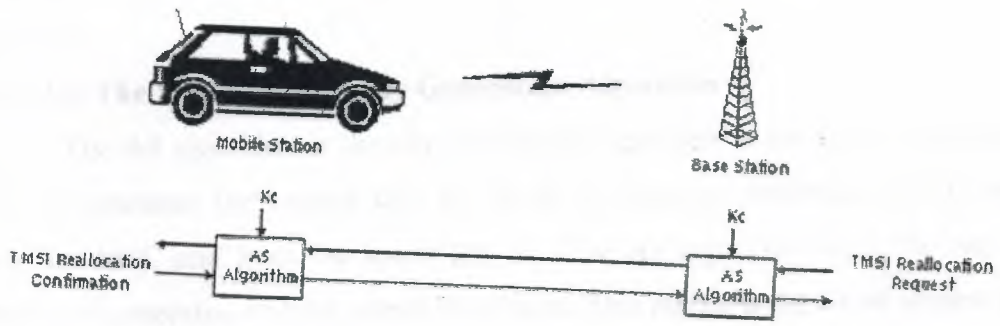

Figure 3.6 TMSK Reallocation Mechanism

3.2 Identification of used algorithms

3.2.1 A3 The MS Authentication Algorithm

The A3 is the authentication algorithm in the GSM security model. Its function is to generate the SRES response to the MSC's random challenge, RAND, which the MSC has received from the HLR. The A3 algorithm gets the RAND from the MSC and

the secret key Ki from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the Ki secret are 128 bits long. Figure3.7

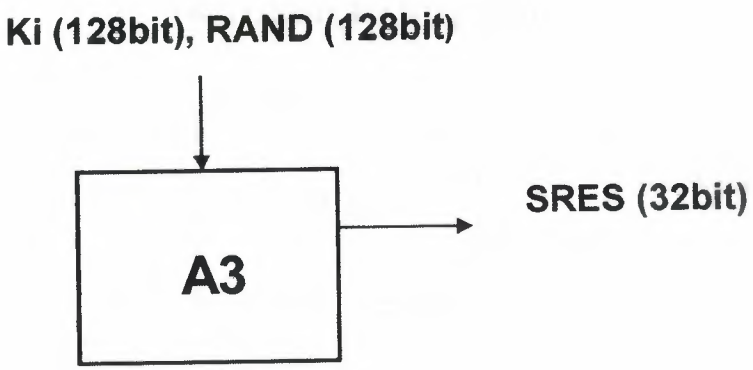

Figure 3.7 Signed response (SRES) calculation

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM Consortium. Other algorithms have been named as well, but almost every operator uses the COMP128 except a couple of exceptions Figure3.9.

The COMP128 takes the RAND and the Ki as input, but it generates 128 bits of output, instead of the 32-bit SRES. The first 32 bits of the 128 bits form the SRES response.

3.2.2 A8, The Voice-Privacy Key Generation Algorithm

The A8 algorithm is the key generation algorithm in the GSM security model. The A8 generates the session key, Kc, from the random challenge, RAND, received from the MSC and from the secret key Ki. The A8 algorithm takes the two 128-bit inputs and generates a 64-bit output from them. This output is the 64-bit session key Kc. See Figure 3.8. The BTS receives the same Kc from the MSC. HLR was able to generate the Kc, because the HLR knows both the RAND (the AuC generated it) and the secret key Ki, which it holds for all the GSM subscribers of this network operator. One session key, Kc, is used until the MSC decides to authenticate the MS again. This might take days.

As stated before, COMP128 is used for both the A3 and A8 algorithms in most GSM networks. The COMP128 generates both the SRES response and the session key, Kc, on one run. The last 54 bits of the COMP128 output form the session key, Kc, until

the MS is appended to authenticate again. See Figure 3.9. Note that the key length at this point is54 bits instead of 64 bits, which is the length of the key given as input to the

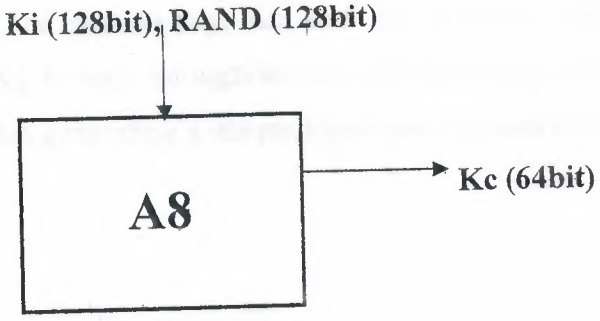

Figure 3.8 Session key (Kc) calculation

A5 algorithm. Ten zero-bits are the key generated by the COMP128 algorithm. Thus, we have a key of 64 bits with the last ten bits zeroed out. This effectively reduces the key space from 64 bits to 54 bits. This is done in all A8 implementations, including those that do not use COMP128 for key generation, and seems to be a deliberate feature of the A8 algorithm implementations.

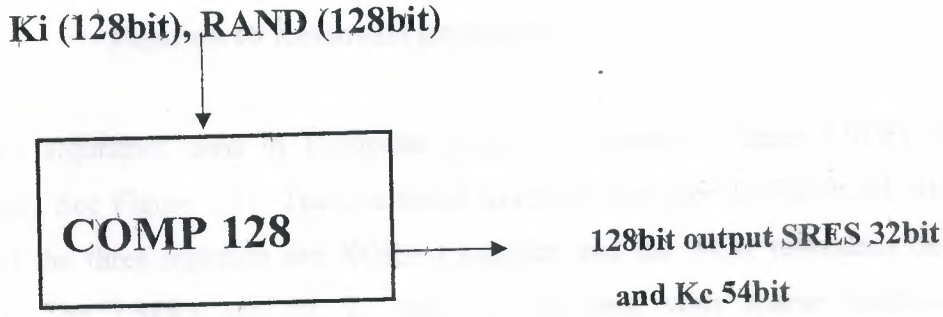

Figure 3.9 COMP128 calculation

Both the A3 and A8 algorithms are stored in the SIM in order to prevent people from tampering with them. This means that the operator can decide which algorithms to use independently from hardware manufacturers and other network operators. The authentication works in other countries as well, because the local network asks the HLR of the subscriber's home network for the five triples. Thus, the local network does not have to know anything about the A3 and A8 algorithms used.

3.2.3 A5/1 The Strong Over-the-Air Voice-Privacy Algorithm

The A5 algorithm is the stream cipher used to encrypt transmissions over-the-air. The stream cipher is initialized all over again for every frame sent. The stream cipher is initialized with the session key, Kc, and the number of the frame being de/encrypted. The same Kc is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique keystream for every frame. See Figure 3.10.

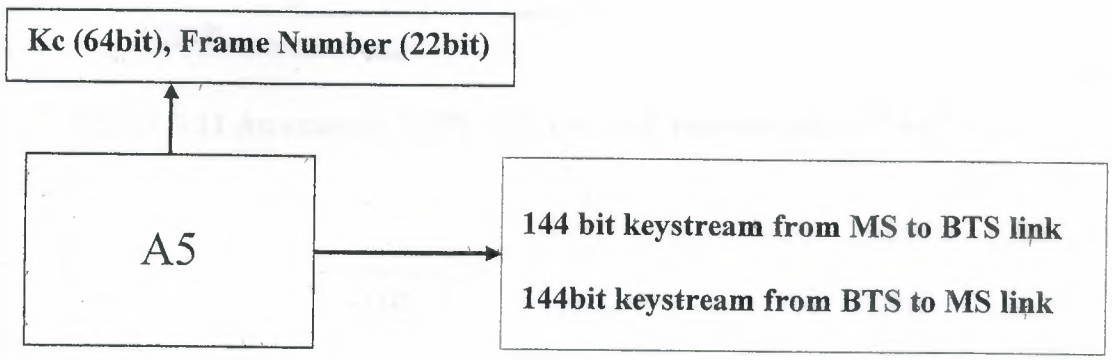

Figure 3.10 Keystream generation

The A5 algorithm used in European countries consists of three LSFRs of different lengths. See Figure 3.11. The combined length of the three LSFRs is 64 bits. The outputs of the three registers are XORred together and the XOR represents one keystream bit. The LSFRs are 19, 22 and 23 bits long with sparse feedback polynomials. All three registers are clocked, based on the middle bit of the register. A register is clocked if its middle bit agrees with the majority value of the three middle bits. For example, if the middle bits of the three registers are 1, 1 and 0, the first two register are clocked or if the middle bits are 0, 1 and 0, then the first and third register are clocked. Thus, at least two registers are clocked on every round . See Figure 3.11.

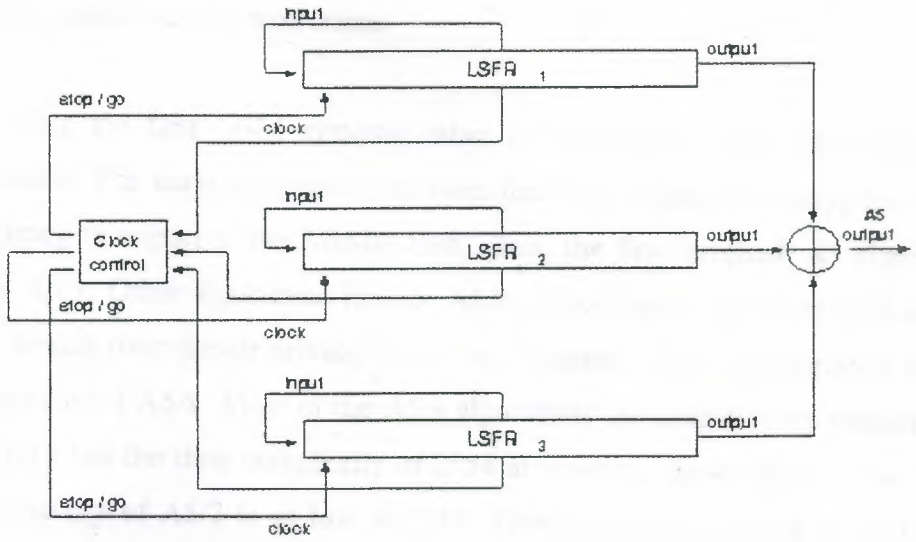

Figure 3.11 An example LSFR with feedback polynomial of $x^6 + x^4 + x$

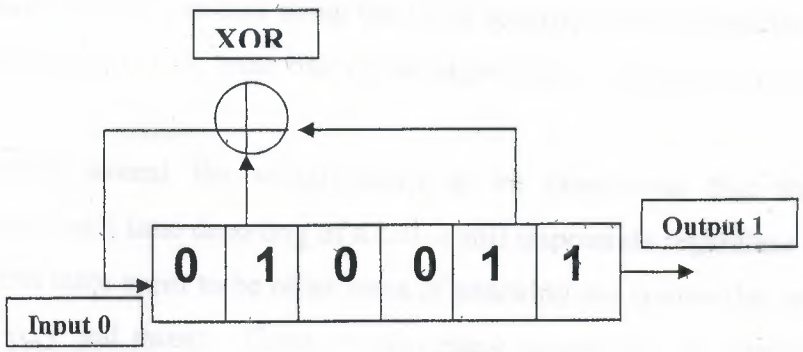

Figure 3.12 A5 LSFR constructions

The three LSFRs are initialized with the session key, Kc, and the frame number. The 64-bit Kc is first loaded into the register bit by bit. The LSB of the key is XORred into each of the LSFRs. The registers are then all clocked (the majority clocking rule is disabled). All 64 bits of the key are loaded into the registers the same way. The 22-bit frame number is also loaded into the register in the same way except that the majority clocking rule applies from now on. After the registers have been initialized with the Kc and the current frame number, they are clocked one hundred times and the generated keystream bits are discarded. This is done in order to mix the frame number and keying material together. Now 228 bits of keystream output are generated. The first 114 bits are

used to encrypt the frame from MS to BTS and the next 114 bits are used to encrypt the frame from BTS to MS. After this, the A5 algorithm is initialized again with the same Kc and the number of the next frame.

Since the first GSM systems, other A5 algorithms have been designed and implemented. The main motivation has been that the original A5 encryption algorithm is too strong to export to the Middle East. Thus, the first 'original' A5 algorithm was renamed A5/1. Other algorithms include A5/0, which means no encryption at all, and A5/2, a weaker over-the-air privacy algorithm. Generally, the A5 algorithms after A5/1 have been named A5/x. Most of the A5/x algorithms are considerably weaker than the A5/1, which has the time complexity of 2^54 at most as, shown above. The estimated time complexity of A5/2 is as low as 2^16. This encryption is used in the USA. The other A5 implementations have not leaked. Thus, there are no real facts about them, just guesses and assumptions.

3.3 Possible Interception Attacks

The interesting question about the GSM security model is whether a call can be eavesdropped, now that at least one of the algorithms it depends on has been proven faulty.

Scientist around the world seems to be unanimous that the over-the-air interception and real time decoding of a call is still impossible regardless of the reduced key space. But there seem to be other ways of attacking the system that are feasible and seem to be very real threats. There are also many attacks that are realistic, yet do not abuse any of the faults in the security algorithms.

1) Brute-Force Attack against A5

A real-time brute-force attack against the GSM security system is not feasible, as stated above. The time complexity of the attack is 2^54 (2^64 if the ten bits were not zeroed out). This requires too much time in order to be feasible in eavesdropping on GSM calls in real time. It might be possible to record the frames between the MS and the BTS and launch the attack afterwards though.

If we have a Pentium III class chip with approximately 20 million transistors and the implementation of one set of LSFRs (A5/1) would require about 2000 transistors, we would have a set of 10,000 parallel A5/1 implementations on one chip. If the chip was clocked to 600 MHz and each A5 implementation would generate one output bit for each clock cycle and we would need to generate 100+114+114 output bits, we could try

approximately 2M keys per second per A5/1 implementation. A key space of 2^54 keys would thus require about 900,000 seconds, 250 hours, with one chip. The attack can be optimized by giving up on a specific key after the first invalid keystream bit. This would cut the required time down by one third. The attack can also be distributed between multiple chips, thus drastically decreasing the time required.

2) Divide-and-Conquer Attack against A5

A divide-and-conquer attack manages to reduce the complexity from 2^54 of the brute-force attack to 2^45, which is a relatively dramatic change (2^9 = 512 times faster). The divide-and-conquer attack is based on a known-plain-text attack. The attacker tries to determine the initial states of the LSFRs from a known keystream sequence. The attacker needs to know 64 successive keystream bits that can be retrieved if the attacker knows some cipher text and the corresponding plain text. This depends largely on the format of the GSM frames sent back and forth. The GSM frames contain a lot of constant information, e.g. frame headers. The required 64 bits might not always be known, but 32 to 48 bits are usually known, sometimes even more. Keep in mind that the attacker needs only one 64-bit plain text segment.

In short the divide-and-conquer attack is implemented by guessing the content of the two shorter LSFRs and then computing the third LSFR from the known keystream. This would be a 2^40 attack, if the clocking of the first two registers were not dependent on the third register. Because the middle bit of the third register is used for clocking, we have to guess about half of the bits in the third register between the clock bit and the LSB as well. This fact increases the time complexity from 2^40 to 2^45.

Another divide-and-conquer attack based on the same assumptions with the average complexity of 2^40.16. Golic showed that only 2^62.32 internal states could be reached from the 2^64 initial states. Based on this assumption, he describes how to obtain linear equations by guessing n bits in the LSFRs. By solving these linear equations, one could recover the initial states of the three LSFRs. The complexity of solving the linear equations is 2^41.16. On average, one would resolve the internal state with 50 per cent chance in 2^40.16 operations.

A Time-Memory Trade-Off Attack based on the Birthday Paradox in the same paper. The objective of the attack is to recover the internal states of the three LSFRs at a known time for a known keystream sequence corresponding to a known frame number, thus reconstructing the session key, Kc.

3) Accessing the Signaling Network

As the two examples above clearly state, the A5 algorithm is not secure cryptographically, as there is another more feasible attack than the brute-force attack and it is not secure in practice either, because the brute-force attack in itself is not very hard to implement with current hardware. Yet, the algorithm is secure enough to prevent over-the-air call interception and real-time encryption cracking. Unfortunately, the air waves between the MS and the BTS are not the only vulnerable point in the GSM system.

As stated earlier, the transmissions are encrypted only between the MS and the BTS. After the BTS, the traffic is transmitted in plain text within the operator's network.

This opens up new possibilities. If the attacker can access the operator's signaling network, he will be able to listen to everything that is transmitted, including the actual phone call as well as the RAND, SRES and Kc. The SS7 signaling network used in the operator's GSM network is completely insecure if the attacker gains direct access to it.

In another scenario, the attacker could attack the HLR of a particular network. If the attacker can access the HLR, he will be able to retrieve the Kis for all the subscribers of that particular network. Luckily the HLR is usually a bit more secure than the rest of the network, thus making it a slightly less probable point of entry, yet not completely improbable either keeping in mind the potential gain involved.

Accessing the signaling network is not very difficult. Although the BTSs are usually connected to the BSC through a cable, some of them are connected to the BSC through a microwave or even a satellite link. This link would be relatively easy to access with the right kind of equipment. Most of the commercially available equipment for GSM eavesdropping seem to use this particular vulnerability. Unfortunately I cannot to verify this, because the equipment and specifications are available only to law enforcement personnel and such. The microwave link might be encrypted, however, depending on the hardware manufacturer, thus making it slightly more difficult to monitor it. It is really a question about whether the attacker wants to crack the A5 encryption protecting the session of a specific MS or the encryption between the BTS and the BSC and gaining access to the backbone network. The possibility of accessing the cable leaving the BTS should not be ruled out either. This might be a very real threat and an attack could go undetected for a long time, if implemented carefully. The ability to tap on to the data transmitted between the BTS and BSC would enable the attacker to

either monitor the call by eavesdropping on the channel throughout the call or he could retrieve the session key, Kc, by monitoring the channel, intercept the call over the air and decrypt it on the fly. Now that he knows the Kc, the real-time encryption is not a problem.

Another approach is through social engineering. This approach should not be underestimated although it sounds ludicrous. The attacker might pretend to be a repair man or such, enter a suitable building and install a wire tap. He might also bribe an engineer to do it for him or to give him all the Kis for all the subscribers of that particular operator. The possibilities are countless and real.

4) Retrieving the Key from the SIM

The security of the whole GSM security model is based on the secret Ki. If this key is compromised the whole account is compromised. Once the attacker is able to retrieve the Ki, he can not only listen to the subscribers calls, but also place calls billed to the original subscriber's account, because he can now impersonate the legitimate subscriber. The GSM network has trip wires for this: If two phones with the same ID are powered at the same time, the GSM network notices this, makes a location query for the phones, notices that the 'same' phone is in two different locations at the same time, and closes the account, thus preventing the attacker and the legitimate subscriber from placing calls. But this is not relevant if the attacker is only interested in listening to the calls of the subscriber, as is assumed in this paper. In this case, the attacker can stay passive and just listen to the call, thus staying invisible to the GSM network.

The Smartcard Developer Association and the ISAAC security research group discovered a flaw in the COMP128 algorithm that effectively enabled them to retrieve the secret key, Ki, from a SIM. The attack was performed on a SIM they had physical access to, but the same attack is applicable when launched over-the-air as well.

The attack is based on a chosen-challenge attack that works, because the COMP128 algorithm is broken in such a way that it reveals information about the Ki when the appropriate RANDs are given as arguments to the A8 algorithm. The SIM was accessed through a smartcard reader connected to a PC. The PC made about 150.000 challenges to the SIM and the SIM generated the SRES and the session key, Kc, based on the challenge and the secret key. The secret key could be deduced from the SRES responses through differential cryptanalysis. The smartcard reader used in implementing the attack could make 6.25 queries per second to the SIM card. So the attack required about eight hours to conduct. The results had to be analyzed as well, but this was

apparently very quick, compared to the actual attack. Thus, the attacker needs to have physical access to the target SIM for at least eight hours. This is still very reasonable.

Again this vulnerability is also applicable in a social engineering scenario. One can assume that a corrupt GSM dealer would clone SIM cards in this way and then sell the cloned cards to third parties who wish to remain anonymous and do not want to buy legitimate SIMs. One could also try to sell a cloned SIM to a certain person in order to be able to eavesdrop on his calls later. A corrupt employee might also provide the attacker with the SIM card of the victim, so that the attacker can clone the SIM and later eavesdrop on the owner's calls. These are all very realistic scenarios in which the vulnerability found in the COMP128 algorithm compromises the whole security model of the GSM system, thus leaving the subscribers in the open with no security at all.

5) Retrieving the Key from the SIM over the Air

The SDA and ISAAC researchers are confident that the same SIM-cloning attack could be launched over the air as well. Unfortunately, they can probably not confirm their suspicions, because the necessary equipment is illegal in the United States. The over-the-air attack is based on the fact that the MS is required to respond to every challenge made by the GSM network. If the signal of the legitimate BTS is over powered by a rogue BTS of the attacker, the attacker can bomb the target MS with challenges and re-construct the secret key from these responses. Again the MS has to be available to the attacker over the air for the whole time it takes to conduct the attack. It is not known how long the attack would take when conducted over the air. Estimates vary from eight to thirteen hours .

The attack might be conducted in a subway, where the signal of the legitimate BTS is not available, but the phone is still turned on. The subscriber would be unaware of such an attack though the fact that the battery of the phone has run out slightly quicker than usual might make him suspicious. The attack can also be performed in parts: instead of performing an eight-hour attack, the attacker could tease the phone for twenty minutes every day on the victim's way to work. Once the SIM is cloned, the SIM-clone is usable until the subscriber gets a new SIM, which in practice does not happen very often.

In another scenario, the subscriber is on a business trip in another country. The attacker has somehow bullied the local GSM operator to perform this attack on the subscribers' phone. The attacker would again be able to reconstruct the Ki based on the MS's SRES answers and the attack would probably go unnoticed, because the

challenges originate from a legitimate network. Keep in mind that the local network does not know anything about the Ki, because the triples originate from the HLR of the subscribers home network. Thus, the local network has to deduce the Ki from the A3 responses.

6) Retrieving the Key from the AuC

The same attack used in retrieving the Ki from a SIM card can be used to retrieve the Ki from the AuC. The AuC has to answer to requests made by the GSM network and return valid triples to be used in MS authentication. The procedure is basically identical to the procedure used in the MS to access the SIM card. The difference is that the AuC is a lot faster in processing requests than a SIM card is, because it needs to process a lot more requests compared to one SIM card. The security of the AuC plays a big role in whether this attack is possible or not and that is out of the scope of this paper.

7) Cracking the A8 Algorithm

Another possibility is that someone will be able to crack the A8 key generation algorithm and retrieve the secret key, Ki, based on the random challenge, RAND, the session key, Kc, and the SRES response (assuming the same algorithm is used for both A3 and A8 as is the case with COMP128) with a minimal amount of work. For example, the attacker may find a RAND that produces the Ki as a result (an over simplified example). All three variables are obtained relatively easily. The RAND and SRES are sent over the air in plain text and the session key Kc can be relatively easily deduced from the encrypted frames and the known plain text given enough time. Vulnerability like this in the key generation algorithm would of course devastate the whole GSM security model and give the GSM Consortium something to think about when designing their next security algorithms.

3.4 Possible Improvements

Security could be improved in some areas with relatively simple measures. The operator could use another cryptographically secure algorithm for A3. This would require issuing new SIM-cards to all subscribers and updating HLR software. This would effectively disable the attacker from cloning SIM-cards, the most dangerous attack, which is discussed above. This would also be the easiest improvement introduced here, because the network operator can make the changes itself and does not need the support of hardware or software manufacturers or the GSM Consortium.

Another solution would be to employ a new A5 implementation with strong encryption so that a brute-force attack is not feasible in any case. This would disable the attacker from recording transmitted frames and cracking them in his spare time. This improvement would require the cooperation of the GSM Consortium. The hardware and software manufacturers would have to release new versions of their software and hardware that would comprise with the new A5 algorithm.

Third solution would be to encrypt the traffic on the operators' backbone network between the network components. This would disable the attacker from wiretapping to the backbone network. This solution could probably also be implemented without the blessings of the GSM Consortium, but the cooperation of the hardware manufacturers would still be required.

In sum, none of the improvements above are too hard to implement. They all present new expenses mostly to the network operator and are not thus very attractive from the network operator's point of view. Thus, these improvements will probably not be implemented until the insecurity of the GSM networks becomes public knowledge and the network operators are forced to improve the security of the network. All three improvements would be necessary in order to secure the network against all attacks introduced in this chapter.

IV. ATHENTICATION AND FRAUD

4.1 Authentication mechanism

As the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the Authentication Center. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjunction with the subscriber's secret key and a ciphering algorithm called A3, to generate a number that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated.

The above calculated number is also used, together with a TDMA frame number and another ciphering algorithm called A5, to encipher the data sent over the radio link, preventing others from listening in. Enciphering is an option for the very paranoid, since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.

When the MS (which contains the SIM) first comes to the area of a particular MSC, the MSC sends the Challenge of the first triple to the MS. The MS calculates a SRES with the A3 algorithm using the given Challenge and the Ki residing in the SIM. The MS then sends the SRES to the MSC, which can confirm that the SRES really corresponds to the Challenge sent by comparing the SRES from the MS and the SRES in the triple from the HLR. Thus, the MS has authenticated itself to the MSC.

Authentication in a digital setting is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message. Authentication protocols can be based on either conventional secret-key cryptosystems like DES or on public-key systems like RSA; authentication in public-key systems uses digital signatures.

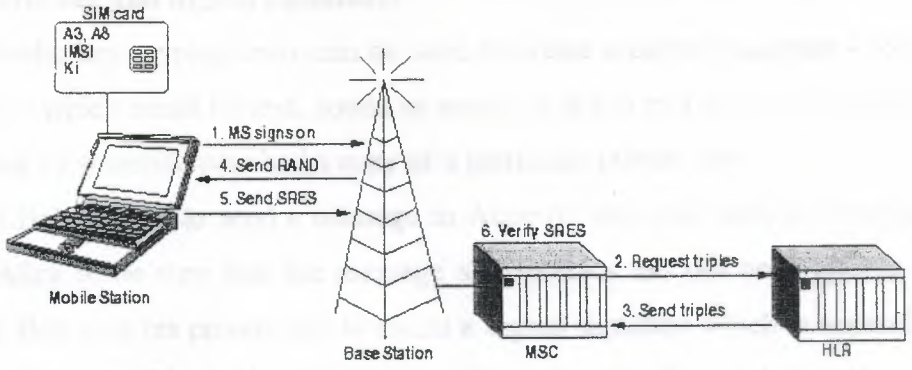

Figure 4.1 mobile station authentications

4.2 Authentication and Signatures

Mobile phone must present SRES to a RAND Before allowing the phone to access the network. The challenge is unique, and is generated within the home system (the system where the phone is registered). The algorithm and the master key are both stored on SIM. This allows for the possibility that the algorithm may actually vary with different service providers, and indeed this is the case for about 40% of phones. The algorithm A3 accepts a 64 bit challenge and produces a 64 bit response, based on the secret key in the SIM. At the same time, an algorithm A8 calculates the corresponding session key for privacy during the call. The "standard" algorithm performing these functions together is called COMP128. This algorithm is held tightly secret by the GSM MoU; only the interface to it is public.

Because the algorithm might not even be known at a visited system, the home system has to perform all of the verification and key generation functions. As an optimization for network traffic, a number of triplets are forwarded upon the first access. These consist of:

1. A challenge to be sent to the mobile station
2. The expected response
3. The session key to be used after authentication succeeds.

Relying on the secrecy of the algorithm is rarely a good move, and indeed COMP128 was disclosed in 1998. Furthermore, the algorithm is weak, allowing disclosure of the Key with a few million interactions with the SIM card.

4.2.1 Public key and digital signature:

Public key cryptography can be used to create a digital signature - to "sign" a digital file (which could be text, sound or anything at all) in a way which proves that it was signed by someone who had a copy of a particular private key.

If Bob wanted to send a message to Alice (in this case without encryption) but wanted Alice to be sure that the message she receives has not been altered since he signed it, Bob uses his private key to create a digital signature which is appended to the message. This would look like a dozen or so lines of gobbledygook text at the end of the message. Here is the preceding paragraph (reformed into narrower lines for convenience), digitally signed with my private key:

If Bob wanted to send a message to Alice (in this case without encryption) but wanted Alice to be sure that the message she receives has not been altered since he signed it, Bob uses his private key to create a digital signature which is appended to the message. This would look like a dozen or so lines of gobbledygook text at the end of the message.

Alice uses PGP and Bob's public key to verify the signed document. If any change has occurred to either the document or the signature, then PGP will detect this. Assuming that Bob is the only person who has a copy of his private key, she knows that the message she received is identical to what Bob signed. Bob could also encrypt the signed message with Alice's public key, so that only she could decrypt it.

4.3 Cloning and Fraud

Even if the SIM card does ultimately prove itself invulnerable to cloning, GSM will still not put a stop to fraud.

The GSM networks in operation throughout the world all share a common goal -- to deliver high quality, reliable and secure wireless communication services to their subscribers. The design of the GSM network, and later the DCS1800 network, was a tremendous effort of will, engineering talent, financial capital and marketing foresight. The resulting standard created a more secure way to deliver wireless telecommunications services compared with analogue networks in operation at the time.

The selection and endorsement of the GSM standard by many countries around the world today is testimony to the success of that effort. Increasing numbers of wireless subscribers demand seamless operation of their services while roaming to and from their homes, offices, and wherever their personal and business interests may draw them.

Their itineraries may require that they travel to a meeting in the same city where they live, in the same country, or even in a compatible network on the other side of the world. Herein lies the crux of the problem.

Accelerating use of mobile communication services by a growing subscriber base across an expanding network of participating roaming partners has created an opportunity to technically de-fraud the GSM network to a degree most participants in the early design of the network would not have thought possible. The experience of fraud in analogue and D-AMPS wireless networks provides a good glimpse into how it mutates over time, always seeking the path of least resistance. What was once solved with subscriber and handset identity validation by the (HLR) and (VLR) transformed into a new form of fraud via the capture and transmission of valid identity pairs by impostors. In other words, fraud has mutated from tumbling into cloning.

What was solved with the use of (PINs) transformed into a new form of fraud via the capture and transmission of those stolen PINs or via the hijacking of a voice channel by a fraudster once the network security features were performed. The battle, and the list of new forms of fraud, goes on.

It's the analogue carriers' painful experience that for any one technological solution to fraud, there exists a multitude of ways to circumvent that technology. The security goal becomes less a search for the silver bullet, and more a process of gathering as much hard data about what is actually happening on the network in order to detect and mitigate the changing forms of wireless fraud as they emerge.

Normally, when faced with the threat of billions of dollars of wireless fraud, the impulse is to build more and more complex technological solutions to prevent a security breach. Fraud always targets the weakest link. In the GSM network today, the weakest links are in international roaming markets.

The "challenge and response" technique incorporated into the GSM authentication process allows the (SIM) to verify its (IMSI) by demonstrating knowledge of the authentication algorithm and the unique key, Ki. According to the protocol, the home system sends a random challenge to the handset. Only the handset can encrypt the challenge, using both the algorithm and Ki resident within the SIM assigned to that subscriber. Using the stored algorithm, the SIM is able to generate the correct response back to the home system.

In such a protocol, the single point of failure is the Authentication Center in the home system.

However, with diligence and adherence to strict security protocols, the Authentication Center could conceivably be made reasonably secure from theft of IMSI and Ki sets, both by outside and inside thieves. In theory, authentication should prevent fraudulent access to wireless service.

However, the high technology route may miss the mark. The methods to defraud a system can often revolve around quite simple and direct applications of the principle that a chain is only as strong as its weakest link.

Let's take a look at increasing international roaming in GSM networks as one example of this principle in action. As mentioned above, GSM and DCS1800 networks are expanding at unprecedented rates. The volume of billable calling traffic is increasing to levels that were only dreamed of just a few years ago. Of course, in order to deliver billable calling traffic, locally or across the globe, there is a tremendous amount of non-signaling traffic which is required to support all that billable activity.

The validation and authentication protocols themselves, which must be transmitted in order to deliver secure wireless service for each call, reserve a lot of communications overhead. In order to provide for the volume of calling and non-signaling traffic required today, the network administrators may choose to configure their VLRs to stand in as alternates for the "unique challenge and response" protocol of authentication. Instead of requiring the home system to test the results of authentication's "challenge and response" while the subscriber is roaming, the HLR may abdicate its authentication responsibilities to the VLR.

In this scenario, it is the serving system's VLR which sends the unique challenge and tests the response from the SIM. The VLR will have previously requested and received the triplets from the home system prior to the unique challenge in order to allow the VLR to remove some of the intersystem communications traffic.

The response is then tested against a fresh set of stored triplets -- the unique challenge, the response, and Ki. The serving system has two additional configuration options. The VLR may chose to re-use the triplets in order to further reduce the traffic back to the home system for fresh triplet sets. The VLR may also be configured not to authenticate on every call.

Today, the network designers' goal is to deliver wireless service to roaming subscribers within the constraints of the intersystem network capacity. Unfortunately, this is counter to the previous goal we have been discussing, namely the application of sophisticated authentication technologies to deliver wireless service in a secure network.

If increasing network traffic efficiencies are the goal, then it becomes expedient to relax the very deployment of the oft-admired GSM authentication protocol.

Contrary to the better judgment of the original designers of the system, it becomes reasonable to allow the VLR to subsume the role of the home system, opening up the VLR to theft of valid authentication triplets. It even becomes acceptable to reuse authentication triplets at the VLR instead of reaching back to the home system for fresh sets. Amazingly, it becomes all right to configure the home or visited system not to authenticate on each and every call. Success appears to be the culprit in the rising tide of GSM international roaming fraud. There is too much traffic to do it right.

The hard choices in deploying GSM authentication today are but one example of the weak spots that fraudsters target in their attack on GSM networks. With the expansion of GSM networks, let's assume that the capacity figures and projections of the network administrators are valid and that they must restrict the non-signaling traffic. There are techniques which can be employed to limit the network exposure to fraud.

In the roaming example described above, the problem is most acute when subscribers' itineraries take them to international markets. The problem is worse for two reasons. First, the intersystem traffic is heavier. With heavier traffic, the network administrators' urge to circumvent the authentication protocol is stronger. Secondly, the fraudulent usage is more expensive in roamed markets. Unlike fraud in the home market where the cost of service is frequently analyzed in the soft currency terms of either unbillable network capacity or subscriber disaffection with fraudulent calls displayed on bills, fraud which occurs in a roaming market requires the billing and settlement in hard currency between roaming partners for a portion of the price of the service which was used -- or in this case, misused.

The GSM MoU Association has taken steps to mitigate the gaps in network security. It has begun by requiring certain reporting protocols between roaming partners. The requirements reflect an acknowledgment that if wireless service is to be delivered in this way, and if the authentication deployment network is to be configured within the constraints of the capacities of the roaming partners, then certain logical business rules need to be applied to protect the interests of the home carriers with whom the burden of payment resides.

As with may roaming agreements within AMPS and D-AMPS systems, GSM roaming partners now must report back to the home system the details of service which was delivered to their roaming subscribers shortly after that service was delivered.

Typically, the interval between delivery of the service to the roaming subscriber and reporting the service delivery to the home carrier is 24 hours. The home carrier then is free to assess the risk of service delivery to that subscriber and is in a position to notify the visited system of any change in that subscribers authorized use of roaming privileges.

The new reporting requirements also target the troublesome rise in subscription fraud. The illegal use of roaming privileges by a subscriber who has no intention of ultimately paying the bill is a costly crime for the home carrier. As with the technical roaming fraud described above, the home carrier is responsible for settling the roaming charges in hard, not soft, currency.

Fraud management systems which incorporate mechanisms to integrate service usage data are an additional weapon in the arsenal of the GSM carrier as they battle the early forms of technical and subscription fraud emerging in their networks.

These fraud management systems perform the role of early-warning systems for carriers, complementing the GSM roaming reporting requirement with hard data about the patterns of service usage on their networks. The designers continue to improve a robust network. The wireless vendor community must apply itself to the full range of fraud issues, and build solutions to remove exposure and anticipate the fraudsters' next move. For example, the integration of features to deliver and receive roaming service usage data in near real-time would be a welcome start. 24 hours is better than two days; one hour is even better.

Is there fraud after GSM? Unfortunately, yes. The question isn't so much whether a SIM can be cloned, as is claimed in the labs, or not. Fraud always targets the weakest link. In the GSM world today, the weakest links are subscription fraud and technical fraud in international roaming markets.

The challenge is to monitor and profile the activity using hard data, and to be alert to the changing face of fraud. As GSM markets grow, so too grow the risks, with compromises taken to deliver the service in the real world. The industry needs to learn about fraud and fight it using high technology, common sense business rules and integrated information and fraud management systems.

4.4Cracking GSM's Security Code

How secure are your digital cellular-phone conversations? Could someone be listening in on your calls? These questions and others were raised recently when two Israeli researchers claimed to have cracked the GSM (global standard for mobile communications) encryption code, making it easy to theoretically eavesdrop on phone conversations.

A5/1 is the encryption method used by GSM to protect the over-the-air privacy of cellular communications. Worldwide, about 230 million people use GSM service, 5 million of whom live in the United States.

Those researchers believe that GSM's level of security makes it vulnerable to hardware-based attacks by large organizations though not to software-based attacks by hackers. They describe a new attack on A5/1 based on subtle flaws in the encryption. The attack can find the key in less than a second using a single PC with 128MB of RAM and two 73GB hard disks, by analyzing the output of the A5/1 algorithm in the first two minutes of the conversation.

Although some researchers believe that but Attacks against A5/1 are still considered not practicable, because there is still no evidence of any commercial violation of the A5/1 algorithm, which has now been in use for more than 10 years.

CONCLUSION

GSM network proved itself more secure compared to other telecommunication networks, voice speech is transformed into radio waveform. This form is encrypted and transmitted over the air, reaches the receiver person decrypted and then transformed into speech again.

This encryption and decryption process maintains an acceptable security level. Also GSM authenticates the subscriber using a secret key (Ki) stored in both (SIM) and (AuC), both (MS) and (AuC) through certain calculations both got same key if so, subscriber is authenticated and call is performed. Authentication process is a good solution for cloning and preventing any one to call in other person's account.

But in spite of that, GSM security model is broken on many levels and is thus vulnerable to numerous attacks targeted at different parts of an operator's network.

Assuming that the security algorithms were not broken, the GSM architecture would still be vulnerable to attacks targeting the operator's backbone network or HLR and to various social engineering scenarios in which the attacker bribes an employee of the operator, etc.

Further more, the secretly designed security algorithms incorporated into the GSM system have been proven faulty. The A5 algorithm used for encrypting the over-the-air transmission channel is vulnerable against known-plain-text and divide-and-conquer attacks and the intentionally reduced key space is small enough to make a brute-force attack feasible as well. The COMP128 algorithm used in most GSM networks as the A3/A8 algorithm has been proved faulty so that the secret key Ki can be reverse-engineered over-the-air through a chosen challenge attack in approximately ten hours.

All this means that if somebody wants to intercept a GSM call, he can do so. It cannot be assumed that the GSM security model provides any kind of security against a dedicated and professional attacker. The required resources depend on the attack chosen. Thus, one should not rely solely on the GSM security model when transferring confidential data over the GSM network.

In addition to the possibility of call interception, the faulty COMP128 algorithm makes SIM cloning a threat as well, thus making it possible for an attacker to place calls at someone else's expense.

However, the reality is that although the GSM standard was supposed to correct the problems of phone fraud and call interception found in the analog mobile phone systems by using strong crypto for MS authentication and over-the-air traffic encryption, these promises were not kept. The current GSM standard and implementation enables both subscriber identity cloning and call interception. Although the implementation of cloning or call interception is a little bit more difficult, due to the digital technology that is used, compared to the analog counterparts, the threat is still very real, especially in cases where the transmitted data is valuable. Basically, we are where we used to be with the analog cell phones when it comes to security although the GSM Consortium tries to deny it.

In a technological world, it is always imperative to stay one step ahead of the bad guys. In the GSM community, GSM is always 10 steps or further ahead, because of GSM's sophisticated encryption safeguards and diligent efforts to constantly upgrade the security of the network.

At last I can say that although GSM security is broken by professional attackers but GSM phones are still more secure than analog cellular phones, which do not encrypt conversations, eavesdropping on calls is certainly beyond the reach of the average man on the street. It requires a digital scanner; today digital scanners are expensive. and as attackers creates more ways to break security of the network there are always new ways to encrypt data which takes some time for attackers to break.

REFERENCES

[1] Fakhreddin Mamdov, Telecommunications (Lecture Note), Near East University Press, lefkosa, 1999

[2] Schneier B., Applied Cryptography, 2nd Ed., Wiley, New York, retrieved 29.9.1999

[3] Anon., "Crack A5", *"http://jya.com/crack-a5.htm* " retrieved 29.9.1999

[4] Anderson Ross, "A5 - The GSM Encryption Algorithm" "*http://chem.leeds.ac.uk/ICAMS/people/jon/a5.html*" retrieved 17.6.1994

[5] Racal Research Ltd., "GSM System Security Study" "*http://jya.com/gsm061088.htm* " retrieved 29.9.1999

[6] Ian Goldberg and Marc Brinceno, "GSM Cloning", *"http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html"* retrieved 24.10.1999

[7] Lauri Pesonen,"GSM Interception", retrieved 21.11.1999 *"http://www.dia.unisa.it/ads.dir/corso-swcurity*."

[8] David Margrave, George Mason's University "security and encryption", *"http://www.spyhad.narod.ru/phreak/gsm-security.html."*

[9] Robin Whittle, "GSM Interception", retrieved 19.12.1996 "http://www.ozemail.com.au/firspr/contreg/link.htm"