



NEAR EAST UNIVERSITY

**GRADUATE SCHOOL OF APPLIED
AND SOCIAL SCIENCES**

**GSM AND GPRS SECURITY USING DES
APPLICATION**

Hani Jaber

Master Thesis

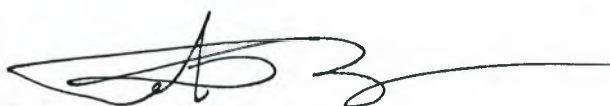
**Department of Electrical and Electronic
Engineering**

Nicosia 2003



**Approval of the Graduate School of Applied and
Social Sciences**

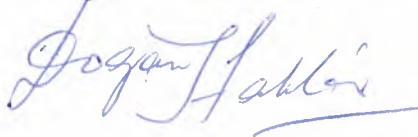
**Prof. Dr. Fakhraddin Mamedov
Director**



**We certify this thesis is satisfactory for the award of the
Degree of Master of Sciences in Electrical and Electronic Engineering**

Examination Committee in Charge:

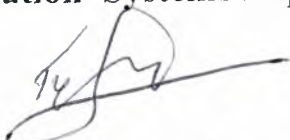
**Assist. Prof. Dr. Doğan Haktanır, Committee Chairman, Electrical and
Electronic Engineering Department, NEU**



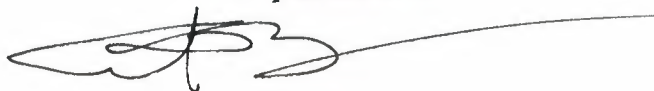
**Assist. Prof. Dr. Kadri Bürüncük, Committee Member, Electrical and
Electronic Engineering Department, NEU**



**Assoc.Prof. Dr. İlham Huseynov Committee Member, Computer
Information Systems Department, NEU**



**Prof. Dr. Fakhraddin Mamedov, Supervisor, Electronic Engineering
Department, NEU**



ACKNOWLEDGEMENTS

All thanks and praise are due to Allah who most certainly favoured me over much of his creations.

First of all I would like to thank sincerely my thesis advisor Prof. Dr Fakhraddin Mamedov for his valuable advice given throughout the preparation of this thesis.

I largely appreciate the productive and constructive advices of Assoc.Prof.Dr Adnan Khashman during my study period.

I would like to express my gratitude to Assist. Prof. Dr. Doğan Haktanır, Assist. Prof. Dr. Kadri Bürüncük and Assoc.Prof. Dr. İlham Huseynov for their valuable advices.

I would like to thank my parents for helping me consistently and constructively all the way through my study period and my brothers and sisters.

A very devoted and unique thank goes to my colleagues Hazem Abu Shaban and Reyad Bader for giving me exclusive and consistent help.

ABBREVIATIONS

A3	Authentication Algorithm
A5	Ciphering Algorithm
A8	Ciphering Key Computation
AGCH	Access Grant Channel
AK	Anonymity Key
AKA	Authentication And Key Agreement
AMF	Authentication Management Field
AMPS	Advanced Mobile Phone Service
AoC	Advice Of Charge
ARQ	Automatic Repeat Request Mechanism
AUC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
BAIC	Barring Of All Incoming Calls
BAOC	Barring Of All Outgoing Calls
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BER	Bit Error Rate
BOIC	Barring Of Outgoing International Calls
BOIC-exHC	Barring Of Outgoing International Calls Except Those Directed Toward The Home Plmn Country
bps	Bits Per Second
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Sub-System
BTS	Base Transceiver Station
C/I	Carrier-To-Interference Ratio
CBC	Cipher Block Chaining
CC	Call Control
CCCH	Common Control Channel
CDMA	Code Division Multiple Access
CEPT	Conference Of European Posts And Telecommunications
CFB	Call Forwarding On Mobile Subscriber Busy
CFNRc	Call Forwarding On Mobile Subscriber Not Reachable
CFNRy	Call Forwarding On No Reply
CFU	Call Forwarding Unconditional
CG	Charging Gateway
CGI	Cell Global Identity
CKSN	Cipher Key Sequence Number
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CM	Communication Management
CoLP	Connected Line Identification Presentation
CoLR	Connected Line Identification Restriction
CS	Circuit Switched
CUG	Closed User Group
CW	Call Waiting

DCCH	Dedicated Control Channel
DCS	Digital Cellular System
DES	Data Encryption Standard
DNS	Domain Name Server
DSA	Digital Signature Algorithm
DTX	Discontinuous Transmission
ECB	Electronic Code Book
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control Channel
FCCH	Frequency-Correction Channel
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction Code
FER	Frame Erasure Rate
GIWU	GSM Interworking Unit
GMSC	GSM Mobile Services Switching Center
GMSK	Gaussian Minimum Shift Keying
GP	Guard Period
GSM	Global System For Mobile Communications
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
JDC	Japanese Digital Cellular
Kc	Ciphering Key
Ki	Individual Subscriber Authentication Key
KSI	Key Set Identifier
KSS	Key Stream Segment
LA	Location Area
LAI	Location Area Identity
LFSR	Linear Feedback Shift Register
LOS	Line-Of-Sight
MAC	The Message Authentication Code Included In Autn, Computed Using F1
ME	Mobile Equipment
MM	Mobility Management
MoU	Memorandum Of Understanding
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSISDN	Mobile Station Isdn Number
MSRN	Mobile Station Roaming Number
NADC	North American Digital Cellular
NIST	National Institute Of Standards And Technology
NMT	Nordic Mobile Telephone
NSS	Network And Switching Subsystem
OAM	Operation, Administration And Maintenance
OMS	Operation And Maintenance Subsystem
OSS	Operation And Support Subsystem

PAD	Packet Assembler Disassemble
PCH	Paging Channel
PCS	Personal Communications Services
PDC	Personal Digital Cellular
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PS	Packet Switched
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
P-TMSI	Packet-TMSI
Q	Quintet,
RACH	Random Access Channel
RAI	Routing Area Identifier
RAND	Random Challenge
RF	Radio Frequency
RPE-LTP	Regular Pulse Excitation Long-Term Prediction
RR	Radio Resources Management
RSA	Rivest, Shamir, Adleman
S	Stealing Flags
S DES	Simplified Data Encryption Standard
SACCH	Slow Associated Control Channel
SCH	Synchronization Channel
SDCCH	Standalone Dedicated Control Channel
SDCCH	Standalone Dedicated Control Channel
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIM	(GSM) Subscriber Identity Module
SMS	Short Message Services
SM-SC	Short Message Service Center
SMS-CB	Short Message Services Cell Broadcast
SMS-MO/PP	Short Message Services Mobile Originating/Point-To-Point
SMS-MT/PP	Short Message Services Mobile Terminating/Point-To-Point
SN	Serving Network
SNR	Signal To Noise Ratio
SQN	Sequence Number
SQNHE	Individual Sequence Number For Each User Maintained In The Hlr/Auc
SQNMS	The Highest Sequence Number The SIM Has Accepted
SRES	Signed Response
SS	Supplementary Services
T	Triplet, GSM Authentication Vector
TACS	Total Access Communication System
TCH	Traffic Channel
TCH/F	Traffic Channel/Full Rate
TCH/H	Traffic Channel/Half Rate
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm

UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module
VAD	Voice Activity Detection
VLR	Visitor Location Register
XRES	Expected Response

ABSTRACT

With the drive for a more distributed workforce, industry has become more reliant on mobile communications. Initially used only for voice, mobile telephones are now also used for data transfer. This means that potentially sensitive company information is being transmitted in broadcast form across the air gap between the mobile terminal and the associated base station.

This thesis presents the security measures taken in two of the modern telecommunication systems which are GSM and GPRS and emphasizing on security and encryption algorithms used to make the system as secure as the public switched telephone network.

As an application for this thesis I used software using Delphi for conventional encryption algorithms (Data Encryption Standard (DES)) which considered one of the most widely used in wireless communication system.

TABLE OF CONTENTS

ACKNOWLEDGMENT	i
LIST OF ABBREVIATIONS	iii
ABSTRACT	vii
TABLE OF CONTENTS	viii
INTRODUCTION	1
1. BACKGROUND ON GSM	3
1.1 Overview	3
1.2 Brief History of The Cellular Mobile Radio and GSM	3
1.3 GSM Compared To the Old Analogue-Based Systems	6
1.4 Architecture of The GSM Network	7
1.4.1 Mobile Station	8
1.4.2 The Base Station Subsystem	9
1.4.3 The Network and Switching Subsystem	10
1.4.4 Additional Functional Elements	12
1.5 GSM Radio Channel	12
1.5.1 TDMA Frame Structures, Channel Types, and Burst Types	13
1.6 From Source Information to Radio Waves	14
1.6.1 Speech Coding	15
1.6.2 Channel Coding	16
1.6.3 Interleaving	17
1.6.4 Burst Assembling	18
1.6.5 Ciphering	19
1.6.6 Modulation	19
1.7 Summary	20
2. GSM AUTHENTICATION AND ENCRYPTION	21
2.1 Overview	21
2.2 The Purpose for Security	21
2.3 Limitations of Security	22
2.3.1 The Countermeasures are Designed:	22
2.3.2 The Security Processes Must Not:	22

2.4 Descriptions of The Functions of The Services	23
2.4.1 Anonymity	23
2.4.2 Authentication	23
2.4.3 User Data and Signaling Protection	24
2.5 Implementation and Roaming	24
2.6 Introductions to The GSM Security Model	25
2.6.1 Distribution of Security Features in The GSM Network	25
2.6.2 A3, The Ms Authentication Algorithm	28
2.6.3 A8, The Voice-Privacy Key Generation Algorithm	29
2.6.4 A5/1, The Strong Over-The-Air Voice-Privacy Algorithm	30
2.7. Overview of Cryptography	31
2.7.1 Symmetric Algorithms	31
2.7.2 Public Key Algorithms	31
2.8 Possible Interception Attacks	32
2.8.1 Brute-Force Attack Against A5	32
2.8.2 Divide-And-Conquer Attack Against A5	33
2.8.3 Accessing The Signalling Network	34
2.8.4 Retrieving The Key From The SIM	35
2.8.5 Retrieving The Key From The SIM Over The Air	36
2.8.6 Retrieving The Key From The AUC	37
2.8.7 Cracking The A8 Algorithm	37
2.9 Possible Improvement	38
2.10 Summary	39
3 AUTHENTICATION AND SECURITY IN GPRS ENVIRONMENT	40
3.1 Overview	40
3.2 Short Introduction To GPRS	40
3.2.1 GPRS Network Architecture	42
3.3 GPRS Applications	45
3.3.1 PTP Service	45
3.3.2 PTM Service	46
3.3.3 SM Service	46
3.4 User Authentication and Security Inside GPRS Network	47
3.4.1 Authentication	47

3.4.2 Ciphering	49
3.4.3. Identity Protection	51
3.5 Secure GPRS Interworking With Packet Data Network	51
3.5.1. Transparent Access To Internet	53
3.5.2 Non-Transparent Access to Intranet or ISP	53
3.5.3 Threats From External Networks	54
3.6 Secure Interworking Between GPRS Networks	55
3.7. IPsec	56
3.8 system evaluation	58
3.9 Summary	59
4. CONVENTIONAL ENCRYPTION: MODERN TECHNIQUES	60
4.1 Overview	60
4.2 Simplified DES	60
4.2.1 S-DES Technique	60
4.2.2 S-DES Encryption	64
4.2.3 Relationship To DES	65
4.2.4 Relationship to DES	70
4.3. Block Cipher. Principles	71
4.3.1 Stream Ciphers and Block Ciphers	71
4.3.2 Motivation For The Feistel Cipher Structure	72
4.4 The Data Encryption Standard	75
4.4.1 DES Encryption	77
4.4.2 Key Generation	85
4.4.3 DES Decryption	86
4.5 Summary	86
CONCLUSION	87
REFERENCES	88
APPENDIX A	AI
APPENDIX B	AII

INTRODUCTION

The motivations for security in cellular telecommunications systems are to secure conversations and signaling data from interception as well as to prevent cellular telephone fraud.

The modern digital telecommunication systems like Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS) provide a set of internationally accepted standards describing a digital system which is intended to cope with society's mobile communications security needs well into the next century, the GSM includes methods for data transmission, allowing a user to roam between countries and still use the facility. This dissertation addresses the concern that such a system can be used to record the whereabouts of a user and to monitor the transmitted data.

This thesis aims to explain the security methods which are implemented in the modern cellular telecommunication systems like GSM or GPRS and then it comes in details to one of the most famous and important algorithm which is the Data Encryption Standard (DES) algorithm and the DES software discusses the development of a Delphi program that allows a user to create simplified DES (S-DES) two keys and encrypt and decrypt binary plaintext.

Chapter 1 is an overview of The Global System for Mobile communications which 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. GSM was designed to be compatible with ISDN services.

Chapter 2 discusses the GSM security techniques, the security model and algorithms were developed in secrecy and were never published. Eventually some of the algorithms and specifications have leaked out.

Chapter 3 is about the GPRS environment, it started with a short overview of GPRS networks architecture, GPRS applications and then the authentication mechanism.

Chapter 4 presents the Data Encryption Standard (DES) algorithm, adopted by the U.S. government in 1977, is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, here the application software developed by Simplified DES for simplicity.

1. BACKGROUND ON GSM

1.1 Overview

This chapter presents background information on GSM (group special mobile or general system for mobile communications), it includes a brief history, the new benefits for this digital system and main elements with their functions of the architecture of the GSM network.

1.2 Brief History of the Cellular Mobile Radio and GSM

The Group Special Mobile was established in 1982 within the European Conference of Post and Telecommunication Administrations (CEPT). A Further important step in the history of GSM as a standard for a digital mobile cellular communications was the signing of a GSM Memorandum of Understanding (MoU) in 1987 in which 18 nations committed themselves to implement cellular networks based on the GSM specifications. In 1991 the first GSM based networks commenced operations.

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. GSM was designed to be compatible with ISDN services.

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 [1].

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 criterias:
- 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.
- 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[2]. In 1990, the first phase 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 table 1.1.

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 operationnal 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 1.2 charts the different mobile cellular systems developed since the commercial launch of cellular systems[3].

Table1.2. 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

1.3 GSM Compared To the Old Analogue-Based Systems

GSM provides enhanced features over older analog-based systems, which are summarized below:

- **Total Mobility:** The subscriber has the advantage of a Pan-European system allowing him to communicate from everywhere and to be called in any area served by a GSM cellular network using the same assigned telephone number, even outside his home location. The calling party does not need to be informed about the called person's location because the GSM networks are responsible for the location tasks. With his personal chipcard he can use a telephone in a rental car, for example, even outside his home location. This mobility feature is preferred by many business people who constantly need to be in touch with their headquarters.

- **High Capacity and Optimal Spectrum Allocation:** The former analog-based cellular networks had to combat capacity problems, particularly in metropolitan areas. Through a more efficient utilization of the assigned frequency bandwidth and smaller cell sizes, the GSM System is capable of serving a greater number of subscribers. The optimal use of the available spectrum is achieved through the application Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), efficient half-rate and full-rate speech coding, and the Gaussian Minimum Shift Keying (GMSK) modulation scheme.
- **Security:** The security methods standardized for the GSM System make it the most secure cellular telecommunications standard currently available. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to-end security. The subscriber's anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling.
- **Services:** The list of services available to GSM subscribers typically includes the following: voice communication, facsimile, voice mail, short message transmission, data transmission and supplemental services such as call forwarding.

1.4 Architecture of the GSM Network

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers.

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements[3].

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 1.1.

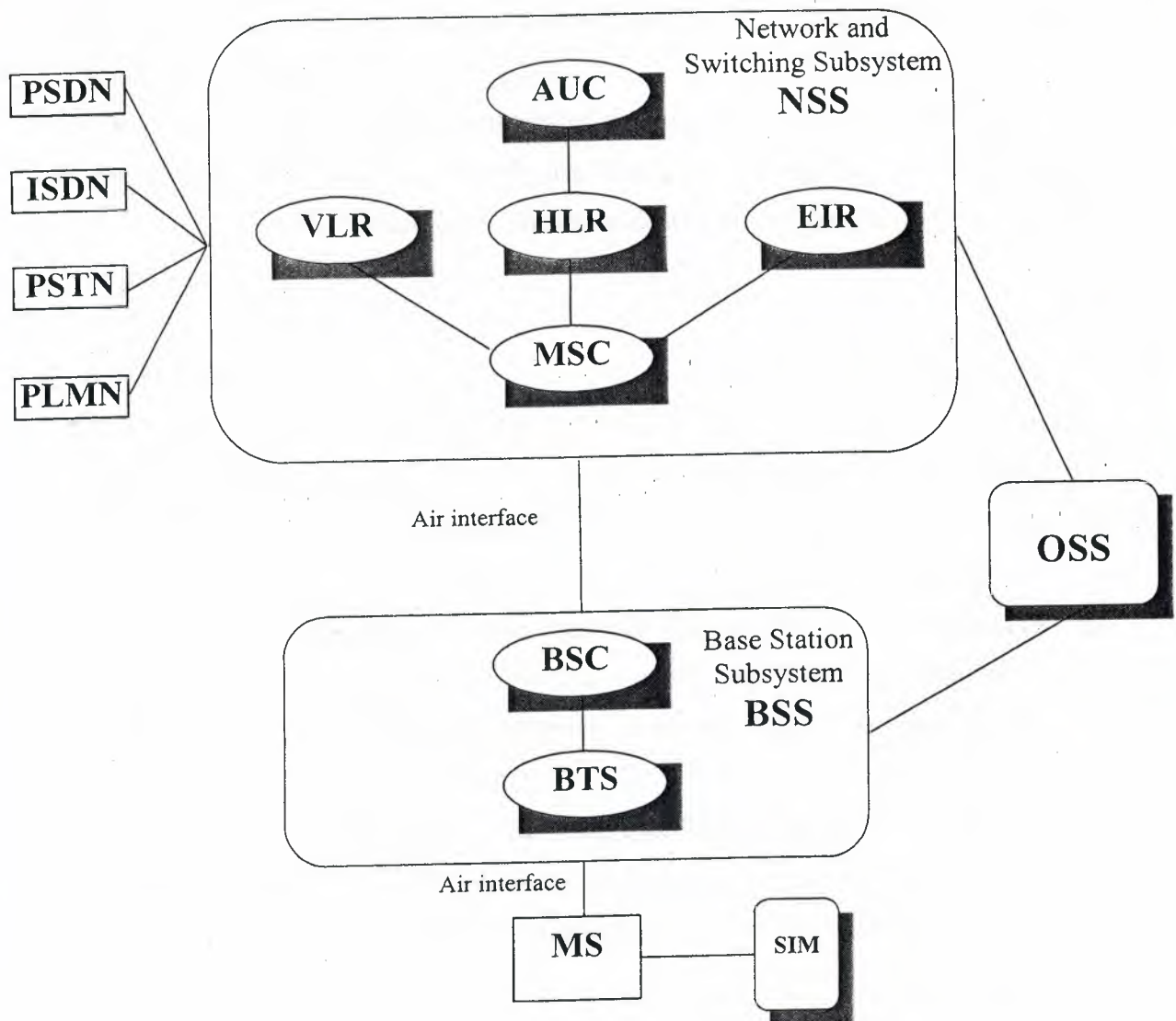


Figure 1.1. Architecture of the GSM network

1.4.1 Mobile Station

A Mobile Station consists of two main elements:

1. The mobile equipment or terminal.

2. The Subscriber Identity Module (SIM).

- **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 handhelds terminals have experienced the biggest success thanks to their 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.

- **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.

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

- **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.

- **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.

1.4.3 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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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).

- **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.

- **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.

1.4.4 Additional Functional Elements

Other functional elements in Switching Subsystem (NSS) are as follows:

- **Message Center (MXE)**—The MXE is a node that provides integrated voice, fax, and data messaging. Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, e-mail, and notification.
- **Mobile Service Node (MSN)**—The MSN is the node that handles the mobile intelligent network (IN) services.
- **Gateway Mobile Services Switching Center (GMSC)**—A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC.
- **GSM Interworking Unit (GIWU)**—The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GIWU, users can alternate between speech and data during the same call. The GIWU hardware equipment is physically located at the MSC/VLR[4].

1.5 GSM Radio Channel

The GSM standard specifies the frequency bands of 890 to 915 MHz for the uplink band, and 935 to 960 MHz for the downlink band, with each band divided up into 200 kHz channels. Other features of the radio channel interface include adaptive time alignment, GMSK modulation, discontinuous transmission and reception, and slow frequency hopping. Adaptive time alignment enables the MS to correct its transmit timeslot for propagation delay. GMSK modulation provides the spectral efficiency and low out-of-band interference required in the GSM system. Discontinuous transmission and reception refers to the MS powering down during idle periods and serves the dual

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 1.3 illustrates the structure of the normal burst.

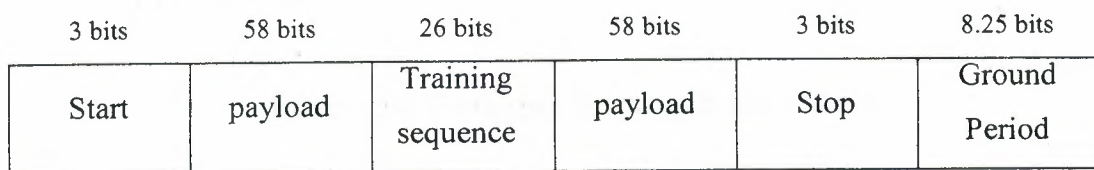


Figure 1.3. Normal Burst Structure

1.6 From Source Information to Radio Waves

The figure 1.4 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa.

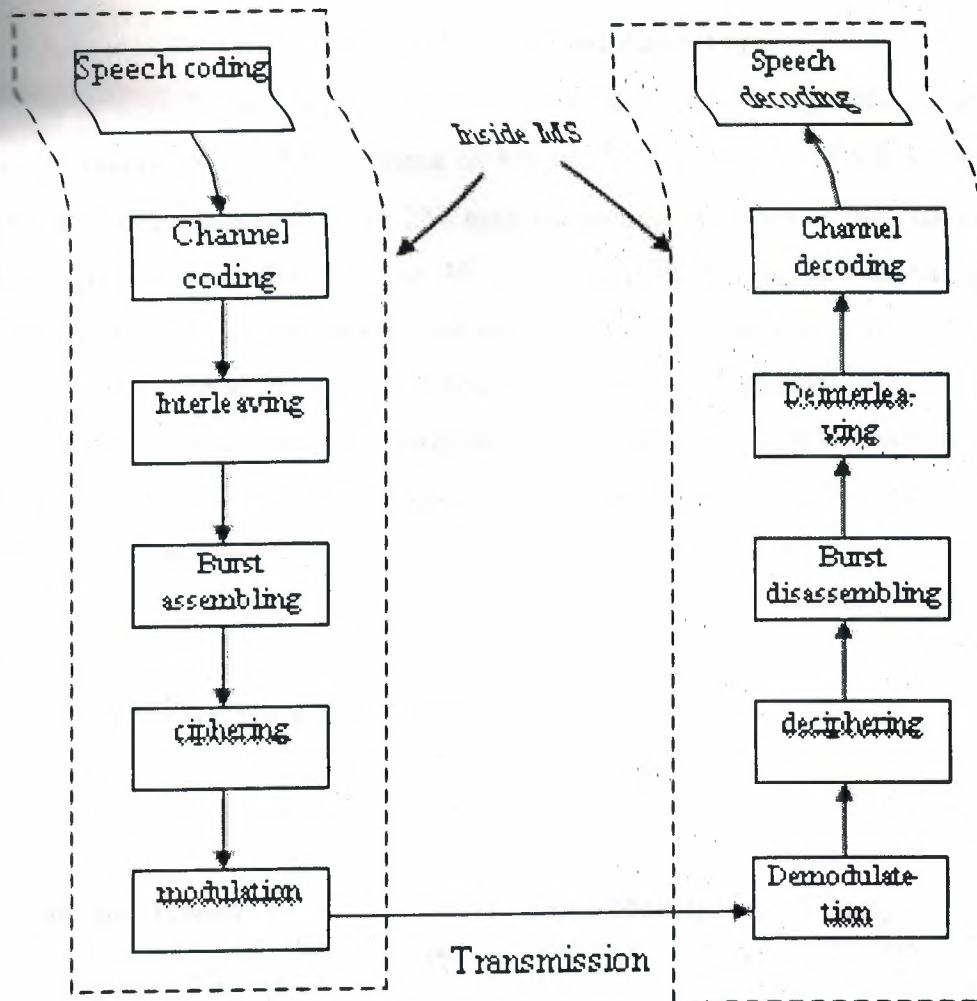


Figure 1.4. From speech source to radio waves

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

1.6.1 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 criterias:

- 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.

1.5.1 TDMA Frame Structures, Channel Types, and Burst Types

The 200 kHz channels in each band are further subdivided into $577 \mu\text{s}$ timeslots, with 8 timeslots comprising a TDMA frame of 4.6 ms. Either 26 or 51 TDMA frames are grouped into multiframes (120 or 234 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 superframe (6.12 s). A hyperframe is composed of 2048 superframes, 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 hyperframe. Figure 1.2 illustrates the various TDMA frame structures[5].

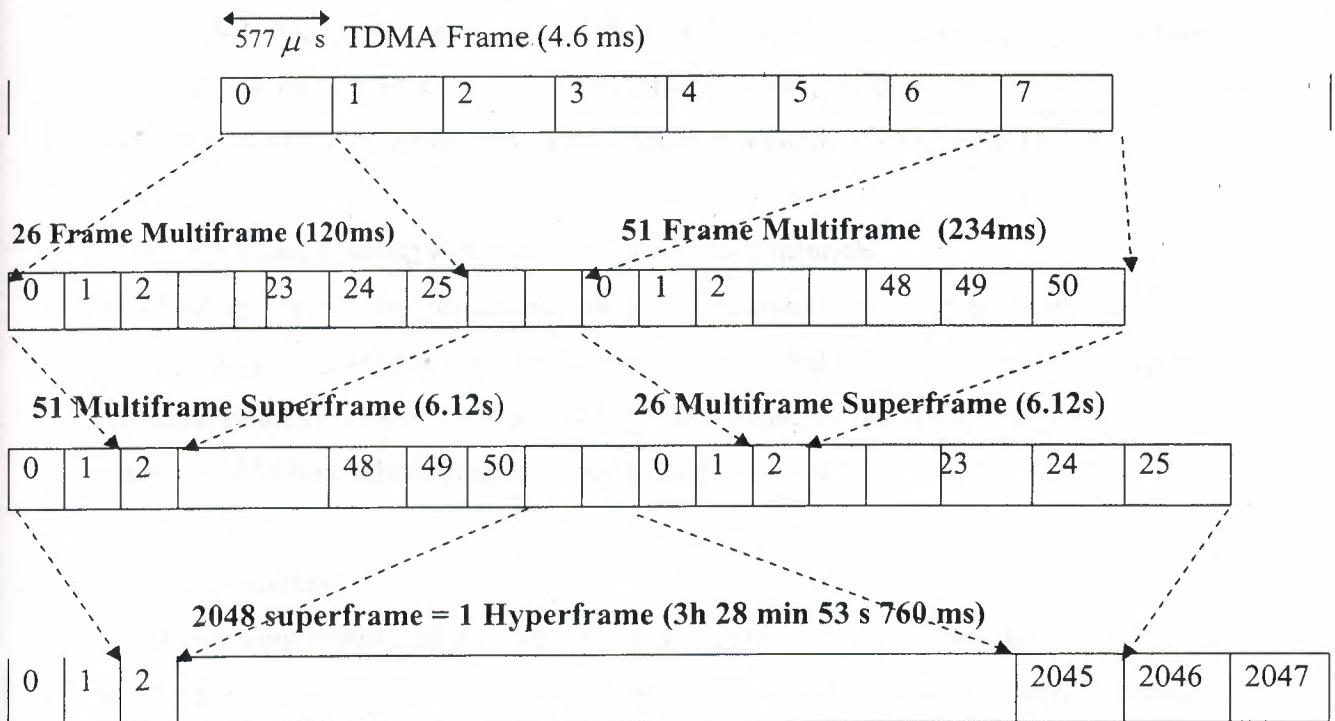


Figure 1.2. TDMA Frame Structures

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.

$C(11 + 15j)$ for $j = 0, 1, \dots, 31$

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

- **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.

- **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.

1.6.3 Interleaving

An interleaving rearranges a group of bits in a particular way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors. Being the errors less concentrated, it is then easier to correct them.

- **Interleaving For The GSM Control Channels**

A burst in GSM transmits two blocks of 57 data bits each. Therefore the 456 bits corresponding to the output of the channel coder fit into four bursts ($4 \times 114 = 456$). The

456 bits are divided into eight blocks of 57 bits. The first block of 57 bits contains the bit numbers (0, 8, 16,448), the second one the bit numbers (1, 9, 17,449), etc.

The last block of 57 bits will then contain the bit numbers (7, 15,455). The first four blocks of 57 bits are placed in the even-numbered bits of four bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the same four bursts. Therefore the interleaving depth of the GSM interleaving for control channels is four and a new data block starts every four bursts. The interleaver for control channels is called a block rectangular interleaver.

- **Interleaving For The GSM Speech Channels**

The block of 456 bits, obtained after the channel coding, is then divided in eight blocks of 57 bits in the same way as it is explained in the previous paragraph. But these eight blocks of 57 bits are distributed differently. The first four blocks of 57 bits are placed in the even-numbered bits of four consecutive bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the next four bursts. The interleaving depth of the GSM interleaving for speech channels is then eight. A new data block also starts every four bursts. The interleaver for speech channels is called a block diagonal interleaver.

- **Interleaving for the GSM data TCH channels**

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of 456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way :

- the first and the twenty-second bursts carry one block of 6 bits each
- the second and the twenty-first bursts carry one block of 12 bits each
- the third and the twentieth bursts carry one block of 18 bits each
- from the fourth to the nineteenth burst, a block of 24 bits is placed in each burst

A burst will then carry information from five or six consecutive data blocks. The data blocks are said to be interleaved diagonally. A new data block starts every four bursts[6].

1.6.5 Ciphering

Ciphering is used to protect signaling and user data. First of all, a ciphering key is computed using the algorithm A8 stored on the SIM card, the subscriber key and a random number delivered by the network (this random number is the same as the one used for the authentication procedure). Secondly, a 114 bit sequence is produced using the ciphering key, an algorithm called A5 and the burst numbers. This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst.

In order to decipher correctly, the receiver has to use the same algorithm A5 for the deciphering procedure.

1.6.6 Modulation

The modulation chosen for the GSM system is the Gaussian Modulation Shift Keying (GMSK).

The aim of this section is not to describe precisely the GMSK modulation as it is too long and it implies the presentation of too many mathematical concepts. Therefore, only brief aspects of the GMSK modulation are presented in this section.

The GMSK modulation has been chosen as a compromise between spectrum efficiency, complexity and low spurious radiations (that reduce the possibilities of adjacent channel interference). The GMSK modulation has a rate of 270 5/6 kbauds and a BT product equal to 0.3. Figure 1.5 presents the principle of a GMSK modulator.

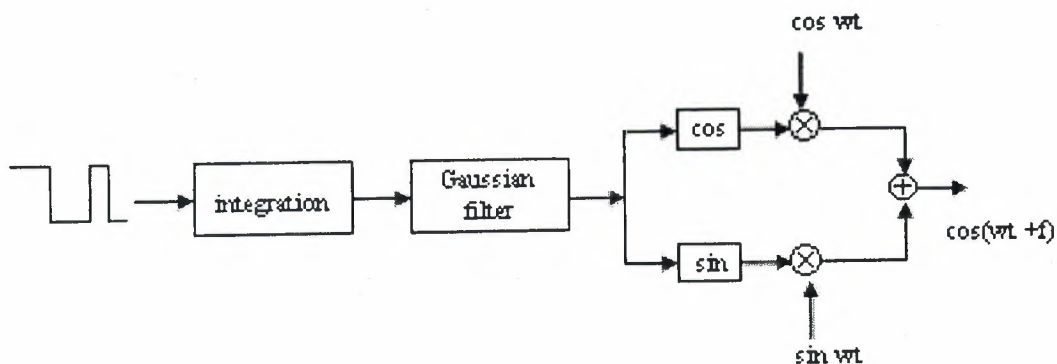


Figure 1.5. GMSK modulator

1.7 Summary

The aim of this chapter was to give the main features of the GSM system and not to provide a complete and exhaustive guide.

The chapter presented a brief history of this system and the function of each part of the system.

As it was shown inside the chapter, GSM is a very complex standard. It can be considered as the first serious attempt to fulfill the requirements for a universal personal communication system. GSM is then used as a basis for the development of the Universal Mobile Telecommunication System (UMTS).

2. GSM AUTHENTICATION AND ENCRYPTION

2.1 Overview

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. Eventually some of the algorithms and specifications have leaked out.

This chapter presents the security processes used in GSM including authentication and encryption algorithms like (A3, A5, A8 and COMP128) and the Possible Interception Attacks to GSM.

2.2 The Purpose for Security

All frauds result in a loss to the operator. It is important to recognize that this loss may be in terms of:

- Not direct financial loss, where the result is lost customers and increase in use of the system with no revenue.
- Direct financial loss, where money is paid out to others, such as other networks, carriers and operators of 'Value Added Networks' such as Premium Rate service lines.
- Potential embarrassment, where customers may move to another service because of the lack of security.
- Failure to meet legal and regulatory requirements, such as License conditions, Companies Acts or Data Protection Legislation [7].

The objective of security for GSM system is to make the system as secure as the Public Switched Telephone Network (PSTN). The use of radio at the transmission media allows a number of potential threats from eavesdropping the transmissions. It was soon apparent in the threat analysis that the weakest part of the system was the radio path, as this can be easily intercepted.

The GSM Group produces guidance on these areas of operator interaction for members. The technical features for security are only a small part of the security requirements; the

greatest threat is from simpler attacks such as disclosure of the encryption keys, insecure billing systems or corruption! A balance is required to ensure that these security processes meet these requirements [7].

At the same time a judgment must be made of the cost and effectiveness of the security measures.

2.3 Limitations of Security

Existing cellular systems have a number of potential weaknesses that were considered in the security requirements for GSM [8].

The security for GSM has to be appropriate for the system operator and customer:

1. The operators of the system wish to ensure that they could issue bills to the right people, and that the services cannot be compromised.
2. The customer requires some privacy against traffic being overheard.

2.3.1 The Countermeasures Are Designed:

1. To make the radio path as secure as the fixed network which implies anonymity and confidentiality to protect against eavesdropping.
2. To have strong authentication, to protect the operator against billing fraud;
3. To prevent operators from compromising each others' security, whether inadvertently or because of competitive pressures.

2.3.2 The Security Processes Must Not:

1. Significantly add to the delay of the initial call set up or subsequent communication;
2. Increase the bandwidth of the channel,
3. Allow for increased error rates, or error propagation;
4. Add excessive complexity to the rest of the system,
5. Must be cost effective.

The designs of an operator's GSM system must take into account the environment and have secure procedures such as:

1. The generation and distribution of keys,
2. Exchange of information between operators,
3. The confidentiality of the algorithms.

2.4 Descriptions of the Functions of the Services

The security services provided by GSM are:

- **Anonymity** So that it is not easy to identify the user of the system.
- **Authentication** So the operator knows who is using the system for billing purposes.
- **Signaling Protection** So that sensitive information on the signaling channel, such as telephone numbers, is protected over the radio path.
- **User Data Protection** So that user data passing over the radio path is protected.

2.4.1 Anonymity

Anonymity is provided by using temporary identifiers. When a user first switches on his radio set, the real identity is used, and a temporary identifier is then issued. From then on the temporary identifier is used. Only by tracking the user it is possible to determine the temporary identity being used.

2.4.2 Authentication

Authentication is used to identify the user (or holder of a Smart Card) to the network operator. It uses a technique that can be described as a "Challenge and Response", based on encryption.

Authentication is performed by a challenge and response mechanism. A random challenge is issued to the mobile, the mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, the response to the challenge is correct.

Eavesdropping the radio channel reveals no useful information, as the next time a new random challenge will be used. Authentication can be provided using this process. A random number is generated by the network and sent to the mobile. The mobile use the

Random number R as the input (Plaintext) to the encryption, and, using a secret key unique to the mobile K_i , transforms this into a response Signed REsponse (SRES) (Ciphertext) which is sent back to the network.

The network can check that the mobile really has the secret key by performing the same SRES process and comparing the responses with what it receives from the mobile [9].

2.4.3 User Data and Signaling Protection

The response is then passed through an algorithm A8 by both the mobile and the network to derive the key K_c used for encrypting the signaling and messages to provide privacy (A5 series algorithms).

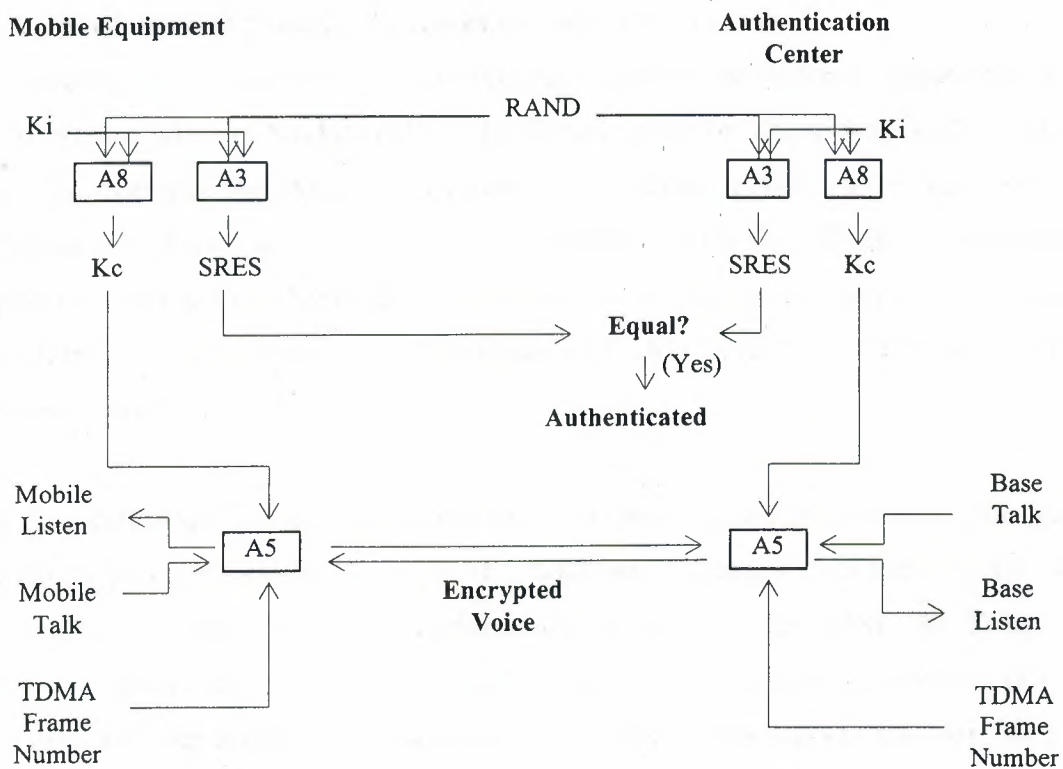


Figure 2.1. Encryption for GSM

2.5 Implementation and Roaming

The authentication algorithm A3 is an operator option, and is implemented within the smart card (known as the Subscriber Interface Module or SIM). So that the operators may inter-work without revealing the authentication algorithms and mobile keys (K_i) to

each other, GSM allows triplets of challenges (R), responses (SRES) and communication keys (Kc) to be sent between operators over the connecting networks.

The A5 series algorithms are contained within the mobile equipment, as they have to be sufficiently fast and are therefore hardware. There are two defined algorithms used in GSM known as A5/1 and A5/2. The enhanced Phase 1 specifications developed by ETSI allows for inter-working between mobiles containing A5/1, A5/2 and unencrypted networks. These algorithms can all be built using a few thousand transistors, and usually takes a small area of a chip within the mobile [10].

2.6 Introductions to the GSM Security Model

2.6.1 Distribution of Security Features In the GSM Network

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, 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 2.2 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

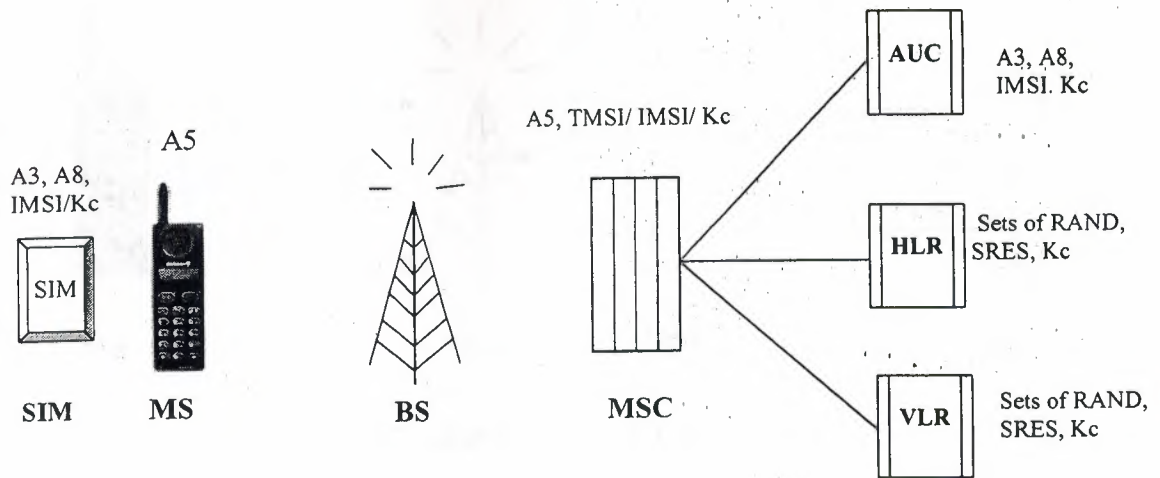


Figure 2.2. Distribution of Security Features in the GSM Network

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 [12].

The GSM Security Model is based on a shared secret between the subscriber's home network's HLR and the subscriber's SIM. The shared secret, called Ki, is a 128-bit key used to generate a 32-bit signed response, called SRES, to a Random Challenge, called RAND, made by the MSC, and a 64-bit session key, called Kc, used for the encryption of the over-the-air channel. 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 are 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.

When the MS 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. Figure 2.3.

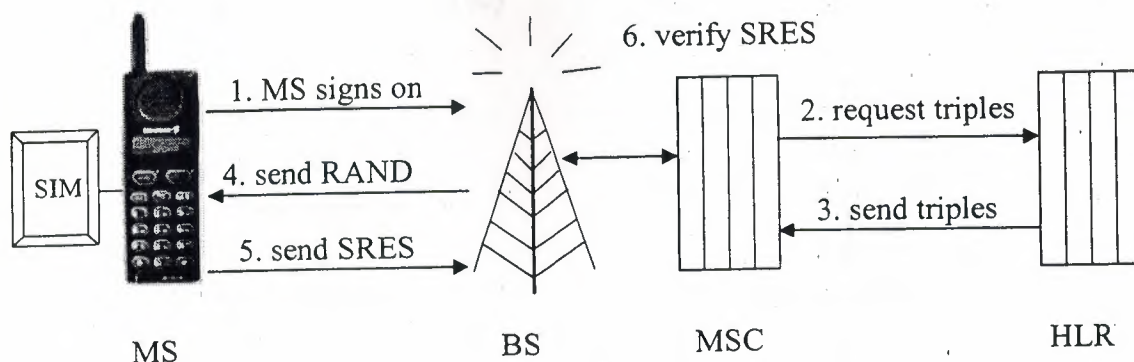


Figure 2.3. Mobile station authentication

The MS then generates a Session Key, K_c , with the A8 algorithm using, again, the Challenge from the MSC and the K_i from the SIM. The BTS, which is used to communicate with the MS, receives the same K_c 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 [12].

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 K_c 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 K_c and the frame numbers. The frame numbers are generated implicitly, which means that anybody can find out the frame number at hand. The same K_c is used as long as the MSC does not authenticate the MS again, in which case a new K_c is generated. In practice, the same K_c 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 K_c is not changed during calls. Figure 2.4.

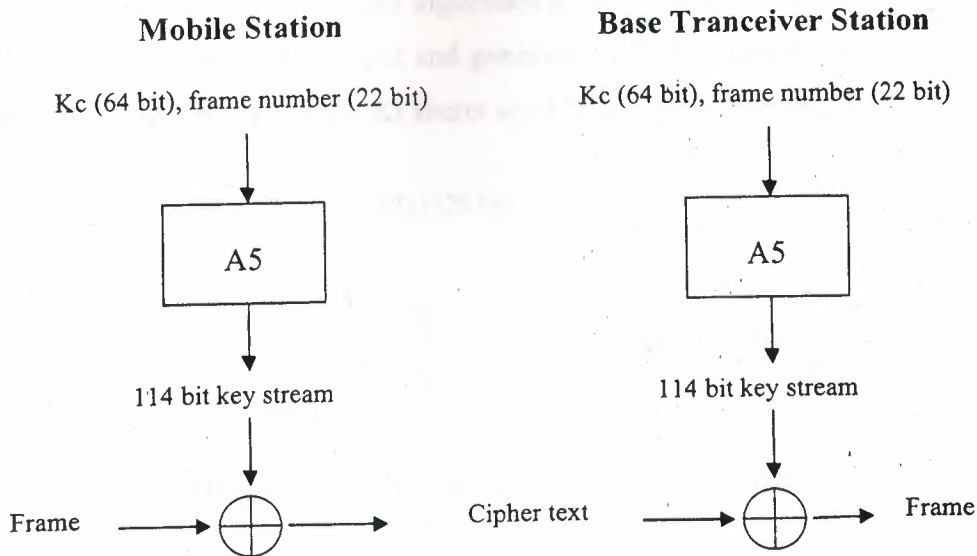


Figure 2.4. Frame encryption and decryption

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 send them in plaintext to the operator's backbone network.

2.6.2 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 K_i from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the K_i secret are 128 bits long. Figure 2.5 [12].

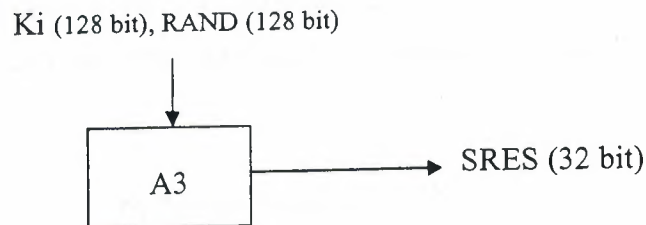


Figure 2.5. Signed response (SRES) calculation

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

has received from the HLR. The A3 algorithm gets the RAND from the MSC and the secret key K_i from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the K_i secret are 128 bits long. Figure 2.5 [12].

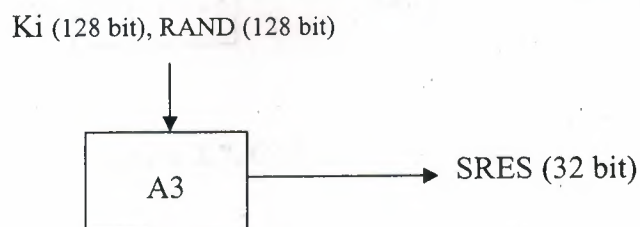


Figure 2.5. Signed response (SRES) calculation

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. Figure 2.7.

The COMP128 takes the RAND and the K_i 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.

2.6.3 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, K_c , from the random challenge, RAND, received from the MSC and from the secret key K_i . 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 K_c . See Figure 2.6. The BTS received the same K_c from the MSC. HLR was able to generate the K_c , because the HLR knows both the RAND (the HLR generated it) and the secret key K_i , which it holds for all the GSM subscribers of this network operator. One session key, K_c , is used until the MSC decides to authenticate the MS again. This might take days [14].

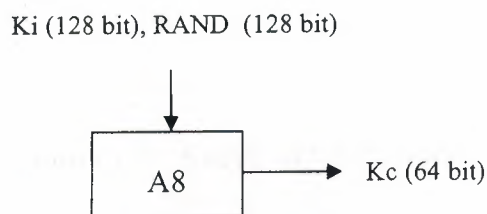


Figure 2.6. Session key (K_c) calculation

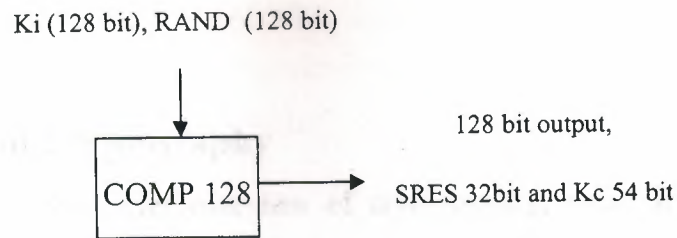


Figure 2.7. COMP128 calculation

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.

2.6.4 A5/1, the Strong Over-the-Air Voice-Privacy Algorithm

The A5 algorithm is the stream cipher used to encrypt over-the-air transmissions. 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 2.8 [14].

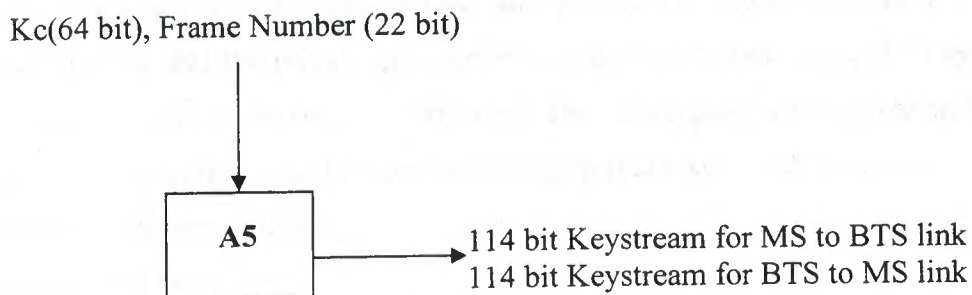


Figure 2.8. Keystream generation

2.7. Overview of Cryptography

This section provides a brief overview of cryptography, with an emphasis on the features that appear in the GSM system.

2.7.1 Symmetric Algorithms

Symmetric algorithms are algorithms in which the encryption and decryption use the same key. For example, if the plaintext is denoted by the variable P , the ciphertext by C , the encryption with key x by the function $E_x()$, and the decryption with key x by $D_x()$, then the symmetric algorithms are functionally described as follows:

$$C = E_x(P)$$

$$P = D_x(C)$$

$$P = D_x(E_x(P))$$

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. The most widely-known example of a symmetric algorithm is the Data Encryption Standard (DES). Symmetric encryption algorithms may be further divided into block ciphers and stream ciphers [15].

2.7.4 Public Key Algorithms

Public key algorithms are characterized by two keys, a public and private key, which perform complementary functions. Public and private keys exist in pairs and ideally have the property that the private key may not be deduced from the public key, which allows the public key to be openly distributed. Data encrypted with a given public key may only be decrypted with the corresponding private key, and vice versa. This is functionally expressed as follows:

$$C = E_{\text{pub}}(P), P = D_{\text{priv}}(C)$$

$$C = E_{\text{priv}}(P), P = D_{\text{pub}}(C)$$

Public key cryptography simplifies the problem of key management in that two parties may exchange encrypted data without having exchanged any sensitive key information. Digital Signatures also make use of public key cryptography, and commonly consist of the output of a one-way hash function for a message (discussed in Section 2.3) with a private key. This enables security features such as authentication and non-repudiation.

The most common example of a public key algorithm is RSA, named after its inventors Rivest, Shamir, and Adleman. The security features of GSM, however, do not make use of any type of public key cryptography [15].

2.8 Possible Interception Attacks

The algorithms have been studied since and critical errors have been found. Thus, after a closer look at the GSM standard, one can see that the security model is not all that good. An attacker can go through the security model or even around it, and attack other parts of a GSM network, instead of the actual phone call. Although the GSM standard was supposed to prevent phone cloning and over-the-air eavesdropping, both of these are possible with little additional work compared to the analog mobile phone systems and can be implemented through various attacks. One should not send anything confidential over a GSM network without additional encryption if the data is supposed to stay confidential.

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.

Scientists around the world seem 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 [19].

2.8.1 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 keyspace 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.

2.8.2 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 clockings 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} [18].

However, J. Golic has proposed 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.

Golic also proposed 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 LFSRs at a known time for a known keystream sequence corresponding to a known frame number, thus reconstructing the session key, K_c .

2.8.3 Accessing the Signalling 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 operators 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 K_c . 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 K_c 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 [19].

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 Kc for all the subscribers of that particular operator. The possibilities are countless and real.

2.8.4 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 chapter. 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, K_i , 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 K_i 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, K_c , 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.

2.8.5 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

suspicious, 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 reconstruct 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.

2.8.6 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 chapter.

2.8.7 Cracking the A8 Algorithm

Another possibility is that someone will be able to crack the A8 key generation algorithm and retrieve the secret key, K_i , based on the random challenge, RAND, the session key, K_c , 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 K_i 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 K_c can be relatively easily deduced from the encrypted frames and the known plain text given enough time.

A 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.

2.9 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 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.

2.9 Summary

This chapter presented the security mechanisms specified in the GSM standard which made it the most secure cellular telecommunications system available. The use of authentication, encryption, and temporary identification numbers by (A3, A5, A8 and COMP128) algorithms used ensures the privacy and anonymity of the system's users, as well as safeguarding the system against fraudulent use. GSM systems with these security measures is much more secure than previous analog systems.

3. AUTHENTICATION AND SECURITY IN GPRS ENVIRONMENT

3.1 Overview

This chapter presents the security measures applied in General Packet Radio Service (GPRS), it began with giving a short introduction to GPRS and the function of each part followed by GPRS Applications. After this overview for this system the chapter presented Security measures applied between GPRS Networks.

3.2 Short Introduction to GPRS

GPRS is a new technique for mobile networks, like GSM, which provides high-speed packet switched data service. In the future the most important application of the GPRS is probably mobile access to the private and public IP networks (e.g., Internet, video telephoning).

Since GPRS operates with different kind of networks security functions are vital for secure data transmission over GPRS. GPRS has quite good user authentication mechanism.

Wireless mobile communication has gained more and more popularity lately. Nowadays people move a lot and they want to have the same communication facilities with them as at home or in the office and mobile phones are very handy for this purpose. During the last decade mobile phones have been used mainly for speech communication and data communication has not gained much popularity. Mobile data has been used mainly by the white collar workers such as professionals, managerial staff, and sales people. In the private sector the only widely used mobile data application has been the GSM short message service (SMS) [20].

Users have perceived need for mobile data. However, the technology used at the moment is not powerful enough to serve these needs. In the near future two new techniques are introduced to the GSM network: High Speed Circuit Switched Data (HSCSD) and General Packet Radio Service (GPRS). HSCSD offers high data rate circuit switched connections (up to 115.2 kbit/s) while GPRS offers high data rate

packet switched connections (up to 172.8 kbit/s). None of the techniques itself will be the killer application which make mobile data communication popular. Merely, they provide transmission services for a killer application with mobility as a value added service. The killer application may be a secure, high-speed access to the Internet.

GPRS can be seen as an access networks to other network which offers mobility as an value added service. It offers possibility that traveling employees can communicate with corporate LAN very easily even from abroad. To be able to use GPRS for transmitting confidential or private data the system must offer authentication and security functions. GPRS offers ciphering function over the radio network as well as authentication to the GPRS network.

The first section of this chapter considers security issues of the GPRS. GPRS operates with other networks, secure and insecure, public and private. Therefore, security of data transmission is very important. Additionally, GPRS users are not located at the same place all the time making user authentication even more important and difficult than in fixed networks [20].

Before considering security issues, in the second section, GPRS is introduced shortly. Those parts of the GPRS network that are essential for understanding the rest of this chapter are introduced and Few applications that can be used over the GPRS network are presented for justifying the security issues later on this chapter.

GPRS is developed by European Telecommunication Standards Institute (ETSI). Standardization started in 1993 and the specifications are completed for the Phase 1, but few minor modifications are still expected. One of the main goals in the GPRS design has been to support bursty data transfer and occasional transmission of large amount of data in an economical way. Both of these properties are very common for current data transmission applications.

Although GPRS is considered as a GSM service, it has its own core network and the radio network is shared between the GPRS and GSM core networks. The GPRS core network is attached to the GSM radio network via an open interface. Additionally, GSM may utilize the GPRS core network to achieve more efficient performance and the GPRS user may use some of the GSM supplementary services. However, it is possible

to build a GPRS network which is not attached to any GSM network. In that case the GPRS network needs its own radio network.

3.2.1 GPRS Network Architecture

Figure 3.1 illustrates structure of a combined GPRS/GSM network. The important network elements for this chapter are described shortly and the rest of the elements are just mentioned below [21].

MS - Mobile Station. There are three types of GPRS mobile stations: Class A, Class B, and Class C. The Class A mobiles are capable of using the GPRS packet switched and the GSM circuit switched bearer services at the same time. For example, Class A mobile can have a normal GSM voice call and GPRS data transfer going on at the same time. The Class B mobiles are capable of having an attachment to both the GSM and the GPRS networks at the same time. However, they can use only either circuit switched or packet switched service at the time. Among the Class C mobiles the selection between the GSM and the GPRS networks is done manually. Thus the Class C mobiles can be attached either to the GSM or to the GPRS network but not to both at the time.

SGSN - Serving GPRS Support Node. The SGSN is one of the main components of the GPRS network. The main functions of the SGSN are to handle MS registration and authentication into the GPRS network, to manage MS mobility, to relay traffic, and to collect statistics and charging information.

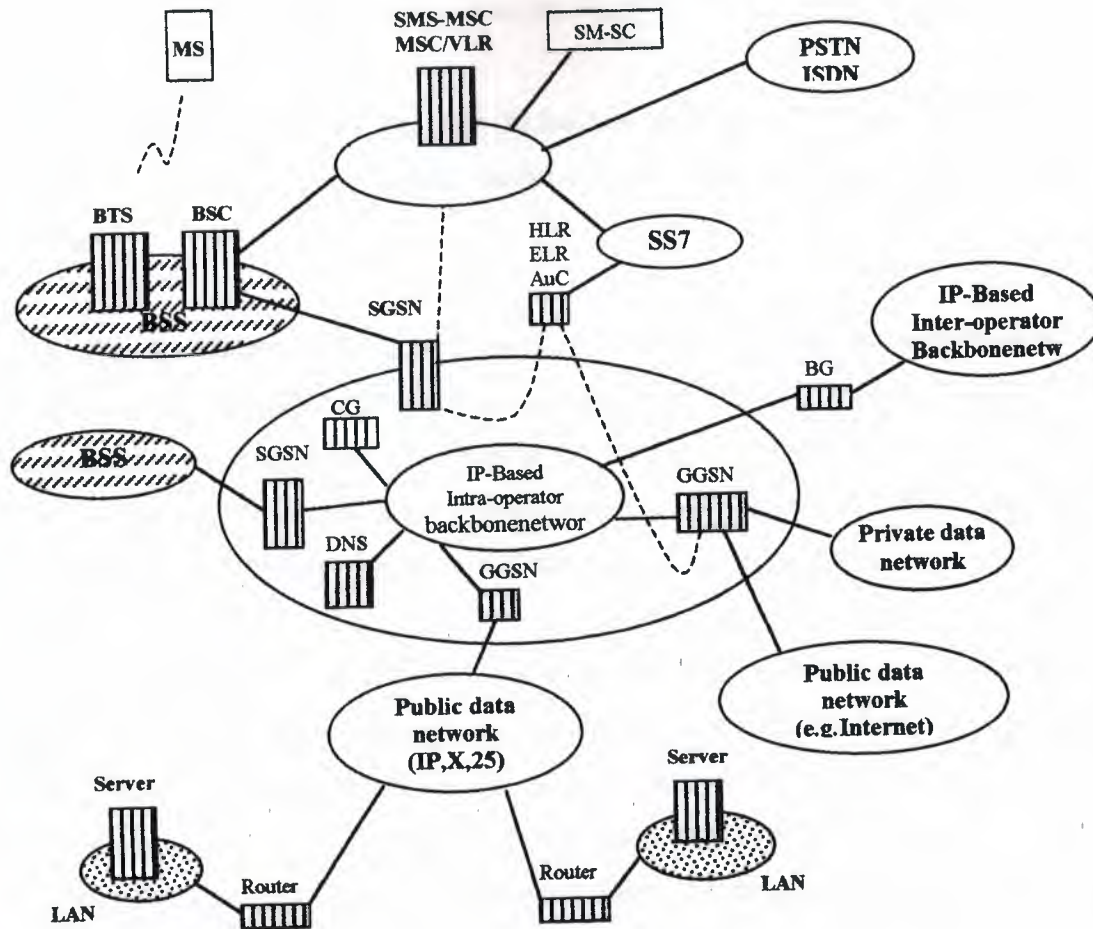


Figure 3.1. Example of GPRS/GSM network.

GGSN - Gateway GPRS Support Node. The GGSN is the interface between the GPRS backbone and external data networks. The functionality of the GGSN is similar to a router in data networks. It routes end user data from external data networks to the SGSN currently serving the destination MS and mobile originated data to the external destination data networks and to the SGSNs.

HLR - Home Location Register. The main function of the HLR is to store MS profiles. It holds information about allowed packet data protocols per MS as well as allowed PDP addresses per protocol. It also holds the same information as the HLR in the bare GSM network.

AuC - Authentication Center. The AuC includes information for identifying authorized users of the GPRS network and for preventing unauthorized use of the network. AuC is often a physical part of the HLR.

EIR - Equipment Identity Register. In the EIR each mobile is listed as in GSM: black list for stolen mobiles, gray list for mobiles under observation, and white list for other mobiles.

BG - Border Gateway. The main function of the BG is to ensure a secure connection between different GPRS networks over the inter-operator backbone network. The functionality of the BG is not defined in the GPRS specifications. It could consist of a firewall, security functions, and routing functions. BGs as well as their functionality are selected by the GPRS operators' mutual agreement to enable roaming.

LIN - Lawful Interception Node. The LIN is used to collect information about some pre-defined subscriber or subscribers. The information could include, e.g., the data sent and received by the interception target, location information, and subscriber information. The lawful interception is an action based on the law which is performed by the GPRS network. The GPRS network has to be able to deliver required user data and other network related information to the Law Enforcement Agency (LEA) whenever wanted.

GPRS backbone networks. The GPRS backbone network can be either intra- or inter-operator network. The main function of the intra-operator backbone network is to connect the GSNs of a single operator. The inter-operator backbone network connects GPRS operators and provides international GPRS roaming. GPRS backbone networks are IP based.

The intra-operator GPRS backbone network is implemented as a set of local area networks (LAN) connected with routers. The transmission media can be Ethernet, FDDI, ATM, Frame Relay etc. In most cases, the intra-operator backbone is a private network to ensure the security and good performance. Private IP addresses can be used in the intra-operator backbone because addresses are not visible outside of the network.

The inter-operator GPRS backbone network can be based on either public (e.g., Internet) or private (dedicated) IP network. They are implemented as a wide area network connecting intra-operator backbone networks using routers. The transmission media used with inter-operator backbones can be PTP links, ATM, Frame Relay etc. It is chosen by the GPRS operators' mutual agreement to enable roaming. All the interconnected GPRS backbone networks comprise one big network and therefore the IP address allocation must be co-ordinated.

3.3 GPRS Applications

GPRS supports applications based on two standard data protocols: Internet Protocol (IP) and X.25. This means that the GPRS user can communicate with public or private data network which are supporting those protocols. GPRS also supports specific point-to-point (PTP) and point-to-multipoint (PTM) services as well as transfer of the short messages (SM) over GPRS radio channels [22].

3.3.1 PTP service

The PTP service allows a single user to communicate with another single GPRS user or a server (or user) which is located in an external network. The PTP service can be further divided into connectionless and connection oriented services. In the connectionless service each packet is independent of the preceding and succeeding packet. This service is of the datagram type and is intended to support bursty applications.

IP has a great significance in today's data networks and its significance will increase in the near future. IP is used in the Internet and most of the intranets. GPRS supports IP and it provides mobility as an additional feature when compared to access from fixed networks. For GPRS user the IP over GPRS communication seems to be similar to the IP over fixed network communication. There are two visible differences when compared to the fixed networks. The user has opportunity to change her location and continue communication all the time. Another difference is that the GPRS network service quality is worse than in the fixed network. When the user has an access to the Internet via a fixed network she has access to a number of services such as public data

banks. However, if the access is provided via GPRS, the user has an access to the same services but her location can change during the access.

At the moment the most useful applications received from the Internet for the GPRS user are probably email and access to the WWW. Those users who have an access to the intranet of a company may basically take advantage of all services provided by the intranet. For example, access to the data bases, the use of tool software, or even access to the shared disks. If the company has a group communication software the employees could arrange teleconferences. Companies may achieve remarkable savings by allowing their employees to utilize GPRS services worldwide. Employees can participate much better to the work although they are on business trip. They have also access to the newest information all the time. Based on these examples it can be said that commercial success of GPRS depends quite much on authentication and security mechanisms that can be used.

Connection oriented service provides a logical relation between the users. The duration of the connection may vary from few seconds to several hours. This service is intended to support bursty transactive or interactive applications. GPRS is able to support applications based on the X.25 protocol. X.25 connections over GPRS are not studied further in this chapter, because of its small significance compared to IP.

3.3.2 PTM service

The PTM service allows the user to send data packets from one sender to many recipients. The PTM service won't be available in the GPRS Phase 1 and therefore it is not further studied in this chapter.

3.3.3 SM service

The GPRS users may use the SMS offered by GSM. The maximum length of the short message is 160 characters. The service is able to handle PTP and PTM messages.

3.4 User Authentication and Security inside GPRS Network

3.4.1 Authentication

The user authentication procedures in GPRS are similar to procedures used in GSM. The difference is that the procedures are executed from the SGSN instead of the MSC. Additionally, the authentication procedure performs the selection of the ciphering algorithm and the synchronization for the ciphering. Authentication mechanism uses "authentication triplets" which are received from the HLR and stored into the SGSN. Authentication triplets consists of

- **RAND:** random number between 0 and 2128-1.
- **SRES:** signed response which is result of the A3 algorithm used for subscriber authentication.
- **Kc:** Ciphering key which computed using the A8 algorithm and it is used by the GPRS Encryption Algorithm (GEA).

The subscriber authentication procedure is illustrated in Figure 3.2 and Figure 3.3. If the SGSN does not have previously stored authentication triplets, they are acquired from the HLR by sending message Send Authentication Info. The HLR responds with Send Authentication Info Ack message and now the SGSN has the authentication triplet. When the SGSN has the authentication triplet it sends message Authentication Request including RAND to the MS and the MS computes SRES from RAND and secret Subscriber authentication key Ki.

The MS then sends Authentication Response including SRES to the SGSN and if the SRES computed by the HLR equals to the SRES computed by the MS, the MS is considered to be authenticated to use the network.

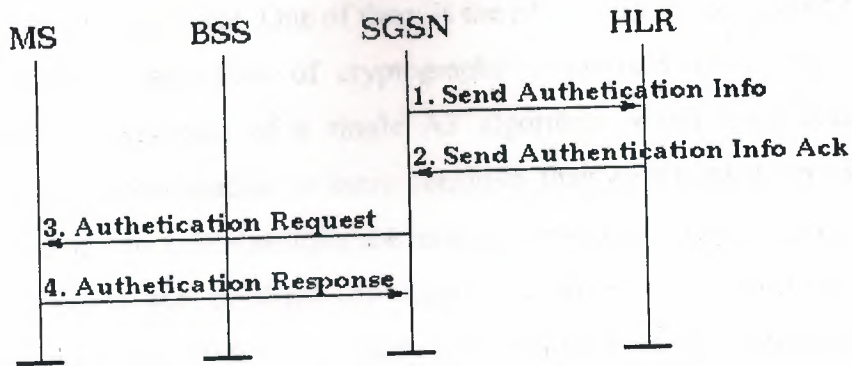


Figure 3.2. GPRS authentication procedure.

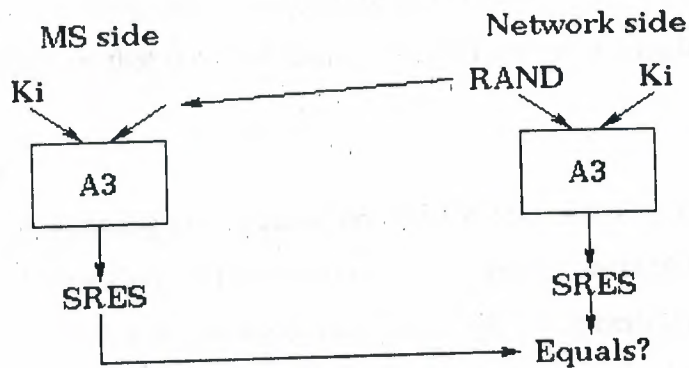


Figure 3.3. Authentication computation.

During authentication procedure the SGSN informs to the MS whether ciphering is used or not. If ciphering is wanted to use the MS starts ciphering after sending Authentication Response message and the SGSN after receiving a valid Authentication Response.

It is important to note that all security functions inside the GPRS network are based on the secrecy of the secret key K_i . It is stored into the SIM (Subscriber Identification Module) card and into the HLR at subscription time and it is not known by the subscriber.

The algorithm A3 used to compute SRES can be operator dependent while allowing full inter-PLMN (public land mobile network) roaming. Operators can therefore choose A3 applicable to their own subscribers. However, ETSI has designed one algorithm and

operators may use it if they want. ETSI's A3 algorithm is secret. Several reasons justify A3 to be operator dependent. One of them is the administrative complexity linked to the specification and distribution of cryptographic algorithms when they are to cross borders. The management of a single A3 algorithm would have been even more complex, since authentication is more sensitive than communication ciphering. The consequences of a broken algorithm are more far-reaching in the case of authentication. Another reason is the existence of algorithms fit for authentication and already implemented on smart cards but possibly not open for sharing. A limiting factor being the smart card memory capacity, the choice of having an operator-dependent A3 algorithm enables communication operators to use a single algorithm, e.g., SIM and pay-phone access. The GPRS user authentication is relatively good. A problem is copying of SIM which has been reportedly done. With a copied SIM unauthorized user can do many harmful things to the original user. However, copying is still quite difficult to perform and requires that the SIM card is several hours in wrong hands [23].

3.4.2 Ciphering

In GPRS data and signaling during data transfer are ciphered. Ciphering functionality is placed on Logical Link Control (LLC) layer. The ciphering method is GPRS Encryption Algorithm (GEA) which is a secret algorithm. The scope of ciphering in GPRS is from the ciphering function at the SGSN to the ciphering function in the MS in contrast to the GSM ciphering which is a single logical channel between the BTS and MS as illustrated in Figure 3.4.

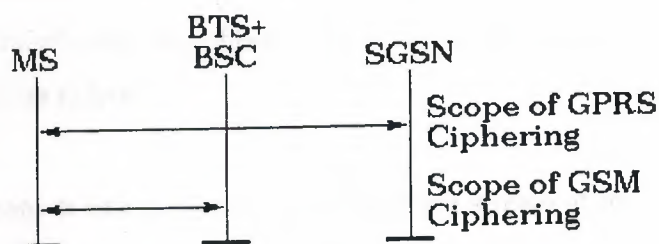


Figure 3.4 Scope of GPRS ciphering.

Mutual key setting is the procedure that allows the MS and the network to agree on the key K_c to use in the ciphering and deciphering algorithms. The K_c is handled by the

SGSN independently from the MSC. If the MS is able to use both GSM and SGSN services then it have two different keys one in the MSC and one in the SGSN.

Key setting is triggered by the authentication procedure, but the network may initiate key setting as often as the operator wishes. Key setting procedure is not encrypted and shall be performed as soon as the identity of the mobile subscriber is known by the network. The transmission of the K_c to the MS is indirect and uses the authentication RAND value. K_c is derived from RAND using algorithm A8 and K_i as illustrated in Figure 3.5 The maximum length of K_c is only 64 bits. After computation the key is stored by the MS until it is updated at the next key setting.

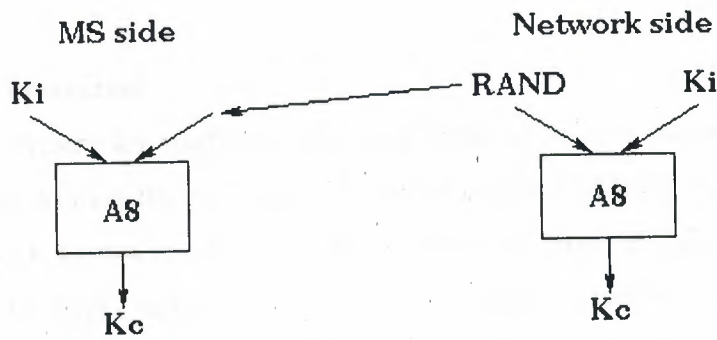


Figure 3.5 K_c computation.

The MS and the SGSN must co-ordinate the instants at which the ciphering and deciphering processes start. The authentication procedure governs the start of ciphering as explained in Section 3.4.1. Once the encryption has been started neither the MS or the SGSN shall go to an unciphered session. During ciphered session only few signaling messages may be transferred unciphered and if any other messages are transferred unciphered they shall be deleted.

The enciphering stream at one end and the deciphering stream at the other end must be synchronized, for enciphering bit stream and the deciphering bit streams to coincidence. Synchronization is guaranteed by driving the GEA by explicit variables INPUT and DIRECTION. INPUT is the sequence number of the LLC packet and its initial value is selected by the network. DIRECTION is either from the MS to the network or from the network to the MS allowing INPUT to be identical in both directions. The output of the

GEA is exclusive or'd with the clear text at the sending end and with the ciphered text at the receiving end. Figure 3.6 illustrates GPRS ciphering process.

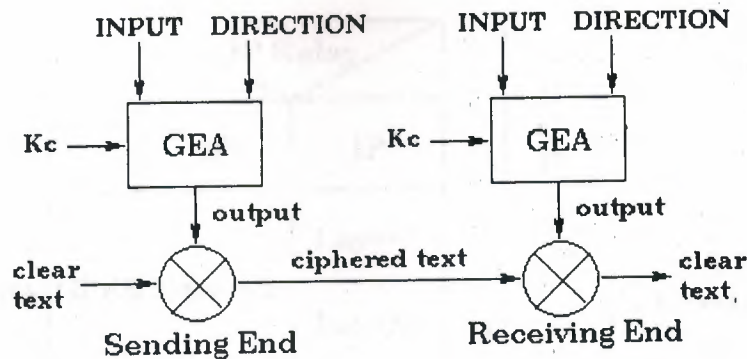


Figure 3.6. Ciphering process.

3.4.3. Identity Protection

Encryption is efficient for confidentiality, but it cannot be used to protect every single message exchanged over the radio path. As stated earlier ciphering with K_c applies only when the network knows the identity of the subscriber. Before ciphering is started the user identity is kept secret from outsiders using temporary user identification parameters. Without temporary identification parameters a third-party could listen users identity and know where she roams at the particular moment. That is considered harmful for user's privacy.

3.5 Secure GPRS Interworking with Packet Data Network

As stated earlier GPRS supports interworking with packet data networks (PDN) and more specifically with IP. These interworked IP networks may be either the Internet or intranets. GPRS is able to operate with IPv4 and in the future with IPv6. Figure 3.7 illustrates the Gi reference point and protocol stack needed for GPRS interworking with IP networks.

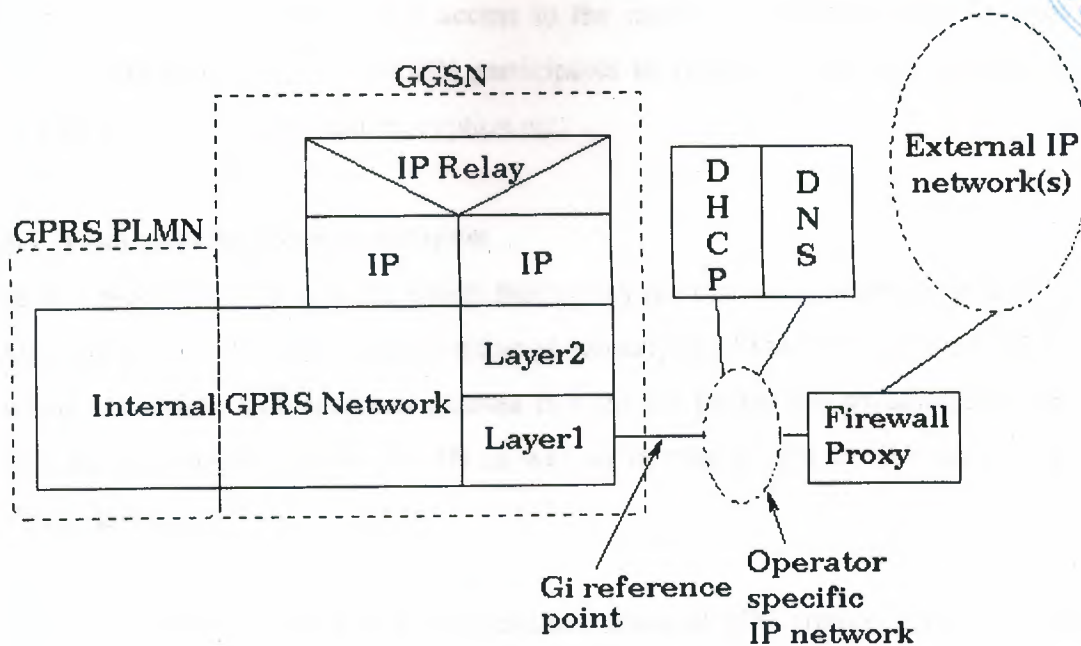


Figure 3.7. Gi reference point for GPRS with IP interworking.

The Gi reference point is located between the GGSN and the external IP network. From the viewpoint of the external IP network, the GGSN is seen as a normal IP router. The Layer1 and Layer2 protocols are negotiated between the GPRS and external IP network operators.

Between the GGSN and the external IP network the following assumptions are valid in generic case:

A firewall is configured by the GPRS operator. Basically, all applications based on IP are supported but the GPRS operator may restrict their usage. Also, in the most cases it is necessary to restrict access from the external IP networks to the GPRS network.

A domain name server is managed by the GPRS operator or it can be managed by the operator of the external IP network operator.

The GGSN may allocate dynamic PDP addresses by itself or use an external device such as an dynamic host configuration protocol (DHCP) server which can be operated, e.g., by the external IP network operator.

For access to the external IP networks GPRS offers either direct transparent access to the Internet, or a non-transparent access to the intranets or Internet Service Provider (ISP). In the latter case, the GGSN participates to functions like user authentication, user authorization, end-to-end encryption etc.

3.5.1. Transparent Access to Internet

The MS receives an IP address which belongs to the operator's addressing space. This address is a public IP address given either at subscription time (static address) or at PDP context activation. The received address is used for packet transmission between the nodes of the Internet and the GGSN as well as to map packet for the correct internal GPRS addresses.

The MS need not to send any authentication request at PDP context activation and the GGSN need not to participate in the user authentication, authorization, or encryption processes. Thus, the GPRS facilities are not used to preserve privacy and transferring of the confidential information is unsafe. However, special intranet protocols, such as IPSec, can be used allowing the GPRS user to communicate over all insecure public networks securely. User authentication and encryption are left on responsibility of the "intranet protocol" if they are at all needed. Figure 3.8 illustrates this. An "intranet protocol", IPSec, is introduced in section 3.7.

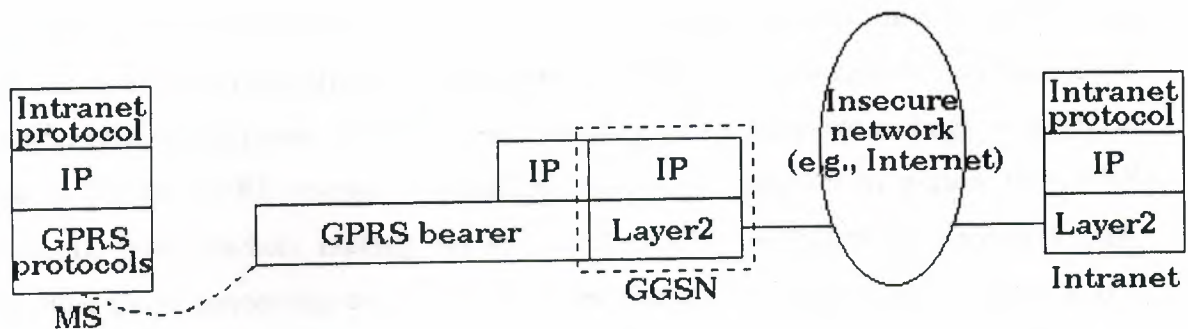


Figure 3.8 GPRS transparent access.

3.5.2 Non-transparent Access to Intranet or ISP

The MS receives an IP address which belongs to the address space of the intranet or ISP. This address is a public IP address given either at subscription time (static address)

or at PDP context activation (dynamic address). The received address is used for packet transmission between the intranet or ISP, and the GGSN as well as to map packet for the correct internal GPRS addresses. This requires a link between the GGSN and an address allocation server of the intranet or ISP. This server may be based on, e.g., Radius or DHCP.

When non-transparent access is used the MS transmits an authentication request at PDP context activation and the GGSN requests user authentication from the same server as the IP address was acquired. Also protocol configuration options are retrieved from that server. Necessary information for authentication comes from user in PDP context activation messages.

The connection between the GPRS network and ISP can be arranged over any network, even an insecure such as the Internet. The connection be a dedicated link or a special secured tunnel arranged using some security protocol (e.g., IPSec). The type of connection is selected by mutual agreement between the GPRS operator and the ISP administrator.

3.5.3 Threats from External Networks

If the GPRS network is attached to an insecure public network several threats may appear from that network. This section lists few of them.

Inside the GPRS network all information, such as subscriber information and routing tables, is in clear text format and not protected in any way. Subscriber information is confidential information. Also incorrect routing tables may cause huge economical losses for the GPRS operator. Therefore, it is very important to protect the GPRS network from crackers making firewall (and GGSN) configuration very important. Another threat concerning configuration of the firewall is denial of service attacks. If a cracker is able to deny service of GGSN (or any other network element) financial losses for the operator are probably enormous. Also, inside GPRS network a cracker would be able to send GPRS signaling messages and thus affecting behavior of the GPRS network and connections.

A cracker could also cause huge bills for a GPRS user. In GPRS the billing will be based on the amount of the transferred data. Therefore, it may be possible to cause harm

for a GPRS user by sending large spam emails (GPRS user also pays received data) from the external network or to create a virus (located in the user's laptop) which could send dummy packets from the MS without the user even knowing it.

3.6 Secure Interworking Between GPRS Networks

The interworking between GPRS operators enables roaming, i.e., the GPRS user is able to access from other operators' GPRS networks (Visited PLMN) to the Home PLMN. Figure 3.9 illustrates interworking between two GPRS operators. GPRS networks are connected to each other via inter-operator backbone network as mentioned in Section 3.2.1. The inter-PLMN link may be any packet data network (1) (e.g., the Internet) or dedicated link (2). Dedicated link may be chosen to fulfill QoS requirements and to improve security. All data and signaling between the GPRS operators are transmitted via BGs. GPRS operators may support IPSec and accompanying specifications for authentication and encryption as a basic set of security functionality in its BGs. However, other security protocols may be selected by a bilateral agreement between the GPRS operators.

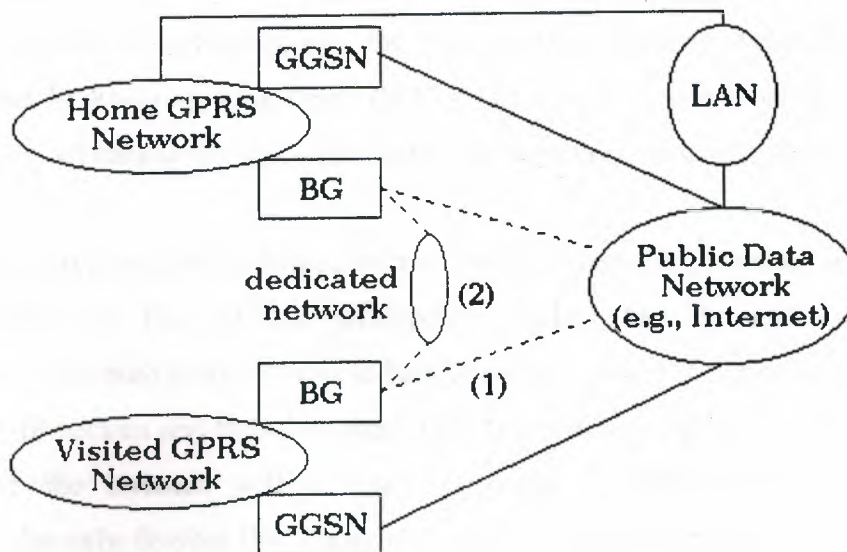


Figure 3.9 Interworking between GPRS networks.

When the user is roaming in the VPLMN data can be routed to its destination (LAN in this case) in several ways. The actual routing depends on bilateral agreements between the GPRS operators and agreements between the HPLMN operator and the user.

If the user has static IP address then data is always routed via HPLMN because the IP address points to the GGSN of the HPLMN. If the user has dynamic IP address then data can be routed via the HPLMN or directly to the LAN via the Internet depending on the agreements mentioned above. Administrators must be very careful when planning LAN protection. The employees should have access to the LAN perhaps from varying IP addresses but on the other hand, unauthorized users should have no access.

In the case of roaming, RAND for the MS and the both SRES and Kc for the network are acquired and calculated in the AuC of the HPLMN. This allows authentication to be successful even the A3 algorithm is operator dependent. Also, in this way the key Ki is kept secret all the time.

3.7. IPSec

As already stated in section 3.5, IPSec can be used to create secure connection from an user's MS to a LAN of a company. This section gives an overview to IPSec and is mainly based on references . Other sources are mentioned separately.

IPSec consists of several open standards and its purpose is to ensure secure private communication over IP networks, e.g., the Internet. It is based on standards developed by the Internet Engineering Task Force (IETF). IPSec ensures confidentiality, integrity, and authenticity of data communications across an insecure, public IP network.

IPSec offers encryption and authentication on network layer. It provides an end-to-end security solution in the network architecture itself. Thus the end systems and applications do not need to know how to handle security issues. Encrypted packets look like ordinary IP packets and thus they can be easily routed through any IP network, such as GPRS or the Internet, without the intermediate network nodes know about encryption. The only devices that know about the encryption are the end points. This feature greatly reduces both implementation and management costs.

IPSec defines a new set of headers to be added to IP datagrams and they provide information for securing the payload of the IP packet as follows:

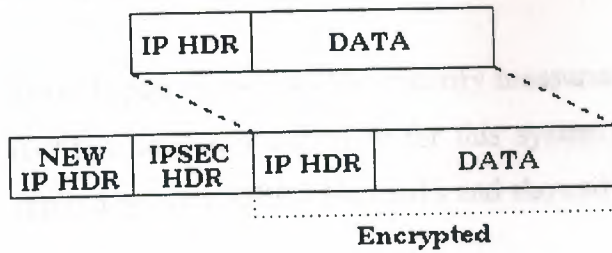
Authentication header (AH). When this header is placed to an IP datagram, the integrity and authenticity of the data are ensured, including the invariant fields in the outer IP header. Confidentiality of data is not protected. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is too slow and would greatly reduce network throughput.

Encapsulating security payload (ESP). When this header is placed to an IP datagram, the confidentiality, integrity, and authenticity of the data protected. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.

Figure 3.10 illustrates IPSec operation modes: transport and tunnel modes. In transport mode, only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. This capability allows enabling special processing (e.g., quality of service) in the intermediate network based on the information in the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis.

In tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPSec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to enjoy the benefits of IP Security. Tunnel mode also protects against traffic analysis; with tunnel mode an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

Tunnel Mode



Transport Mode

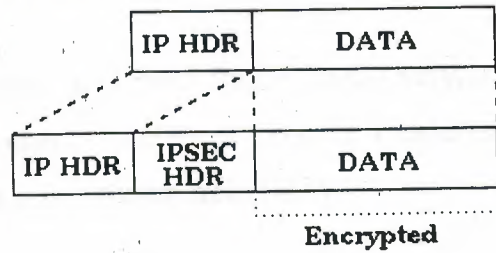


Figure 3.10 IPsec tunnel and transport modes.

As defined by the IETF, IPsec transport mode can only be used when both the source and the destination systems understand IPsec. In most cases IPsec is used in tunnel mode allowing the implementation of the IPsec in the network architecture without modifying the operating system or any applications on PCs, servers, and hosts. This is also the situation with GPRS.

3.9 system evaluation

because if the authentication is not trustful lots of damage may be caused. However, authentication does not work against copying of SIM. If it can be copied then unauthorized user may use the identity of the authorized user until the subscription is invalidated.

The security of the transmitted data cannot be kept cryptographically excellent. Because the GEA is secret it cannot be well evaluated. Most probably, if the algorithm is compromised, the transferred data can be deciphered relatively easily. Also the key length, 64 bits, is too short nowadays. Another thing is that transmission is ciphered only between the SGSN and the MS. This makes lawful interception very easy which can be seen to hurt user's privacy.

Because data between the MS and corporate LAN is almost always transmitted over insecure networks, the GPRS security functions are not enough. To make transmission secure an external intranet protocol is needed. One solution is to use IPsec. It fits well to the IP world and can be seen safe enough. Most probably it will become de-facto standard and corporates can take advantage from IPsec development. IPsec restricts lawful interception a little bit because contents of the packets are relatively difficult to extract. However, user's location can be still tracked easily.

3.9 Summary

This chapter introduced the security measures applied in General Packet Radio Service (GPRS), after this overview for this system the chapter presented Security measures applied between GPRS Networks and showed how it is different from GSM.

4. CONVENTIONAL ENCRYPTION: MODERN TECHNIQUES

4.1 Overview

The aim of this chapter is to illustrate the principles of modern conventional encryption. It presents one of the most widely used conventional encryption Algorithms: the Data encryption Standard (DES). Although numerous conventional encryption algorithms, have been developed since the introduction of DES, it remains the most important such algorithm. Further, a detailed Study of DES provides an understanding of the principles used in other conventional encryption algorithms.

4.2 Simplified DES

Simplified DES is an educational rather than a secure encryption algorithm. It has similar properties and structure to DES with much smaller parameters. It was developed by Professor Edward Schaefer of Santa Clara University. The reader might find it useful to work through an example by hand while following the discussion in this section, and the application of this algorithm by using of Delphi program is in appendix A and the source code in appendix B.

4.2.1 S-DES Technique

Figure 4.1 illustrates the overall structure of the simplified DES, which we will refer to as S-DES. The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of cipher text as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext.

The encryption algorithm involves five functions: an initial permutation (IP); a complex function labelled f_k , which involves both permutation and substitution operations and depends on a key input; a simple permutation function that switch (SW) the two halves of the data; the function f_k again, and finally a permutation function that

is the inverse of the initial permutation (IP^{-1}), the use of multiple stages of permutation and substitution results in ignore complex algorithm, which increases the difficulty of ryptanalysis [22].

The function f_k , takes as input not only the data passing the rough-the encryption algorithm, but also an 8-bit key. The algorithm could have been designed to work with a 16-bit key, consisting of two 8-bit subkeys, one used for each occurrence of f_k . Alternatively, a single 8-bit key could have been used, with the same key use twice in the algorithm. A compromise is to use a 10-bit key from which two 8-b subkeys are generated, as depicted in Figure 4.1, In this case, the key is first subjected to a permutation (P10). Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an bit output (P8) for the first subkey (K_1). The output of the shift operation also fee into another shift and another instance of P8 to produce the second subkey (K_2).

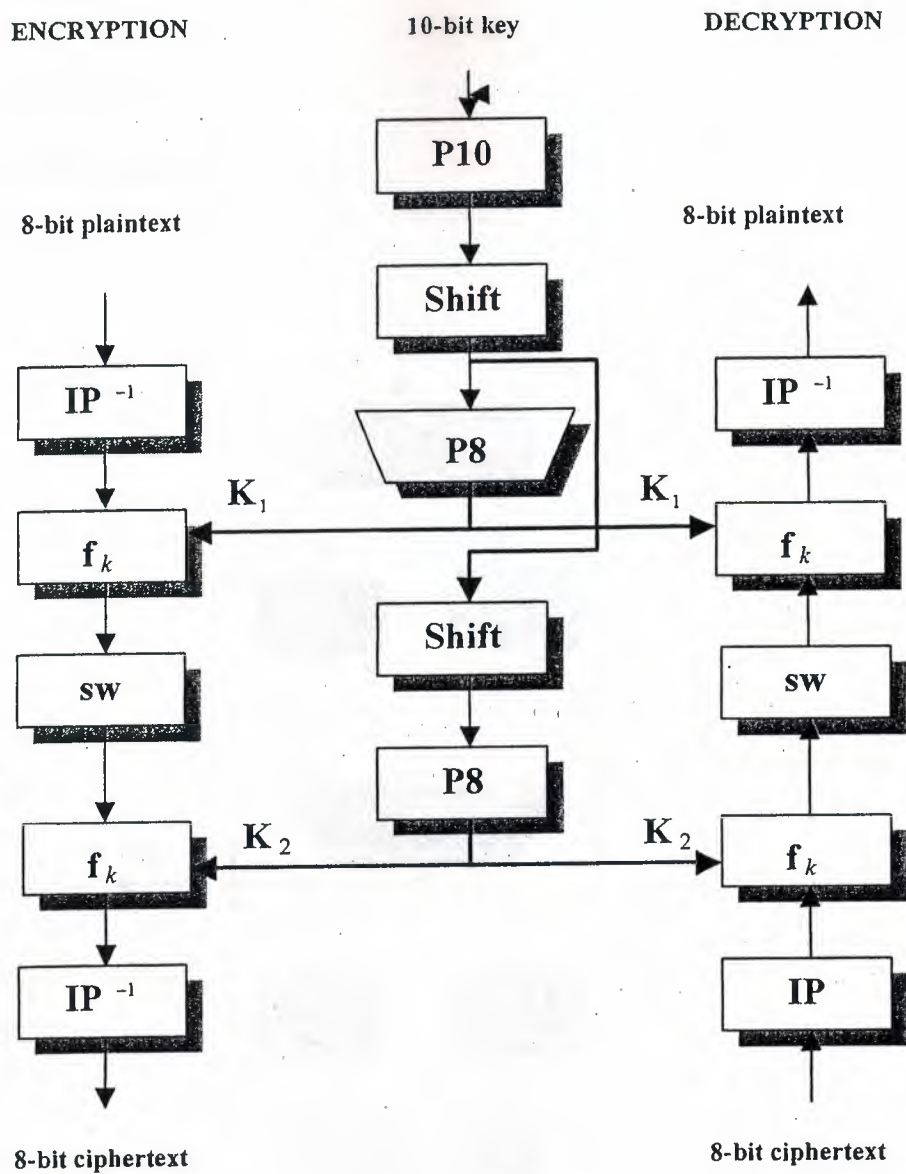


Figure 4.1. Simplified DES Scheme.

We can concisely express the encryption algorithm as a composition of functions: $IP^{-1} \circ f_k \circ SW \circ K_1$

which can also be written as

$$\text{Ciphertext} = \text{IP}^{-1} (f_{k_2} (\text{SW}(f_{k_1} (\text{IP}(\text{plaintext}))))))$$

where

$$K_1 = \text{P8} (\text{Shift} (\text{P10} (\text{key})))$$

$$K_2 = \text{P8} (\text{Shift} (\text{Shift} (\text{P10} (\text{key}))))$$

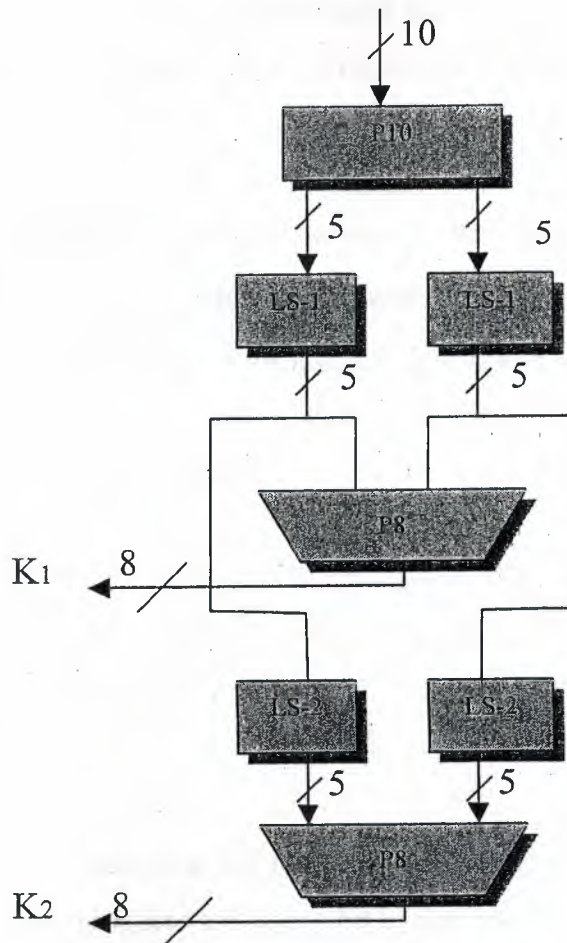


Figure 4.2. Key Generations for Simplified DES.

Decryption is also shown in Figure 4.1 and is essentially the reverse of encryption:

$$\text{plaintext} = \text{IP}^{-1} (f_{k_1} (\text{SW}(f_{k_2} (\text{IP}(\text{ciphertext}))))))$$

We now examine the elements of S-DES in more detail.

4.2.2 S-DES Key Generation

S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit subkeys are produced for use in particular stages of the encryption and decryption algorithm. Figure 4.2 depicts the stages followed to produce the subkeys [23].

First, permute the key in the following fashion. Let the 10-bit key be designated as $(k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10})$. Then the permutation P10 is defined as

$$\text{P10}(k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10}) = (k_3 k_5 k_2 k_7 k_4 k_{10} k_1 k_9 k_8 k_6)$$

P10 can be concisely defined by the display:

P10									
3	5	2	7	4	10	1	9	8	6

This table is read from left to right; each position, in the table gives the identity of the input bit that produces the output bit in that position. So the first output bit is bit 3 of the input; the second output bit is bit 5 of the input, and so on. For example, the key (1010000010) is permuted to (1000001100). Next, perform a circular left shift (LS-1), or rotation, separately on the first five bits and the second five bits. In our example, the result is (0000111000).

Next we apply P8, which picks out and permutes 8 of the 10 bits according to the following rule:

P8							
6	3	7	4	8	5	10	9

The result is subkey 1 (K_1). In our example, this yields (10100100).

We then go back to the pair of 5-bit strings produced by the two LS-1 functions and perform a circular left shift of 2 bit positions on each string. In our example, the value (00001 11000) becomes (00100 00011). Finally, P8 is applied again to produce K_2 . In our example, the result is (01000011).

4.2.3 S-DES Encryption

Figure 4.3 shows the S-DES encryption algorithm in greater detail. As was mentioned, encryption involves the sequential application of five functions. We examine each of these.

- **Initial and Final Permutations**

The input to the algorithm is an 8-bit block of plaintext, which we first permute using the IP function:

IP							
2	6	3	1	4	8	5	7

This retains all 8 bits of the plaintext but mixes them up. At the end of the algorithm, the inverse permutation is used:

IP^{-1}							
4	1	3	5	7	2	8	6

It is easy to show by example that the second permutation is indeed the reverse of the first: that is: $IP^{-1}(IP(X)) = X$

- **The Function f_K**

The most complex component of S-DES is the function f_K , which consists of a combination of permutation and substitution functions. The functions can be expressed as follows. Let L and R be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to f_K and let F be a mapping (not necessarily one-to-one) from 4-bit strings to 4-bit strings. Then we let: $f_K(L, R) = (L \oplus F(R, SK), R)$ where SK is a subkey and \oplus is the bit-by-bit exclusive-OR function. For example, suppose the output of the IP stage in Figure 4.3 is (10111101) and $F(1101, SK) = (1110)$ for some key SK . Then $f_K(10111101) = (01011101)$ because $(1011) \oplus (1110) = (0101)$.

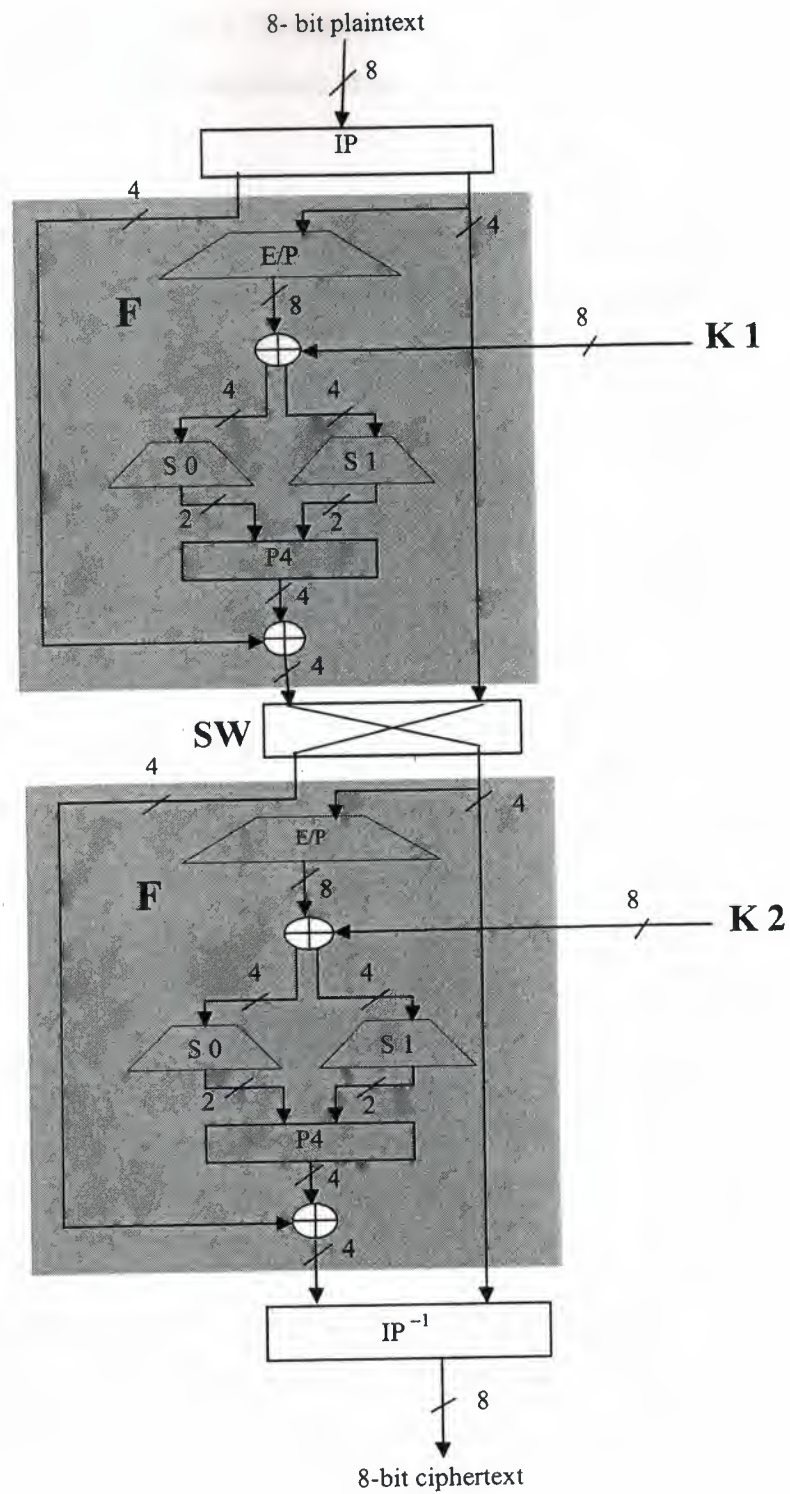


Figure 4.3. Simplified DES Scheme Encryption Detail.

We now describe the mapping F. The input is a 4-bit number $(n_1 n_2 n_3 n_4)$. The first operation is an expansion / permutation operation:

E/P							
4	1	2	3	2	3	4	1

For what follows, it is clearer to depict the result in this fashion:

$$\begin{array}{c|c|c|c} n_4 & n_1 & n_2 & n_3 \\ \hline n_2 & n_3 & n_4 & n_1 \end{array}$$

The 8-bit subkey $k = (k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18})$ is added to this value using exclusive-OR:

$$\begin{array}{c|c|c|c} n_4 + k_{11} & n_1 + k_{12} & n_2 + k_{13} & n_3 + k_{14} \\ \hline n_2 + k_{15} & n_3 + k_{16} & n_4 + k_{17} & n_1 + k_{18} \end{array}$$

Let us rename these 8 bits:

$$\begin{array}{c|c|c|c} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} \\ \hline p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} \end{array}$$

The first four bits (first row of the preceding matrix) are fed into the S-box S0 to produce a 2-bit output, and the remaining 4 bits (second row) are fed into S1 to produce another 2-bit output. These two boxes are defined as follows:

$$S_0 = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{matrix} \end{array}$$

$$S_1 = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{matrix} \end{array}$$

The S-boxes operate as follows: The first and fourth input bits are treated as 2-bit numbers that specify a row of the S-box, and the second and third input bits specify a column of the S-box. The entry in that row and column, in base 2, is the 2-bit output. For example, if $(p_{0,0} p_{0,3}) = (00)$ and $(p_{0,1} p_{0,2}) = (10)$, then the output is from row 0, column 2 of S_0 , which is 3, or (11) in binary. Similarly, $(p_{1,0} p_{1,3})$ and $(p_{1,1} p_{1,2})$ are used to index into a row and column of S_1 to produce an additional 2 bits. Next, the 4 bits produced by S_0 and S_1 undergo a further permutation as follows:

P4			
2	4	3	1

The output of P4 is the output of the function F.

- **The Switch Function**

The function f_K , only alters the leftmost 4 bits of the input. The switch function (SW) interchanges the left and right 4 bits so that the second instance of f_K operates on a different 4 bits. In this second instance, the E/P, S_0 , S_1 , and P4 functions are the same. The key input is K_2 .

- **Analysis of Simplified DES**

A brute-force attack on simplified DES is certainly feasible. With a 10-bit key, there are only $2^{10} = 1024$ possibilities. Given a ciphertext, an attacker can try each possibility and analyze the result to determine if it is reasonable plaintext.

What about cryptanalysis? Let us consider a known plaintext. attack in which a single plaintext $(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8)$ and its ciphertext output $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$ are known and the key $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$ is unknown. Then each c_i is a polynomial function g_i of the p_j 's and k_j 's. We can therefore express the encryption algorithm as 8 nonlinear equations in 10 unknowns. There are a number of possible solutions, but each of these could be calculated and then analyzed. Each of the permutations and additions in the algorithm are linear-maps. The non linearity comes from the S-boxes. It

is useful to write down the equations for these boxes. For clarity, rename $(P_{0,0}, P_{0,1}, P_{0,2}, P_{0,3}) = (a, b, c, d)$ and $(P_{1,0}, P_{1,1}, P_{1,2}, P_{1,3}) = (w, x, y, z)$, and let the 4-bit output be (q, r, s, t) . Then the operation of the SO is defined by the following equations:

$$q = abcd + ab + ac + b + d$$

$$r = abcd + abd + db + ac + ad + a + c + 1$$

where all additions are modulo 2. Similar equations define S1. Alternating linear maps-with these nonlinear maps results in complex polynomial expressions for the ciphertext bits, making cryptanalysis difficult. To visualize the scale of the problem, note that a polynomial equation in 10 unknowns in binary arithmetic can have 2^{10} possible terms. On average, we might therefore expect each of the 8 equations to have 29 terms. The interested reader might try to find these equations with a symbolic processor. Either the reader or the software will give up before much progress is made.

4.2.4 Relationship to DES

DES operates on 64-bit blocks of input. The encryption scheme can be defined as

$$IP^{-1} \circ f_{K_{16}} \circ SW \circ f_{K_{15}} \circ SW \circ \dots \circ SW \circ f_{K_1} \circ IP$$

A 56-bit key is used, from which sixteen 48-bit subkeys are calculated. There is an initial permutation of 56 bits followed by a sequence of shifts and permutations of 48 bits.

Within the encryption algorithm, instead of F acting on 4 bits $(n_1 n_2 n_3 n_4)$, it acts

on 32 bits $(n_1 \dots n_{32})$. After the initial expansion/permutation, the output of 48 bits can be diagrammed as

n_{32}	n_1	n_2	n_3	n_4	n_5
n_4	n_5	n_6	n_7	n_8	n_9
.
.
.
n_{28}	n_{29}	n_{30}	n_{31}	n_{32}	n_1

This matrix is added (exclusive-OR) to a 48-bit subkey. There are 8 rows, corresponding to 8 S-boxes. Each S-box has 4 rows and 16 columns. The first and last bit of a row of the preceding matrix picks out a row-of an S-box, and the middle 4 bits pick out a column.

4.3. Block Cipher. Principles

Virtually all symmetric block encryption algorithms in current use are based on a structure referred to as a feistel block cipher. For that reason, it is important to examine the design principles of the Feistel cipher. We begin with a comparison of stream ciphers and block ciphers. Then we discuss the motivation for the Feistel block cipher structure. Finally, we discuss some of its implications [24].

4.3.1 Stream Ciphers and Block Ciphers

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenere cipher and the Vernam cipher. A block cipher is one in which a block of plaintext is treated as a whole, and used to produce a ciphertext block of equal length. Typically, a block size of 64 bits is used. Using various of the modes of operation explained later in this chapter, a block cipher can be used to achieve the same effect as a stream cipher.

Far more effort has gone into analyzing block ciphers. In general, they seem applicable to a broader range of applications than stream ciphers. The vast majority of network-based conventional cryptographic applications make use of block ciphers. Accordingly, the concern in this chapter, and in our discussions throughout the book of symmetric encryption, will be solely on block ciphers.

4.3.2 Motivation for the Feistel Cipher Structure

A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits. There are 2^n possible different plaintext blocks and, for the encryption to be reversible (i.e., for decryption to be possible), each must produce a unique ciphertext block. Such a transformation is called reversible, or nonsingular. The following examples illustrate nonsingular and singular transformation for $n = 2$.

Reversible Mapping		Irreversible Mapping	
Plaintext	Ciphertext	Plaintext	Ciphertext
00	11	00	11
01	10	01	10
10	00	10	01
11	01	11	01

In the latter case, a ciphertext of 01 could have been produced by one of two plaintext blocks. So if we limit ourselves to reversible mappings, the number of different transformations is $2^n !$.

Figure 4.5 illustrates the logic of a general substitution cipher for $n = 4$. A 4-bit input produces one of 16 possible input states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by 4 ciphertext bits. The encryption and decryption mappings can be defined by a tabulation, as shown in Table 4.1. This is the most general form of block cipher and can be used to define any reversible mapping between plaintext and ciphertext.

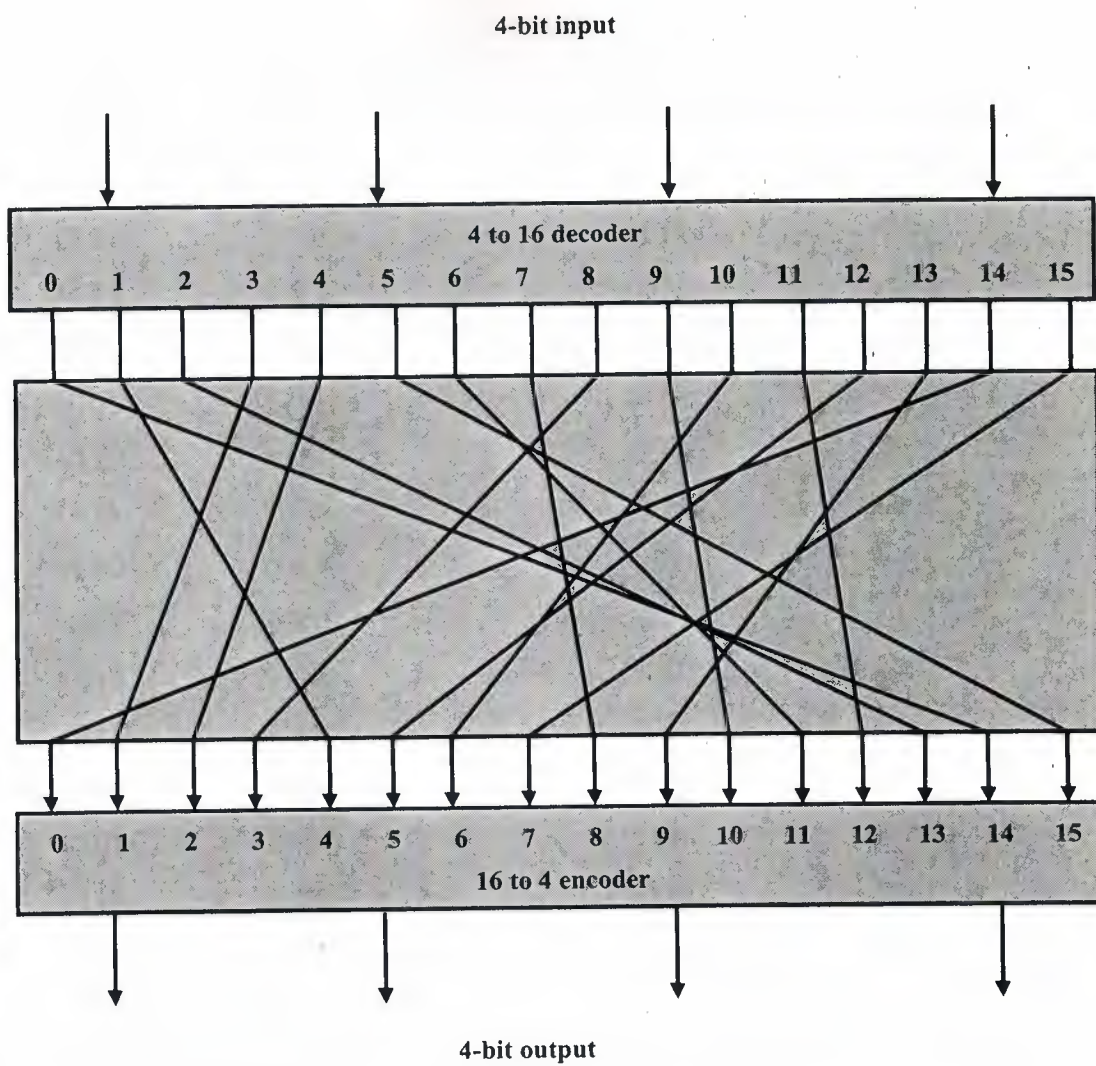


Figure 4.4. General n -bit- n bit block Substitution (shown with $n = 4$)

Table 4.1. Encryption and Decryption Tables for Substitution Cipher of Figure 4.4

Plaintext	Ciphertext	Ciphertext	Plaintext
0000	1110	0000	1110
0001	0100	0001	0011
0010	1101	0010	0100
0011	0001	0011	1000
0100	0010	0100	0001
0101	1111	0101	1100
0110	1011	0110	1010
0111	1000	0111	1111
1000	0011	1000	0111
1001	1010	1001	1101
1010	0110	1010	1001
1011	1100	1011	0110
1100	0101	1100	1011
1101	1001	1101	0010
1110	0000	1110	0000
1111	0111	1111	0101

But there is a practical problem with this approach. If a small block size, such as $n = 4$, is used, then the system is equivalent to a classical substitution cipher. Such systems, as we have seen, are vulnerable to a statistical analysis of the plaintext. This weakness is not inherent in the use of a substitution cipher but rather results from the use of a small block size. If n is large and an arbitrary reversible substitution between plaintext and ciphertext is allowed, then the statistical characteristics of the source plaintext are masked to such an extent that this type of cryptanalysis is infeasible.

An arbitrary reversible substitution cipher for a large block size is not practical, however, from an implementation and performance point of view. For such a transformation, the mapping itself is the key. Consider again Table 4.1, which defines one particular reversible mapping from plaintext to ciphertext for $n = 4$. The mapping

can be defined by the entries in the second column, which show the value of the ciphertext for each plaintext block. This, in essence, is the key that determines the specific mapping from among all possible mappings. In this case, the key requires 64 bits. In general, for an n -bit general substitution block cipher, the size of the key is $n \times 2^n$. For a 64-bit block, which is a desirable length to thwart statistical attacks, the key size is $64 \times 2^{64} = 2^{70} = 2^{10}$ bits.

4.4 The Data Encryption Standard

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

The DES enjoys widespread use. It has also been the subject of much controversy concerning how secure the DES is. To appreciate the nature of the controversy, let us quickly review the history of the DES.

In the late 1960s, IBM set up a research project in computer cryptography led by Horst Feistel. The project concluded in 1971 with the development of an algorithm with the designation LUCIFER [FEIS731], which was sold to Lloyd's of London for use in a cash-dispensing system, also developed by IBM. LUCIFER is a Feistel block cipher that operates on blocks of 64 bits, using a key size of 128 bits. Because of the promising results produced by the LUCIFER project, IBM embarked on an effort to develop a marketable commercial encryption product that ideally could be implemented on a single chip. The effort was headed by Walter Tuchman and Carl Meyer, and it involved not only IBM researchers but also outside consultants and technical advice from NSA. The outcome of this effort was a refined version of LUCIFER that was more resistant to cryptanalysis but that had a reduced key size of 56 bits, to fit on a single chip.

In 1973 the National Bureau of Standards (NBS) issued a request for proposals for a national cipher standard. IBM submitted the results of its Tuchman-Meyer project. This

was by far the best algorithm proposed and was adopted in 1977 as the Data Encryption Standard.

Before its adoption as a standard, the proposed DES was subjected to intense criticism, which has not subsided to this day. Two areas drew the critics' fire. First, the key length in IBM's original LUCIFER algorithm was 128 bits, but that of the proposed system was only 56 bits, an enormous reduction in key size of 72 bits. Critics feared (and still fear) that this key length is too short to withstand brute-force attacks.

The second area of concern was that the design criteria for the internal structure of DES, the S-boxes, were classified. Thus, users could not be sure that the internal structure of DES was free of any hidden weak points that would enable NSA to decipher messages without benefit of the key. Subsequent events, particularly the recent work on differential cryptanalysis, seem to indicate that DES has a very strong internal structure. Furthermore, according to IBM participants, the only changes that were made to the proposal were changes to the S-boxes, suggested by NSA, that removed vulnerabilities identified in the course of the evaluation process.

Whatever the merits of the case, DES has flourished and is widely used, especially in financial applications. In 1994, NIST reaffirmed DES for federal use for another five years; NIST recommends the use of DES for applications other than the protection of classified information. The author feels that, except in areas of extreme sensitivity, the use of DES in commercial applications should not be an immediate cause for concern.

4.4.1 DES Encryption

The overall scheme for DES encryption is illustrated in Figure 4.7. As with any encryption scheme, there are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.

Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an

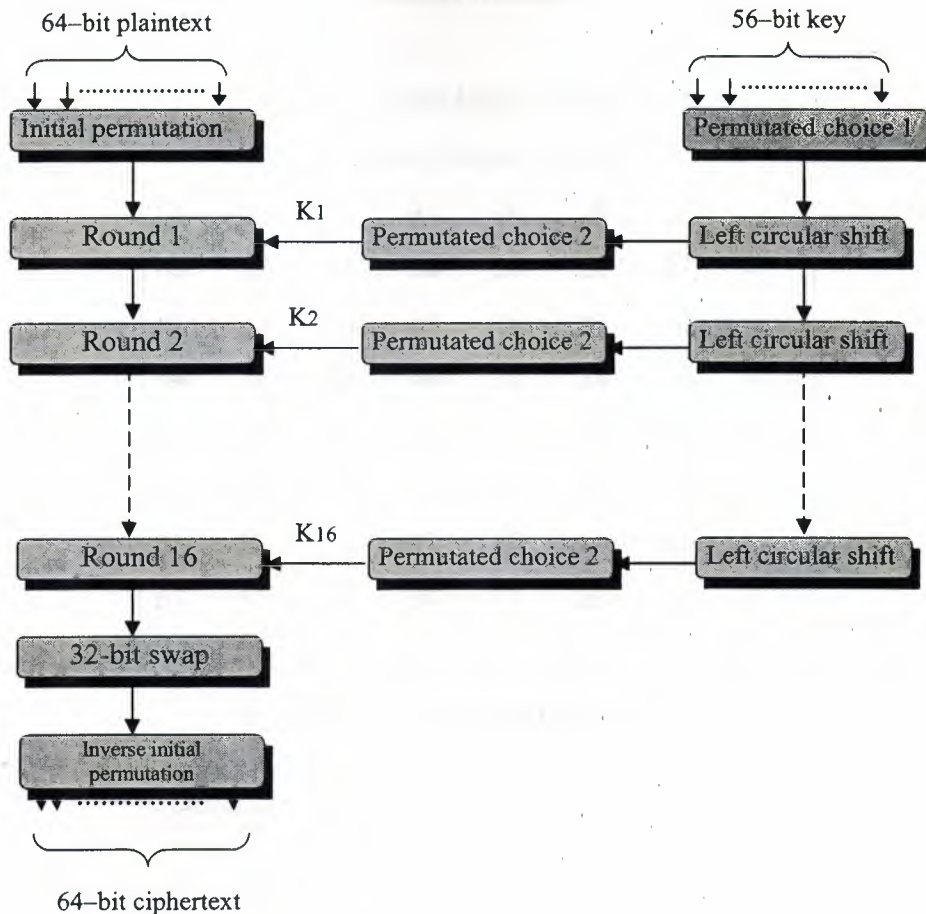


Figure 4.7. General Depiction of DES Encryption Algorithm.

initial permutation (IP) that rearrange the bits to produce the *permuted input*. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput. Finally, the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext. With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher, as shown in Figure 4.5.

The right-hand portion of Figure 4.7 shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the 16 rounds, a subkey (K_i) is produced by the combination of a left circular shift and a

permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated iteration of the key bits.

Table 4.2. Permutation Table for DES

(a) initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
67	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	1	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

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

(c) Expansion Permutation (E)

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

(d) Permutation Function (P)

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

- **Initial Permutation**

The initial permutation and its inverse are defined by tables, as shown in Tables 4.2a and 3.2b, respectively. To see that these two permutation functions are indeed the inverse of each other, consider the following 64-bit input M:

M1	M2	M3	M4	M5	M6	M7	M8
M9	M10	M11	M12	M13	M14	M15	M16
M17	M18	M19	M20	M21	M22	M23	M24
M25	M26	M27	M28	M29	M30	M31	M32
M33	M34	M35	M36	M37	M38	M39	M40
M41	M42	M43	M44	M45	M46	M47	M48
M49	M50	M51	M52	M53	M54	M55	M56
M57	M58	M59	M60	M61	M62	M63	M64

Where M_i is a binary digit . Then the permutation $X = IP(M)$ is as follows:

M58	M50	M42	M34	M26	M18	M10	M2
M60	M52	M44	M36	M28	M20	M12	M4
M62	M54	M46	M38	M30	M22	M14	M6
M64	M56	M48	M40	M32	M24	M16	M8
M57	M49	M41	M33	M25	M17	M9	M1
M59	M51	M43	M35	M27	M19	M11	M3
M61	M53	M45	M37	M29	M21	M13	M5
M63	M55	M47	M39	M31	M23	M15	M7

If we take the inverse permutation $Y = IP^{-1}(X) = IP^{-1}(IP(M))$, it can be seen that the original ordering of the bits restored.

• Details of Single Round

Figure 4.8 shows the internal structure of a single round. Again, begin by focusing on the left-hand side of the diagram. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labelled L (left) and R (right). As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

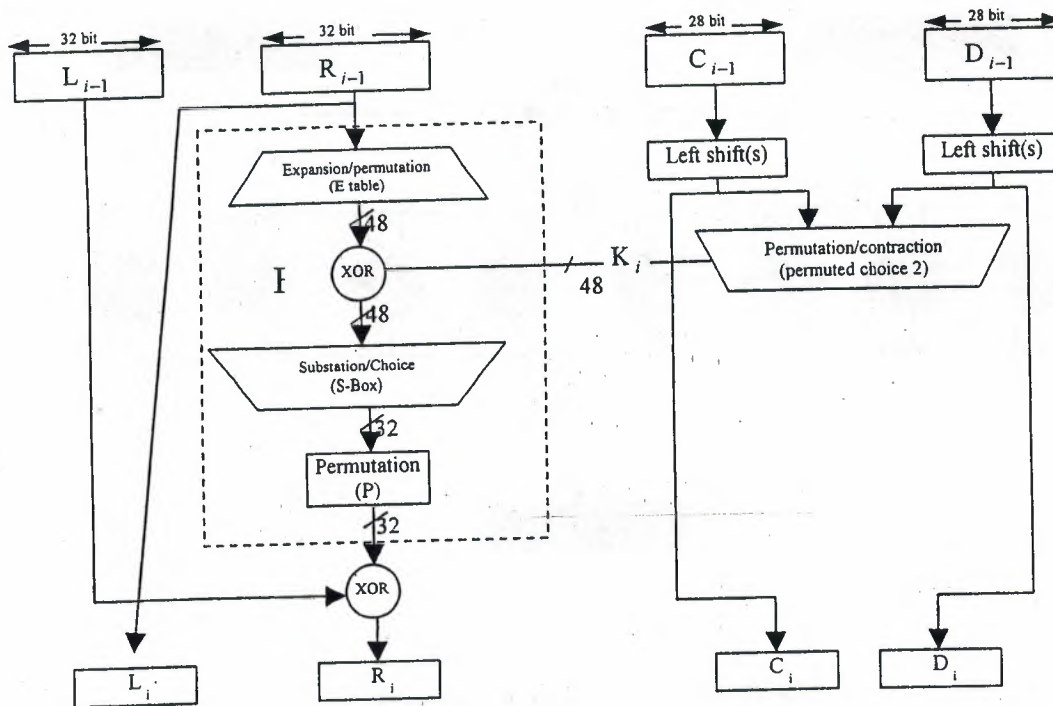


Figure 4.8. Single Round of DES algorithm

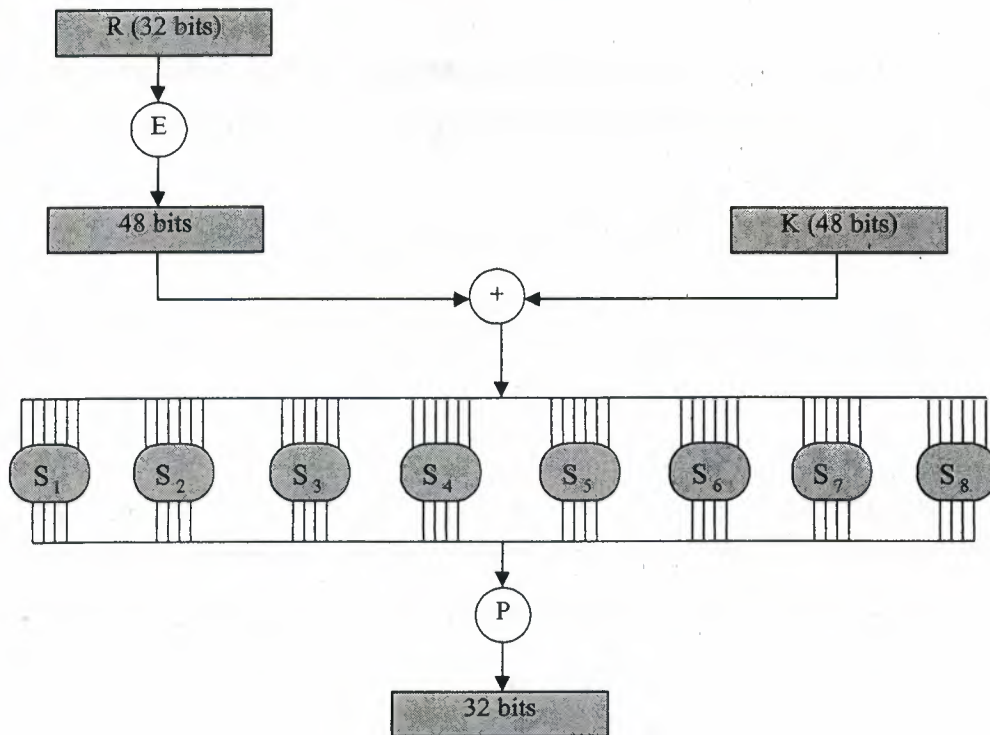


Figure 4.9. calculation of $F(R,K)$.

The round key K_i is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits (Table 4.2c). The resulting 48 bits are XORed with K_i . This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted as defined by Table 4.2d.

The role of the S-boxes in the function F is illustrated in Figure 4.9. The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. These transformations are defined in Table 4.3, which is interpreted as follows: The first and last bits of the input to box S_i form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i . The middle 4 bits

select a particular column. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example---in S, for input 011001, the row is 01 (row 1) and the column is 1100 (column 12). The value in row 1, column 12 is 9, so the outPut is 1001.

Each row of an S-box defines a general reversible substitution. Figure 4.4 may be useful in understanding the mapping. The figure shows the substitution for row 0 of box S,

Table 4.3. S-box in DES

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

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

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

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

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

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

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

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

by taking the outer bits from the two adjacent groups. For example, if part of the input word is

.....efgh ijkl mnop...

this becomes

defghi hijklm lmnopq

The outer two bits of each group select one of four possible substitutions (one row of an S-box). Then a 4-bit output value is substituted for the particular 4-bit input (the middle

four input bits). The 32-bit output from the eight S-boxes is then permuted, so that on the next round the output from each S-box immediately affects as many others as possible.

4.4.2 Key Generation

Returning to Figures 4.7 and 4.8, we see that the 56-bit key used as input to the algorithm is first subjected to a permutation governed by a table labeled Permuted Choice One (Table 4.4a). The resulting 56-bit key is then treated as two 28-bit quantities, labeled C_0 and D_0 . At each round, C_{i-1} and D_{i-1} are separately subjected to a circular left shift, or rotation, of 1 or 2 bits, as governed by Table 4.4c. These shifted values serve as input to the next round. They also serve as input to Permuted Choice Two (Table 4.4b), which produces a 48-bit output that serves as input to the function $f(R_{i-1}, K_i)$.

Table 4.4. Tables Used for DES Key Schedule Calculation

(a) Permuted Choice One (PC-1)

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

(b) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(c) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

4.4.3 DES Decryption

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed

4.5 Summary

This chapter concentrated on the structure of Data encryption Standard (DES), and most conventional encryption Algorithms, It is very complex, that's why its considered the most widely used conventional encryption Algorithms, For simplicity in explanation the chapter started with simplified DES which it takes only 8-bit plain text rather than 64-bit plaintext.

CONCLUSION

Wireless and Personal Communication systems are increasingly being regarded as essential communication tool for nowadays.

This thesis focused on the analysis of authentication and encryption discussing the algorithms techniques used in digital wireless digital systems GSM and GPRS so the long and complicated techniques, the security algorithms starts with authentication of the user then begin encryption, this leads to confidentiality in the using of GSM and with using of GPRS technique which allows the user to utilize more services (e.g. the Internet) it become more secure system.

Chapter 1 presented an overview of The Global System for Mobile communications which 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.

Chapter 2 introduced the GSM security techniques, the security model and algorithms were developed in secrecy and were never published. Eventually some of the algorithms and specifications have leaked out.

Chapter 3 presented the GPRS environment with short overview of GPRS networks architecture, In addition to the authentication and encryption mechanism which is presented in GSM it support IP security as the used holds its own IP address.

Chapter 4 was about the Data Encryption Standard (DES) algorithm, Its a block cipher that transforms 64-bit data blocks under a 56-bit secret key.

The application work was about development of Delphi software to implement the simplified data encryption standard (S-DES).

REFERENCES

- [1] D. M. Balston. The pan-European system: GSM. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.
- [2] Moe Rahnema. Overview of the GSM system and protocol architecture. IEEE Communications Magazine, April 1993.
- [3] M. Mouly and M.-B. Pautet, The GSM System for Mobile Communications, 1992.
- [4] M. Mouly and M.-B. Pautet, GSM Protocol Architecture: Radio Sub-system Signalling, IEEE 41st Vehicular Technology Conference, 1991.
- [5] GSM Specification Series 2.01.88, "GSM Services and Features".
- [6] Mouly M., Pautet M., The GSM System for Mobile Communications. 1992.
- [7] Hodges, M.R.L., "The GSM Radio Interface," British Telecom Technology Journal, Vol. 8, No. 1, January 1990.
- [8] Cooke, J.C.; Brewster, R.L., "Cryptographic Security Techniques for Digital Mobile Telephones," Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications, Vancouver, B.C., Canada, 1992.
- [9] European Telecommunications Standards Institute, Recommendation GSM 02.09, "Security Aspects".
- [10] Hudson, R.L., "Snooping versus Secrecy," Wall Street Journal, February 11, 1994.
- [11] Schneier, B., "Applied Cryptography," J. Wiley & Sons, 1994.
- [12] Williamson, J., "GSM Bids for Global Recognition in a Crowded Cellular World," Telephony, vol. 333, no. 14, April 1992.
- [13] R. Atkinson, RFC 1825: Security Architecture for the Internet Protocol. Naval Research Laboratory. August, 1995.
- [14] Van der Arend, P. J. C., "Security Aspects and the Implementation in the GSM System," Proceedings of the Digital Cellular Radio Conference, Hagen, Westphalia, Germany, October, 1988.
- [15] Schneier B., Applied Cryptography, 2nd Ed., Wiley, New York, 1996, 758, 1999
- [16] Mike Hibbert, Facing up to fraud. Mobile Communications International. July/August 1998.
- [17] Anderson Ross, A5 - The GSM Encryption Algorithm, 1999.

- [18] Briceno M. & Goldberg I. & Wagner D., An Implementation of the GSM A3A8 Algorithm, 1999.
- [19] 3GPP TS43.030 3d Generation Partnership Project: Technical Specification Group Service And System Aspects Security Related Network Function.
- [20] ETSI, GSM 03.60: Digital cellular telecommunications system (Phase 2+); Service Description; Stage 2, Version 6.1.0. July, 1998.
- [21] Lasse Huovinen, The Functionality of the GPRS Interface and Its Implementation in an Experimental System. Master's thesis, Helsinki University of Technology. June 4, 1998.
- [22] Nourouzi, J. Davidson, M. Garner, Mobile Internet and Intranets: The Road Ahead for Corporate Applications. GSM World Congress. February, 1998.
- [23] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.
- [24] Margrave David, GSM Security and Encryption, 1999.
- [25] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.

APPENDIX I

This is the interface of Simplified- Data Encryption Standard (S-DES) project which done by Delphi program.

The screenshot shows a Delphi application window titled 'Form1'. The main title bar of the window is 'Simplified - Data Encryption Standard (S-DES)'. Below the title bar, there is a tabbed interface with five tabs: 'Key', 'Generated Subkey1, Subkey2', 'Plain Text', 'Ciphertext', and 'Deciphertext'. The 'Key' tab is currently selected. Inside the 'Key' tab, there is a text area with the following instructions: 'Enter the Key to generate the two subkeys (Key1, Key2) that will be used in ciphering, deciphering processes. The Key Must be 10-bit binary.' Below this text, there is a text input field labeled 'Key'. At the bottom right of the tab area, there is a 'Next' button. At the bottom center of the window, there is a 'Close' button.

Figure AI.1. Shows where to put the key generator

Form1 Simplified - Data Encryption Standard (S-DES)

Key | Generated Subkey1, Subkey2 | Plain Text | Ciphertext | Deciphertext

The two subkeys to be used in ciphering & deciphering processes

Key

Subkey1

Subkey2

Next

Close

Figure AI.2. Shows the resulted two keys

Form1 Simplified - Data Encryption Standard (S-DES)

Key | Generated Subkey1, Subkey2 | Plain Text | Ciphertext | Deciphertext

Enter the plain text to be ciphered (Must be 8-bit binary)

Message

Next

Close

Figure AI.3. Shows the where to put the plaintext

Form1

Simplified - Data Encryption Standard (S-DES)

Key | Generated Subkey1, Subkey2 | Plain Text | **Ciphertext** | Deciphertext

Cipher text that have been encrypted by using the two subkeys

Ciphertext

Next

Close

Figure AI.4. Shows the produced ciphertext after encryption process.

Form1

Simplified - Data Encryption Standard (S-DES)

Key | Generated Subkey1, Subkey2 | Plain Text | Ciphertext | **Deciphertext**

Finally this the original plain text

DeCiphertext

Check The Result

Close

Figure AI.5. Shows the plaintext after decryption process.

APPENDIX II

This is the source code of Simplified- Data Encryption Standard (S-DES) which done by Delphi program.

```
unit Unit1;
```

```
interface
```

```
uses
```

```
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,  
  Forms,  
  Dialogs, StdCtrls, Buttons, ComCtrls, ExtCtrls;
```

```
type
```

```
  TForm1 = class(TForm)  
    PageControl1: TPageControl;  
    TabSheet1: TTabSheet;  
    Label1: TLabel;  
    KeyGen: TEdit;  
    TabSheet2: TTabSheet;  
    Label2: TLabel;  
    Label3: TLabel;  
    Key1: TEdit;  
    Key2: TEdit;  
    TabSheet3: TTabSheet;  
    Label4: TLabel;  
    msg: TEdit;  
    TabSheet4: TTabSheet;  
    Label5: TLabel;  
    Ciphertext: TEdit;  
    TabSheet5: TTabSheet;  
    Label6: TLabel;  
    DeCiphertext: TEdit;  
    BitBtn1: TBitBtn;  
    BitBtn2: TBitBtn;  
    BitBtn3: TBitBtn;  
    BitBtn4: TBitBtn;  
    Label7: TLabel;  
    Label8: TLabel;  
    Edit1: TEdit;  
    BitBtn5: TBitBtn;  
    Label10: TLabel;  
    Shape1: TShape;  
    Shape2: TShape;  
    Label9: TLabel;  
    Label11: TLabel;  
    Label12: TLabel;  
    Label13: TLabel;  
    Label14: TLabel;
```



```

Label15: TLabel;
procedure BitBtn1Click(Sender: TObject);
procedure BitBtn2Click(Sender: TObject);
procedure BitBtn3Click(Sender: TObject);
procedure BitBtn4Click(Sender: TObject);
procedure BitBtn5Click(Sender: TObject);
private
  { Private declarations }
public
  { Public declarations }
end;

```

```

//-----program-----

```

```

      type array8=array[1..8]of integer;
var
  Form1: TForm1;
  str,ch:string;
  i,temp:integer;
  P10,p10two      :array[1..10]of integer;
  k1,k2,m1,jP,ip,result :array8;
  ConvTemp: array[1..4]of integer;

```

```

implementation

```

```

{$R *.dfm}

```

```

//----- F -----

```

```

function F1(ip:array8;key1:array8):array8;
var
  i,r,c: integer;
  s0,s1:array[0..3,0..3]of integer;
  ep,xr1,xr2,jp:array8;
  p4,p4final :array[1..4] of integer;
begin
  s0[0,0]:=1; s0[0,1]:=0; s0[0,2]:=3; s0[0,3]:=2;
  s0[1,0]:=3; s0[1,1]:=2; s0[1,2]:=1; s0[1,3]:=0;
  s0[2,0]:=0; s0[2,1]:=2; s0[2,2]:=1; s0[2,3]:=3;
  s0[3,0]:=3; s0[3,1]:=1; s0[3,2]:=3; s0[3,3]:=2;

  s1[0,0]:=0; s1[0,1]:=1; s1[0,2]:=2; s1[0,3]:=3;
  s1[1,0]:=2; s1[1,1]:=0; s1[1,2]:=1; s1[1,3]:=3;
  s1[2,0]:=3; s1[2,1]:=0; s1[2,2]:=1; s1[2,3]:=0;
  s1[3,0]:=2; s1[3,1]:=1; s1[3,2]:=0; s1[3,3]:=3;

```

```

ep[1]:=ip[8];
ep[2]:=ip[5];
ep[3]:=ip[6];
ep[4]:=ip[7];
ep[5]:=ip[6];
ep[6]:=ip[7];
ep[7]:=ip[8];
ep[8]:=ip[5];

```

```

//--make xor with k1--//

```

```

for i:=1 to 8 do
  if ep[i]=key1[i] then
    xrl[i]:=0
  else
    xrl[i]:=1;

```

```

//--get p4 part1---//

```

```

r:=xrl[1]*2+xrl[4];
c:=xrl[2]*2+xrl[3];

```

```

if s0[r,c] =0 then
begin p4[1]:=0;p4[2]:=0; end

```

```

else if s0[r,c] =1 then
begin p4[1]:=0;p4[2]:=1; end

```

```

else if s0[r,c] =2 then
begin p4[1]:=1;p4[2]:=0; end

```

```

else if s0[r,c] =3 then
begin p4[1]:=1;p4[2]:=1; end;

```

```

//----//

```

```

//---get p4 part2 --//

```

```

r:=xrl[5]*2+xrl[8];
c:=xrl[6]*2+xrl[7];

```

```

if s1[r,c] =0 then
begin p4[3]:=0;p4[4]:=0; end

```

```

else if s1[r,c] =1 then
begin p4[3]:=0;p4[4]:=1; end

```

```

else if s1[r,c] =2 then
begin p4[3]:=1;p4[4]:=0; end

```

```

else if s1[r,c] =3 then
begin p4[3]:=1;p4[4]:=1; end;

```

```

//--applay p4--//

```

```

p4final[1]:=p4[2];
p4final[2]:=p4[4];
p4final[3]:=p4[3];
p4final[4]:=p4[1];

      //--make xor with the second 4 bit--//
for i:=1 to 4 do
  if p4final[i]=ip[i] then
    xr2[i]:=0
  else
    xr2[i]:=1;
for i:=5 to 8 do
  xr2[i]:=ip[i];
f1:=xr2;
end;
      //-----end function-----

```

```

      //-----keys generator-----

```

```

procedure TForm1.BitBtn1Click(Sender: TObject);
begin
  str:=KeyGen.text;
  if length(str)<>10 then
    begin
      showmessage('The Key must be 10 bit binary');
      exit;
    end;

  for i:=1 to 10 do
    begin
      if (str[i]='1') or (str[i]='0') then
        p10[i]:=strtoint(str[i])
      else
        begin
          showmessage('The Key must be 10 bit binary');
          exit;
        end;
    end;
end;

```

```

p10two[1] :=p10[3];
p10two[2] :=p10[5];
p10two[3] :=p10[2];
p10two[4] :=p10[7];
p10two[5] :=p10[4];
p10two[6] :=p10[10];
p10two[7] :=p10[1];

```



```

p10two[8] :=p10[9];
p10two[9] :=p10[8];
p10two[10]:=p10[6];

//----- LS 1 -----

temp:=p10two[1];
for i:=1 to 4 do
  p10two[i]:=p10two[i+1];
p10two[5]:=temp;

temp:=p10two[6];
for i:=6 to 9 do
  p10two[i]:=p10two[i+1];
p10two[10]:=temp;

//----- generate K1 -----

//----- P8 -----
k1[1]:=p10two[6];
k1[2]:=p10two[3];
k1[3]:=p10two[7];
k1[4]:=p10two[4];
k1[5]:=p10two[8];
k1[6]:=p10two[5];
k1[7]:=p10two[10];
k1[8]:=p10two[9];
//----- wire K1 -----
str:="";
for i:=1 to 8 do
begin
  ch:=inttostr(k1[i]);
  str:=str+ch;
end;
key1.text:=str;
//-----

//----- generate K2 -----

//----- LS 2 -----
p10[1] :=p10two[3];
p10[2] :=p10two[4];
p10[3] :=p10two[5];
p10[4] :=p10two[1];
p10[5] :=p10two[2];
p10[6] :=p10two[8];
p10[7] :=p10two[9];
p10[8] :=p10two[10];
p10[9] :=p10two[6];

```

```

p10[10]:=p10two[7];
//----- P8 -----
k2[1]:=p10[6];
k2[2]:=p10[3];
k2[3]:=p10[7];
k2[4]:=p10[4];
k2[5]:=p10[8];
k2[6]:=p10[5];
k2[7]:=p10[10];
k2[8]:=p10[9];
//----- wire K1 -----
str:="";
for i:=1 to 8 do
begin
  ch:=inttostr(k2[i]);
  str:=str+ch;
end;
key2.text:=str;
edit1.Text:= KeyGen.Text;
PageControl1.SelectNextPage(true);
end;

procedure TForm1.BitBtn2Click(Sender: TObject);
begin
  PageControl1.SelectNextPage(true);
end;

procedure TForm1.BitBtn3Click(Sender: TObject);
begin

  //-----
  //-----encrypt msg-----
  //-----

  //--get plain text--
  str:=msg.text;

  if length(str)<>8 then
  begin
    showmessage('The message must be 8 bit binary');
    exit;
  end;

  for i:=1 to 8 do
  begin
    if (str[i]='1') or (str[i]='0') then
      m1[i]:=strtoint(str[i])
    else
      begin

```

```

        showmessage('The message must be 8 bit binary');
        exit;
    end;
end;
//-- get IP--
ip[1]:=m1[2];
ip[2]:=m1[6];
ip[3]:=m1[3];
ip[4]:=m1[1];
ip[5]:=m1[4];
ip[6]:=m1[8];
ip[7]:=m1[5];
ip[8]:=m1[7];
//*****
result:=f1(ip,k1);

    //----- switch -----
    for i:=1 to 4 do
        ConvTemp[i]:=result[i];

    for i:=1 to 4 do
        result[i]:=result[i+4];

    for i:=5 to 8 do
        result[i]:=ConvTemp[i-4];
    //-----

result:=f1(result,k2);

jp[1]:=result[4];
jp[2]:=result[1];
jp[3]:=result[3];
jp[4]:=result[5];
jp[5]:=result[7];
jp[6]:=result[2];
jp[7]:=result[8];
jp[8]:=result[6];

str:=" ";
for i:=1 to 8 do
begin
    ch:=inttostr(jp[i]);
    str:=str+ch;
end;
Ciphertext.text:=str;
PageControl1.SelectNextPage(true);
end;

procedure TForm1.BitBtn4Click(Sender: TObject);
begin

```



```

//-----deciphering-----
ip[1]:=jp[2];
ip[2]:=jp[6];
ip[3]:=jp[3];
ip[4]:=jp[1];
ip[5]:=jp[4];
ip[6]:=jp[8];
ip[7]:=jp[5];
ip[8]:=jp[7];
result:=fl(ip,k2);

for i:=1 to 4 do
  ConvTemp[i]:=result[i];

for i:=1 to 4 do
  result[i]:=result[i+4];
for i:=5 to 8 do
  result[i]:=ConvTemp[i-4];

result:=fl(result,k1);
ip[1]:=result[4];
ip[2]:=result[1];
ip[3]:=result[3];
ip[4]:=result[5];
ip[5]:=result[7];
ip[6]:=result[2];
ip[7]:=result[8];
ip[8]:=result[6];
  str:=" ";
  for i:=1 to 8 do
    begin
      ch:=inttostr(ip[i]);
      str:=str+ch;
    end;
  DeCiphertext.text:=str;
  PageControl1.SelectNextPage(true);
end;
procedure TForm1.BitBtn5Click(Sender: TObject);
begin
  close;
end;
procedure TForm1.Button2Click(Sender: TObject);
begin
  if DeCiphertext.Text=msg.Text then
    showmessage('The Encryption Succeeded')
  else
    showmessage('The Encryption Failed');
end;

end.

```