Secure Communication Over Android Handset

Prepared By

Mayur Mahajan

12MCEI17

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SPECIALIZATION IN INFORMATION & NETWORK SECURITY

AHMEDABAD-382481

May 2014

Secure Communication Over Android Handset

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology Department of Computer Science and Engineering

Specialization in Information & Network Security

By

Mayur Mahajan

(12MCEI17)

Guided By

Prof. Pooja Shah

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SPECIALIZATION IN INFORMATION & NETWORK SECURITY

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2014

Undertaking for Originality of the Work

I, **Mayur Mahajan**, Roll. No.**12MCEI17**, give undertaking that the Major Project entitled **"Secure Communication Over Android Handset**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology Department of **Computer Science and Engineering** specialization in **Information & Network Security** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place:

Endorsed by

Prof. Pooja Shah

(Signature)

Certificate

This is to certify that the Major Project entitled **"Secure Communication Over Android Handset"** submitted by **Mayur Mahajan (12MCEI17)**, towards the partial fulfillment of the requirements for the degree of Master of Technology Department of **Computer Science and Engineering** Specialization in**Information & Network Security** of Nirma University, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Pooja Shah
Guide, Associate Professor
Department of C.S.E.,
Institute of Technology,
Nirma University, Ahmedabad.

Prof. Sharada Valiveti
Branch Coordinator(INS)
Department of C.S.E.
Institute of Technology
Nirma University, Ahmedabad

Dr. Sanjay Garg
HOD [C.S.E. Dept.],
Institute of Technology,
Nirma University, Ahmedabad

Dr K Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad

Acknowledgements

My deepest thanks to **Prof. Pooja Shah**, Associate Professor, Department of Computer Science and Engineering, Institute of Technology, Nirma University, for giving me an opportunity and guidance throughout the project. It was only due to his valuable opinion, cheerful enthusiasm and ever friendly nature that I was able to do part of my research work in a respectable manner.

I am really thankful to our course Co-ordinator **Prof. Sharada Valiveti**, Information & Network Security, Department of Computer Engineering, Nirma University, Ahmedabad, for his invaluable guidance and assistance, without which the accomplishment of the task would have never been possible. We also thank him for giving this opportunity to explore into the real world.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. Ketan Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank my Institution, all my faculty members in Department of Computer Science.

I would like to thank my colleagues for being with me in any condition. And I am thanking them to keep me calm and cool every time.

Last, but not the least, no words are enough to acknowledge constant support and sacrifices of my family members because of whom I am able to complete the first part of my dissertation work successfully.

Mayur Mahajan

12MCEI17

Abstract

Messages play important role in communication, because they may carry our personal information, such as our PIN code, transaction details, passwords, and personal details which is secret etc. Thus security of messages is also necessary. There is a need of security application which can send all messages securely. These is also a problem with the encryption algorithm, which is best suited to mobile device. Blowfish is an algorithm which is best suited for security purpose on handset devices. Along with the encryption technique of Blowfish, One more security that can be added is an application accessing login. Application accessing login asks for username and password. Through application accessing login, the security of messages also increase, even after the handset is handed over to someone else. The message sent over GSM network, Bluetooth message passing and message sent over internet all are merged into a single application. Thus the security is doubled and privacy to messages can be achieved.

Contents

Undertaking for Originality of the Work iii

Certificate iv

Acknowledgements v

Abstract vi

List of Tables x

List of Figures xi

1 Introduction 1

1.1 General 1

1.2 SMS instead of Call 1

1.3 Applications of SMS 2

1.3.1 Banking 2

1.3.2 Emergency services 2

1.3.3 Reminders of hospital appointments 2

1.3.4 Commercial uses 2

1.3.5 In Business 3

1.4 Motivation 3

1.5 Scope of Project 3

2 Literature Survey and Important Observations 5

2.1 Basic Network Architecture 5

2.2 Features & Protocol Services of SMS 6

2.3 Additional Features 7

2.4 GSM Cryptography 8
2.4.1 Authentication 8
2.4.2 Confidentiality 9
2.5 Discussion 10
2.5.1 GSM Encryption Algorithms 10
2.5.2 Key Length 10
2.5.3 Conclusion 11
2.6 GSM : having constant attack 11
2.7 A5 Weaknesses 12
2.7.1 Interception of GSM traffic 13
2.7.2 US Patent 14
2.8 Algorithms proposed to Secure end-to-end GSM 15
2.8.1 DES 15
2.8.2 AES 15
2.9 Issues 15
2.9.1 Security of SMS in Business Purpose 16
2.9.2 Security in Personal 16

3 Proposed Approach **18**
3.1 Current Scenario 18
3.2 Proposed Approach 19

4 Encryption Algorithm **20**
4.1 Blowfish Algorithm 21
4.2 Methodology 21
4.3 Comparing to different algorithms 23

5 Implementation **26**
5.1 Android Application 26
5.2 Send SMS 28
5.3 Bluetooth Chat 30

6 Conclusion and Future Work **34**

References **35**

Appendices **38**

A Implementation Plateform **39**

B Applications Used **40**

List of Tables

2.1 Time taken for different key lengths 11
2.2 Required machines to break key 11

4.1 Number of rounds in Different Algorithms 24
4.2 Power Analysis in Different Algorithms 24
4.3 Throughput with respect to other algorithms 24

List of Figures

2.1 Flow of SMS in GSM Network 6
2.2 GSM Cryptography 9

3.1 GSM Architecture 18
3.2 Proposed Approach 19

4.1 Blowfish Encryption Algorithm 23
4.2 The F function 23
4.3 Execution Time with respect to other algorithms 25

5.1 Prompting for details of username and password 26
5.2 Welcome screen waiting for user's choice 27
5.3 Asking for phone nu. and message. when message is send and decrypted 28
5.4 Decryption of message at receiver end 29
5.5 Menu options and prompting for Bluetooth permission for visibility . . . 30
5.6 Menu options and pop up list of bluetooth devices 31
5.7 Prompting for passkey 32
5.8 Both the device get paired with each other 32
5.9 Communication between the users via secure bluetooth messages 33

Chapter 1

Introduction

1.1 General

Today the mobile phones are the largest selling product in electronics for consumer in whole world. There are so many areas where the connectivity is not so good, like. poor rural areas. Only voice call and text messages are supported by the phones used in these areas. These phones have spread over most of the areas of the world. Still there are 48 millions of people with no electricity but with these featured mobile phone. It is expected that next year 1.7 billion people who don't have band account but will have cell phones.

As per record, 4.16 billion users had made SMS last year in the world. In 2007 6.1 trillion messages were sent. As we are seeing that mobile phones are getting cheaper and cheaper and telecom infrastructure is also increasing with internet access. However, SMS service is non replaceable. **In 1992, the first SMS was sent. It is one of the most popular communication form among people of young generation. Trillions of messages are being send to each other.**

1.2 SMS instead of Call

In certain respect, short messages from mobile phone has advanced communication. The benefit of SMS is that it we can communicate with other people instantly wherever they are, without disturbing them. SMS can be used for concise, efficient and quick way to communicate. SMS are cheapest form of communication with reliability, which is an advantage to young generation. When voice call conversation are prohibited, then SMS has great advantage. **As the mobile phones popularity, affordability, avail-**

ability in increasing every year, SMS is becoming one of primary mode of communication.[1]

The numbers of messages passing in children of teen ages are increased in 2009 by 50 SMS/day to 60 SMS/day. SMS messaging is a mode of communication through which you can be connected daily.

Mostly teen agers send and receive a great numbers of SMS. More than 75% teens who having mobile phone use SMS.

- An average teen age person does 60 SMS a day.
- More than 14% teens talk everyday with friends. [2]

1.3 Applications of SMS

1.3.1 Banking

There are many people who use internet banking and other applications, which can make transaction from mobile phone via SMS only. e.g. Train bookings, Mobile recharge. The SMS are also used for increasing security in e-banking. OTP (one time passwords) are widely used to get security for personal transactions. These OTPs are sent via SMS only.

1.3.2 Emergency services

SMS are used to inform emergency services in some countries, if the number is registered with the emergency service center. This service is mainly focused on the people with disability, those who can't speak, where due to low quality signal strength voice call is impossible.

1.3.3 Reminders of hospital appointments

Hospital appointments are also reminded by SMS service. National Health Service of England expenses more than $980 million in a year. As per survey 24,709 patients appointment were scheduled in south-east London. With the help of these SMS reminder service 25-28% missed appointment were reduced.

1.3.4 Commercial uses

SMS are also used for commercial purpose, e.g. T.V. serials are asking questions to users, who are watching those serial, these answers are to be sent via SMS. Some T.V. serials

also asks for voting. On behalf of the message performance and cost, the SMS service is best suited.

1.3.5 In Business

During mid-2000s, text messages were started using in business purpose. Since company searches for competitive advantages, so employees are facilitated with new technologies and some good featured applications. All business having SMS service facility for its local employees, so that they got connected to other via instant SMS service.

The investor and stock brokers had got so much relief when the SMS service is facilitate to them. This service gives them the latest updates of stock market.

Several Universities had already implemented SMS texting system for Students to inform about college updates, assignments, projects, bus facilities and books related etc

1.4 Motivation

We are not living in the age, where the strength and economy of any nation is measured by its resources like, e.g. Water, Coal Mine, Metals, fields for irrigation etc.. We are living in informative age, where the strength of any nation is measured by the ideas in people's mind. The ideas in one's mind can bring revolution. Thus security in today's life is so important. SMS security is a footstep towards keeping privacy & confidentiality.

1.5 Scope of Project

As already seen, how SMS messaging are accepted by people in whole world, the security in SMS would also be preferable. Scope of secure SMS would also be wide. Most important use will be in Business application and in Banking. Business purpose messages are confidential to that business only. These are not to be opened to others, these messages are to be in that business people only.

The people who uses internet banking, SMS security will be of great use for them. If the Security application at user end and at the BANK gateway is applied, then the messages between the user mobile and the Bank's SMS Gateway will communicate securely. In current scenario, the user send his ID and Password and other personal details to SMS Gateway in a plain text. If the messages are eavesdropped then all personal details will

be leaked, and eavesdropper can use them for his personal use or steal all the money, because the bank provides all the services and facilities to the mobile user. In proposed scenario, if security system of SMS applied, then the Bank will accept only encoded message and decrypt at his own end. If the eavesdropper get the message he will not be able to get the details, if anyhow we know the details then also he can't encrypt the message, because he wouldn't have key and encryption algorithm. Thus the communication will be secure and the User's information is also secured from eavesdropping.

Also, the people who want their communication secure for any reason can make use of this mechanism to remain safe for their communication.

Currently, our application encrypt and decrypt with only a single key, for more security purpose we need asymmetric key cryptography, so that there will be different encryption and decryption key thus the system will be secure enough. This asymmetric key concept can be achieved by a Key Distribution Environment (KDE). It is a work of KDE to distribute the key securely between the users. Our futute approach towards this project will be to build a KDE environment.

Chapter 2

Literature Survey and Important Observations

SMS is used in business and social applications e.g. Delivery of Emails, Stock Quotations, Electronic Voting, OTP, Mobile banking and many more. SMS is supported by all mobile network technologies like :

- CDMA (Carrier Division Multiple Access)
- GSM (Global System for Mobile communication)
- GPRS (General Packet Radio Service)

SMS can be transmitted to and from any mobile device or any capable device which can generate SMS. Many electric machines are controlled by SMS. Initially SMS could contain maximum 160 characters. Each character was coded in 7 bits, thus is occupies 140 Bytes. End to End delivery of SMS takes place in 2 parts, first part of SMS submission in Short Message Service Center by sender, second part of Delivery to receiver, so it is based on STORE and FORWARD service.[3]

2.1 Basic Network Architecture

Flow of SMS in GSM network consist some Stations and Servers as shown in figure. These stations are:

- **SME (Short Message Entity) -** it receives and sends SMS.

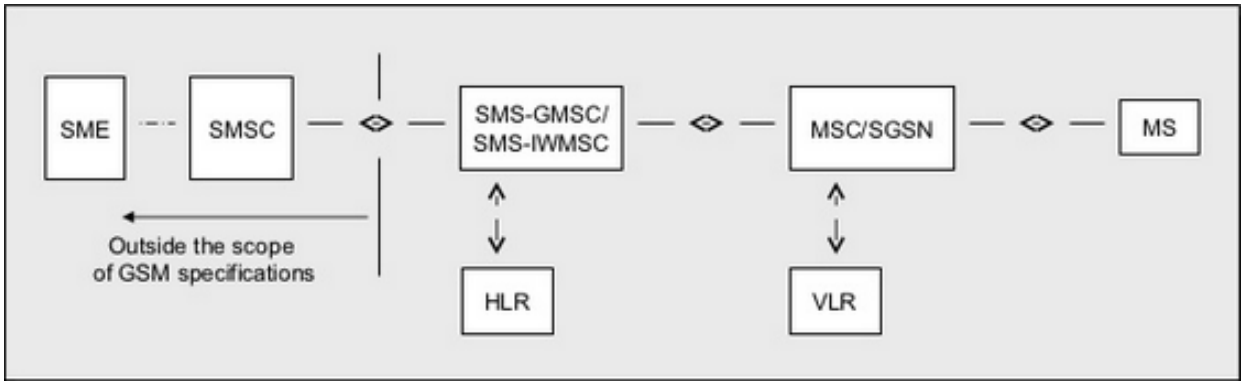

Figure 2.1: Flow of SMS in GSM Network

- **SC (Short Message Service Centre) -** It stores the message and forwards it to Mobile Station or SME
- **SMS-GMSC (Gateway MSC) -** It receives SMS from the Short Message Service Center, interrogates the Home Location Register for routing information and then forward it to the Mobile Switching Center.
  - **HLR (Home Location Register) -** It is a database containing information from the MSC or SGSN.
- **MSC (Mobile Service Centre) -** In a geographical area it performs switching functions for MS.
  - **VLR (Visitor Location Register) -** It contains some temporary information about subscribers who are from other states.
- **SGSN (Serving GPRS Support Node) -** It is a packet switching center for MS. It is used in place of the MSC when information of SMS over GPRS is transferred.
- **MS (Mobile Station) -** It is a device in the cellular network, which is capable of receiving and sending short SMS.[3]

2.2 Features & Protocol Services of SMS

- **SMS is a store and forward technology in point-to-point with 2 services :**
  - SM-MT (Short Message Mobile Terminated) - In SMS delivery protocol transmitting a SMS from the MSC to MS.

  - SM-MO (Short Message Mobile Originated) - In SMS submitting protocol transmitting a SMS from MS to MSC.

- **SMS allows delivery of message while handset is in use or it is powered off. When the handset is powered on, the SMS get received.**
  - When SMS gets deliverd then MS receives TPDU (transport data protocol units)
  - When SMD is submitted to send then MS sends TPDU (transport data protocol units)
  - Remark: the Transport Data Protocol Unit contains the user data.

- **SMS delivery confirmation report is also permitted by SMS protocol.** [3]

2.3 Additional Features

- **SMS of more than 140 Bytes is also concatenated into a longer message that is enabled for transmission by SMS standards.**

- **SMS can be compressed too using some mechanism in GSM**
  - Compression in SMS is applied to user data but not to the Data-Header
  - Longer messages which exceeds 140 Bytes, even after compression, then they can are concatenated.

- **In many areas, like North America, users can send SMS by 5 digit numbers called short-codes.**
  - SMS voting is the best example of short codes.
  - To minimize Spam message or reduction is one of the objective of Short-Codes.
  - These Short codes are chargeable to application provider being used to price and market services.

- **Multi-network and Multi-protocol inter-working is also available by Service gateway products.** [3]

2.4 GSM Cryptography

Usually customer information is stored on phone itself in all technologies, while in GSM it is stored in a personalized smartcard, removable storage i.e. SIM card. The Subscriber Identity Module is very tiny in size, with memory storage and a low power consumption microprocessor. Along with the users information i.e. telephone directory number, speed dial number, SMS, Serving Network, it performs some security functions to make secure communication between network and customer.

When SIM manufacturer company releases SIM, then it is already programmed with secret 128-bit key called Ki which is unique. This key is hidden and invisible to user, but only available to special computer based algorithms that can access SIM card internally. This key Ki is also kept with the network operator, which is used for authentication. Two cryptographic algorithm referred to as A3 and A8 are also contained by SIM, which are used to check authentication and confidentiality. [17]

2.4.1 Authentication

Authentication is the primary security function provided by network operator. Using this it is assured that the requesting phone requesting service to the network is a legitimate and not impostor subscriber. This process is carried out to identify the subscriber by a challenge-response process, which uses a random number.

A random number is sent by the network to the mobile user. This random number (RAND) is of bit. When the user handset receives the random number then it is further processed by SIM card. The SIM card has an algorithm i.e. A3, using this algorithm the random number is given as input and the Ki is the key of 128bit then an output of 32-bit is generated, which is called Signed Response. This output number, called SRES i.e. Signed Response is sent out of the SIM to the network via phone. This phones response to the network is called challenge.

On the other hand the network also have same set of numbers and operations. Network itself do the same process with identical RAND variable and Ki, and generate its own SRES, which is compared with the SRES value received from the mobile station. If after comparison both the numbers are same, then the network consider the phone as legitimate and also allows mobile station to proceed for its services. If the values are not matched then the network denies mobile user to access the service.[18]

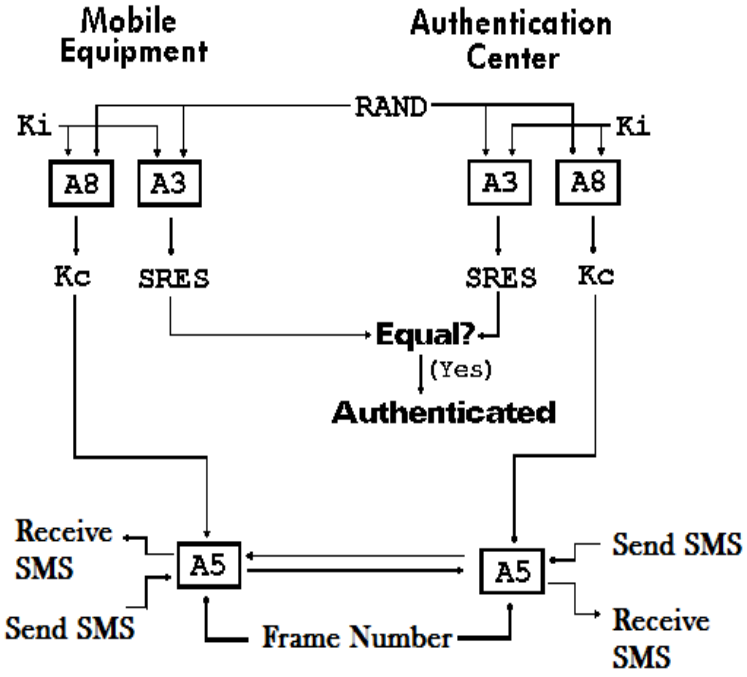

Figure 2.2: GSM Cryptography

This RAND variable has changed the value on every access attempt because of an eavesdropper can record the value and try to access the service. Thus a true user phone will always return the correct 32-bit code while the cloned phone would not be successful to generate proper SRES, and will be thwarted.

2.4.2 Confidentiality

Another service provided by the SIM card is to encrypt the connection between the mobile user and the base station. Usually a radio channel is shared in time division domain with capacity upto 8 users at a time. These 8 time slots are accessed by 8 distinct users to send and receive information over a common radio channel. This time slot is of 4.6 milliseconds and frame number is used to identify them, which is very short time. Two frames are used in a GSM conversation, one in forward direction and other in backward direction, i.e. one from base station to mobile user and other from mobile user to base station. Each frame contains user information of 114 bits. These bits are digitized and compressed speech always.

After a mathematical challenge, same random number with Ki is used again in A8 algorithm, ran by SIM card to generate a 64-bit long key Kc. This Key Kc is given to

mobile by the SIM, where the next algorithm i.e. A5 is to be applied in order to encrypt the user data. A5 algorithm takes this Kc as key input and user data i.e. voice or SMS, to generate secure output, which is to be transmitted over network.

A5 algorithm is a part of mobile phone not a part of SIM card. Mobile phones are to be designed in such a way that encryption and decryption occurs after every 4.6 milliseconds of receiving and sending frame. Each mobile manufacturer company knows the algorithm. Thus it may take additional required hardware on phone and base station, which also raise the cost and increase complexity in network. [4]

2.5 Discussion

2.5.1 GSM Encryption Algorithms

In 1994 the algorithm of GSM A5 algorithm was released secretly, therefore some key points facts related A5 algorithm are :

- It is a stream cipher algorithm which consist three clock controlled LFSRs, which have degree as 19, 22, and 23.
- The middle bits of these three shift is taken and threshold function is applied onto it, which is called the clock control.
- These 3 shift registers having a sum of the degree as 64. This 64-bits helps in initialization of the shift register contents.
- The shift register is also fed by a 22-bit TDMA frame number.
- Each TDMA frame uses two 114-bit stream which are XOR-ed with traffic channels, i.e. uplink and downlink.

2.5.2 Key Length

Assuming a machine, which crack the encryption with a speed of one million encryptions/second, and check how much time it will take to crack our message with the specific key lengths:

As we can see that it takes extremely large time to crack 128-bit key. Today we have machines, which are capable to test millions keys/second. The algorithm, which we use

Key length (bits)	32-bits	40-bits	56-bits	64-bits	128-bits
Time taken	1.19 Hours	12.7 Days	2,291 Years	584,542 Years	10.8 x 10^{24} Years

Table 2.1: Time taken for different key lengths

Key size (bits)	40	56	64	128
1 day	12	836,788	2.14 x10$\hat{8}$	3.9 x 10$\hat{2}$7
1 week	2	119,132	3.04 x 10$\hat{6}$	5.6 x 10$\hat{2}$6
1 year	-	2,291	584,542	10.8 x 10$\hat{2}$4

Table 2.2: Required machines to break key

A5 having 64 bits key size, but having 40 bits of effective length only, provides sufficient security for message with a short time.

2.5.3 Conclusion

GSM provides sufficient security in Authentication and Confidentiality. This is most secure cellular network in telecommunication. All the keys used for authentication, encryption and subscriber identification number are stored on a removable smart card, which is kept with user in mobile handset. Even without encryption algorithm A5/2 in GSM systems, it is providing better security than the analog system. Analog system dont use digital modulation, TDMA channel access and speech coding. [5]

2.6 GSM : having constant attack

BERLIN A German machine engineer said Monday that he had deciphered and distributed the mystery code used to scramble the vast majority of the world's computerized cellular telephone calls, saying it was his endeavor to uncover shortcomings in the security of worldwide remote framework. The movement by the encryption master, Karsten Nohl, planned to address the adequacy of the 21-year-old G.s.m. calculation, a code created in 1988 and still used to secure the protection of 80 percent of versatile calls around the world.

In August, at a programmers' gathering in Amsterdam, Mr. Nohl tested other machine programmers to help him break the G.s.m. code. He said in regards to 24 individuals, a few parts of the Chaos Computer Club, which is situated in Berlin, worked freely to create the vital volume of irregular mixes until they imitated the G.s.m. calculation's code book an inconceivable log of parallel codes that could hypothetically be utilized to

interpret G.s.m. telephone call. "We are not prescribing individuals utilize this data to overstep the law," Mr. Nohl said. "What we are doing is attempting to prod the world's remote administrators to utilize better security."

Mr. Nohl said the calculation's code book was accessible on the Internet through administrations like Bittorrent, which some individuals utilization to download inconceivable amounts of information like movies and music. He declined to give a Web connection to the code book, for dread of the lawful ramifications, yet said its area had spread by informal.

In 2007, the G.s.m. Cooperation created a 128-bit successor to the A5/1, called the A5/3 encryption calculation, yet most system administrators have not yet contributed to make the security update.[6]

2.7 A5 Weaknesses

A5/1 is the solid form of the encryption calculation utilized by about 130 million GSM clients in Europe to secure the over-the-air security of their cell voice and information correspondence. The best distributed ambushes against it require between 240 and 245 steps. This level of security makes it powerless against fittings based ambushes by vast associations, however not to programming built assaults in light of different focuses by programmers.

The primary assault obliges the yield of the A5/1 calculation throughout the initial two minutes of the discussion, and processes the key in something like one second. The second ambush obliges the yield of the A5/1 calculation throughout about two seconds of the discussion, and figures the key in a few minutes. The two ambushes are connected, however utilize diffrent sorts of time-memory tradeoff. The strike were checked with real usage, aside from the preprocessing stage which was widely tested instead of totally executed.[7]

An extremely reasonable ciphertext-just cryptanalysis of GSM scrambled correspondence, and different dynamic ambushes on the GSM conventions. These assaults can even break into GSM arranges that utilize "unbreakable" figures. We first portray a ciphertext-just ambush on A5/2 that obliges a couple of dozen milliseconds of scrambled off-the-air cell discussion and discovers the right enter in under a second on a PC. We stretch out this assault to a (more perplexing) ciphertextonly ambush on A5/1. New (dynamic)

ambushes on the conventions of systems that utilization A5/1, A5/3, or even GPRS. These assaults adventure blemishes in the GSM conventions, and they work at whatever point the cell telephone upholds a frail figure, for example, A5/2. We underline that these strike are on the conventions, and are in this way material at whatever point the phone backs a frail figure, for instance, they are likewise appropriate for ambushing A5/3 systems utilizing the cryptanalysis of A5/1. Not at all like past strike on GSM that require improbable data, in the same way as long known plaintext periods, our assaults are extremely functional and don't require any learning of the substance of the discussion. Besides, we portray how to sustain the assaults to withstand gathering slips. Accordingly, our assaults permit ambushers to tap discussions and unscramble them either progressively, or at any later time. We show a few assault situations, for example, call commandeering, adjusting of information messages and call robbery.[8]

2.7.1 Interception of GSM traffic

Black Hat Hackers are a gathering of machine security analysts. We designed a minimal effort engineering utilizing off of the rack fittings to accept and decode GSM signs. We are the first to execute a minimal effort pragmatic assault against the GSM figure A5/1. Our objective is to bring issues to light and to persuade the Mobile Industry to secure the system. The air interface takes a shot at 4 fundamental recurrence groups. The extent of the remote indicator can surpass 35km. Today's Mobile Phones (MS) are mind blowing compelling sign transceivers. They work on two 32-bit CPU's at in excess of 350 Mhz. Different Nokia cell telephones have been transported by mishap with support usefulness. These telephones might be designed from an ordinary PC to accept any GSM information from the telecast station. These telephones cost between $1-5 USD and are accessible on E-narrows. Other business items like the Sagem follow versatile or Ericsson telephones might be utilized also. The USRP is a product characterized radio and can get and transmit any sort of information between 0 and 3 Ghz. We have created a product module to get and unravel GSM signs. The USRP costs $750 USD. There exists an extensive variety of business testing and block attempt supplies from affiliates all around the globe. Some of these items are customized for tapping GSM discussions.[9]

2.7.2 US Patent

US. patent provision Ser. No. 10/554,587, titled "Cryptanalysis Method and System", recorded by the innovator of the present innovation on Sep. 25, 2006 now US Pat. No. 8,009, 826, Which is a National Phase Application of PCT/Il2004/000364 ?headed on Apr. 30, 2004, Which thusly asserts necessity from Israel Patent IL 155671 ?headed on Apr. 30, 2003, all of Which are thus consolidated into the present depiction in their sum. As per the present creation, there is given a system and framework to performing viable cryptanalysis of GSM encoded interchanges. The strategy utilization figure content just cryptanalysis. The framework needs not be joined by wire to the cell base, rather it may get messages transmitted broadcasting live.
New routines for ambushing GSM encryption and security conventions are unveiled. These systems are much less demanding to apply and much speedier. Fundamentally, for A5/2 GSM, a portable assaulter framework gets the scrambled messages, performs an ef?cient cryptanalysis and empowers listening to the GSM messages and/or to survey related data. At the point when performed on a PC, the procedure may take short of what one second.

On a basic level, a comparative strategy could be connected to A5/1 GSM, however for this situation the encryption is more intricate and may require something like 5 minutes of correspondence messages to decode. A complex framework, which may be di?icult to actualize, may be needed since it need to stay informed regarding recurrence bouncing in GSM.
As per an alternate part of the present development, for A5/1 GSM the agressor framework makes a little cell around itself, which cell incorporates the target GSM telephone. The framework mimics the cell system for the target telephone, and the target telephone for the GSM base. This obliges a transmit capacity in the agressor framework, however the unscrambling is significantly streamlined and much quicker.[10][13]

2.8 Algorithms proposed to Secure end-to-end GSM

2.8.1 DES

Worldwide System for Mobile Communications (GSM) is a standout amongst the most normally utilized cell advances as a part of the world. One of the goals in versatile correspondence frameworks is the security of the traded information. GSM utilizes numerous cryptographic calculations for security like A5/1, A5/2 and A5/3. Indeed thus, these calculations don't give sufficient level of security to securing the classifiedness of GSM. Thus, it is alluring to expand security by extra encryption routines. This paper introduces a voice encryption technique called: "DES with Random stage and Inversion", focused around present voice channel, which overcomes information channel's deficiencies and takes care of the issue of entering the RPE-LTP vocoder by the scrambled voice. The proposed technique satisfies an end-to-end secured correspondence in the GSM; guarantee a great similarity to all GSM systems, and simple usage without any change in these frameworks.[11][20]

2.8.2 AES

Worldwide System for Mobile Communications (GSM) is the most generally utilized cell innovation as a part of the world. Principle objective in versatile correspondence frameworks is security of information traded. GSM utilizes a few cryptographic calculations for security like A5/1, A5/2 and A5/3. Anyhow it has been observed that these calculations are broken by different handy assaults so these calculations don't give sufficient levels of security to ensuring the privacy of GSM thusly it is alluring to secure information by extra encryption. In this paper we have done extra encryption by actualizing AES calculations on GSM Network. This paper likewise dissects the adequacy of these calculations against beast energy assault actualized in the earth.[12][21]

2.9 Issues

Subsequently GSM system is no more secure enough to keep our information secure with itself.

- **Security is a rising concern like that with email, for instance:**

- SPAM sending of spontaneous messages and ads through SMS (e.g. to lure clients to call numbers that have a high for every moment charg
- Infection - resend of message to all numbers in the telephone's location book (e.g. by means of a Trojan Horse)
- Data fraud - recovery of particular data from a SIM (Subscriber Interface Module) card.[16]

2.9.1 Security of SMS in Business Purpose

Security, privacy, dependability and rate of SMS are among the most critical assurances commercial enterprises, for example, budgetary administrations, vitality and things exchanging, medicinal services and ventures request in their mission-discriminating techniques. One approach to certification such a nature of content informing lies in presenting Slas (Service Level Agreement), which are regular in IT contracts. By giving measurable Slas, partnerships can characterize unwavering quality parameters and set up a high caliber of their administrations. Only one of numerous SMS provisions that has demonstrated profoundly famous and fruitful in the money related administrations industry is versatile receipts. In January 2009, Mobile Marketing Association (MMA) distributed the Mobile Banking Overview for money related establishments in which it talked about the favorable circumstances and inconveniences of portable channel stages, for example, Short Message Services (SMS), Mobile Web, Mobile Client Applications, SMS with Mobile Web and Secure SMS.[14]

2.9.2 Security in Personal

Customer SMS ought not be utilized for classified correspondence. The substance of regular SMS messages are known to the system administrator's frameworks and faculty. Accordingly, buyer SMS is not a suitable innovation for secure correspondences.

To address this issue, numerous organizations utilize a SMS passage supplier focused around Ss7 integration to course the messages. The focal point of this universal end model is the capability to course information straightforwardly through Ss7, which gives the supplier perceivability of the complete way of the SMS. This methods SMS messages might be sent specifically to and from beneficiaries without needing to experience the SMS-C of other versatile administrators. This methodology lessens the amount of

portable administrators that handle the message; then again, it ought not be recognized as an end-to-end secure correspondence, as the substance of the message is laid open to the SMS passage supplier. [15]

Disappointment rates without regressive notice could be high between bearers (T-Mobile to Verizon is famous in the US). Universal messaging could be amazingly questionable relying upon the nation of beginning, end and particular bearers.

Chapter 3

Proposed Approach

3.1 Current Scenario

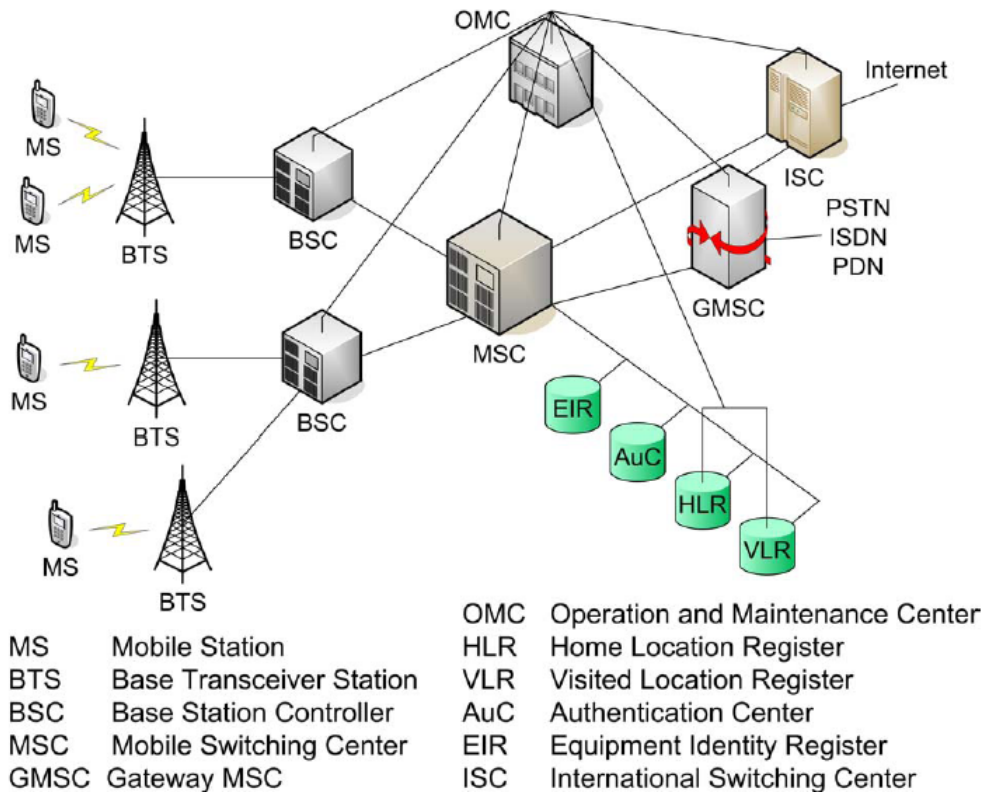

Figure 3.1: GSM Architecture

In current scenario the encryption is in air medium only. The data between mobile station and base station is only encrypted. Rest of the transmission is in plain only. The wiretapping can be done after base station also by service provider side too.

3.2 Proposed Approach

In proposed scenario the encryption is in the full transmission, i.e. from mobile station to mobile station. Even at the service provider side would not be able to capture the original message. Thus at the most vulnerable place, i.e. Air medium, will have double encryption. First which will be made by us and second one is which takes place between mobile station and base station. So if the intercepter captures the medium then also he would not be able to identify that which decryption is original ones. Finally our system will be secured and we would have safe and uninterfered communication.[17]

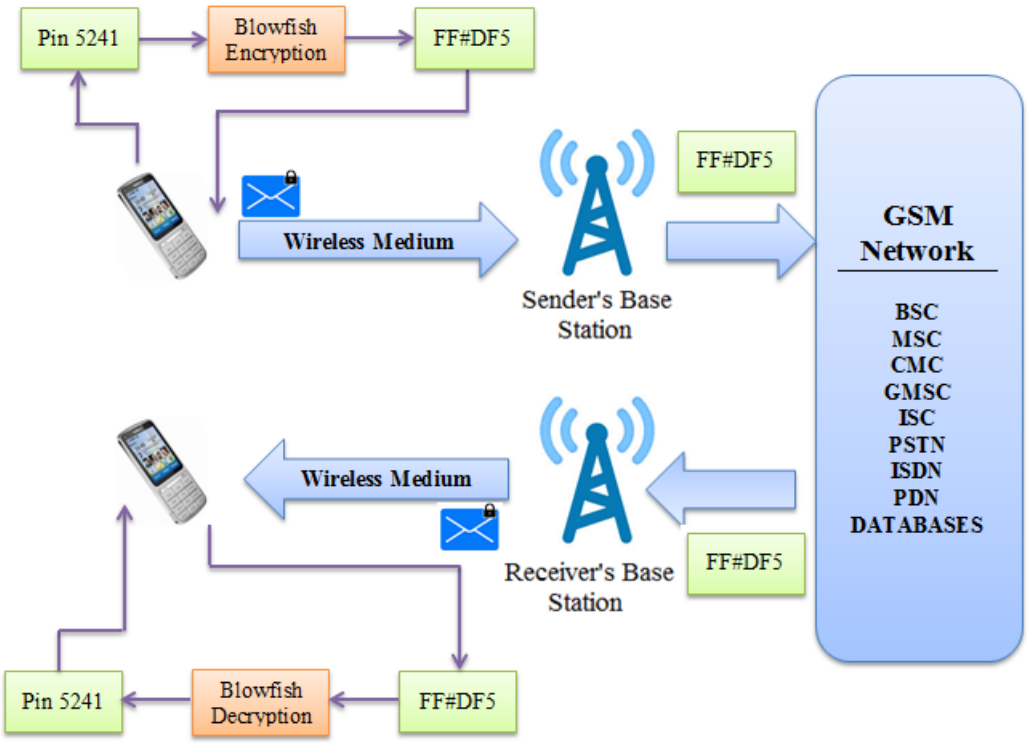

Figure 3.2: Proposed Approach

When we will get the encryption doubled then the attacker will try to find the key but there will not be any single key which will result in decryption of doubled encryption to plain voice directly. So, the attacker would required the key of wireless transmission and then he will be required with the key of our algorithm. In case of hit and trial of keys the time will be longer such that for m combination of wireless medium key he would try all n possible keys, so he will get complexity of m multiplier n. Thus the time required to break the key, if it is possible, increases.

Chapter 4

Encryption Algorithm

Cryptography calculations assume a paramount part in data security. They might be separated into Symmetric and Asymmetric key cryptography. In Symmetric key encryption one and only key is utilized to scramble and decode information. The key ought to be conveyed before transmission between two gatherings. Key assumes an imperative part in encryption and decoding . In the event that a powerless key is utilized within the calculation then effectively information could be decoded. The extent of the key decides the quality of Symmetric key encryption. Symmetric calculations are of two sorts: piece figures and stream figures. The square figures are working on information in gatherings or squares. .Cases are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream figures are working on a solitary bit at once. Rc4 is stream figure calculation. Encryption calculations devour huge measure of figuring assets, for example, battery power, CPU time, and so forth. Deviated key (or open key) encryption is utilized to tackle the issue of key dissemination. In Asymmetric key encryption, two keys are utilized; private keys and open keys. Open key is utilized for encryption and private key is utilized for decoding (e.g Digital Signatures). Open key is known to the general population and private key is known just to the client. Preceding transmission there is no requirement for disseminating them. Hilter kilter encryption strategies are close to 1000 times slower than Symmetric methods, since they require more computational handling force.

4.1 Blowfish Algorithm

It is a standout amongst the most open space encryption calculations. Blowfish was planned in 1993 by Bruce Schneider as a quick option to existing encryption calculations. Blowfish is a symmetric key square figure that uses a 64 bit piece size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less . Blowfish is an extremely secure figure yet it is has been supplanted by Twofish and Rijndael because of its little 64 bit piece size. Blowfish is one of the quickest square figures which has created to date. Gradualness kept Blowfish from being utilized within a few provisions. Blowfish was made to permit anybody to utilize encryption free of licenses and copyrights. Blowfish has stayed in the general population space right up 'til the present time. No assault is known to be effective against it, however it experiences frail keys issue (Bruce, 1996) (Nadeem, 2005).[26]

The Blowfish calculation has numerous focal points. It is suitable and productive for fittings usage and no permit is needed. The rudimentary administrators of Blowfish calculation incorporate table lookup, expansion and XOR. The table incorporates four S-boxes and a P-show. Blowfish is a figure focused around Feistel rounds, and the configuration of the F-capacity utilized adds up to an improvement of the standards utilized within DES to furnish the same security with more excellent speed and proficiency in programming. Blowfish is a 64 bit square figure and is proposed as a swap for DES.

Blowfish is a quick calculation and can scramble information on 32-bit chip at a rate of one byte each 26 clock cycles. The calculation is minimal and can run in under 5k of memory.[24]

4.2 Methodology

A few specifications of Blowfish calculation are as takes after

- A 64 bit square figure with a variable key length.
- There is a P-show and four 32-bit S-boxes. The P-cluster holds 18 of 32-bit subkeys, while every S-box holds 256 sections.
- The calculation comprises of two parts: a key-extension part and an information encryption part.

- Key extension changes over a key of at most 448 bits into a few subkey clusters totaling 4168 bytes.
- The information encryption happens through a 16-round Feistel system. Each one round comprises of a key-subordinate stage, and a key and information subordinate substitution.
- All operations are Xors and increments on 32-bit words.
- The information is a 64 bit information component.[25]

The calculation handled is as takes after :

- Initialize P show and S boxes with Hexadecimal digits of Pi. thing XOR P-exhibit with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key).
- Use the above technique to encode the all-zero string.
- This new yield is P1 and P2.
- Encrypt the new P1 and P2 with the modified subkeys.
- This new yield is presently P3 and P4.
- Repeat the above steps until we get all the components of P exhibit i.e P1, P2.

The Blowfish algorithm is described as:

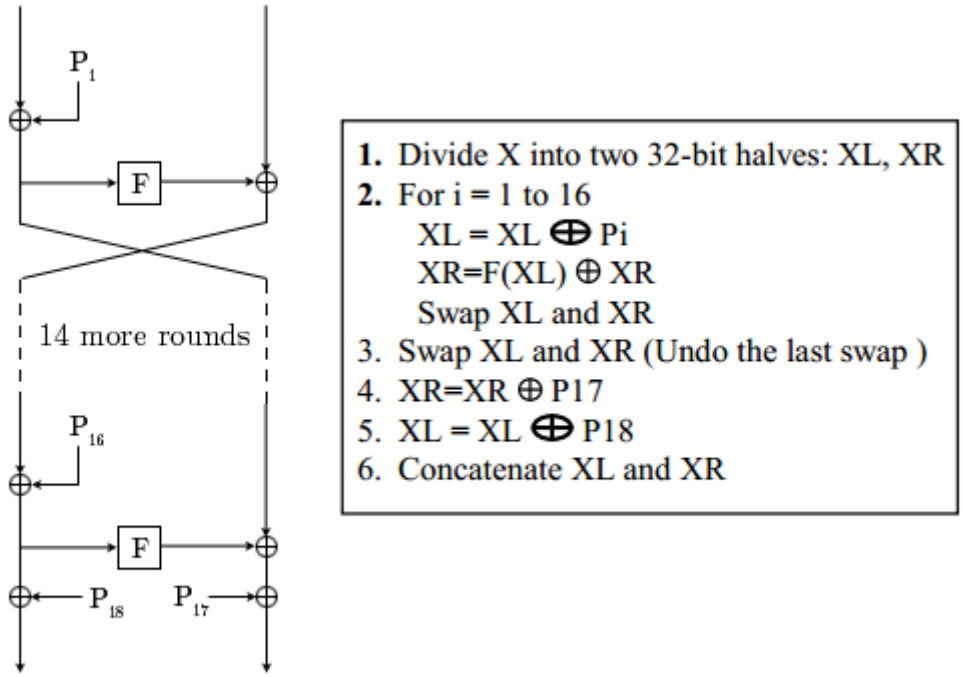

Figure 4.1: Blowfish Encryption Algorithm

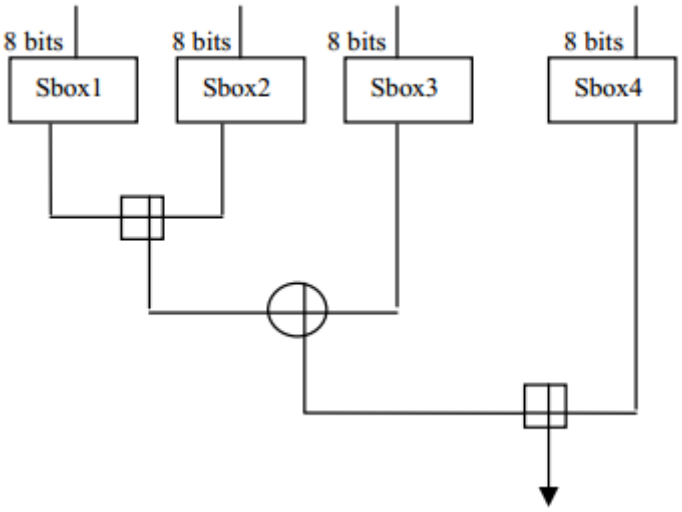

Figure 4.2: The F function
[22]

4.3 Comparing to different algorithms

Paper gives a definite investigation of the most well known symmetric key encryption calculation that is Blowfish and talked about its preferences. Taking into account the profits of Blowfish calculation we have proposed and executed another methodology to further upgrade the current calculation to attain better brings about terms of parameters,

for example, Encryption time, Decryption time and Throughput. The striking characteristic of altered blowfish encryption calculation is that for the same data plaintext the figure content produced at each one time will be distinctive. This is on account of each time another irregular number gets created and this subsequently gives distinction in the provision of F capacity over each one round. The playing point of distinctive figure content produced for the same info is it will enormously upgrade the security part of blowfish calculation. The second greatest preference of this methodology is that it is less tedious as contrasted with blowfish calculation. The above results plainly show that the encryption time and decoding time for adjusted blowfish calculation is just about half to that of blowfish calculation.[26]

Algorithms	**Key-Sizes**	**Block-Sizes**	**Nu. of Round**
DES	56-bits	64-bits	16
3DES	112 or 168-bits	64-bits	48
AES	128, 192 or 256-bits	128-bits	10,12 or 14
Blowfish	32-448 bits	64-bits	16

Table 4.1: Number of rounds in Different Algorithms
[24]

Sr. No.	**Algorithms**	**Key Size**	**Power Consumption (mW)**
1	Blowfish	128	29.86
2	AES	128	2000
3	IDEA	128	58
4	Rijndael	128	82

Table 4.2: Power Analysis in Different Algorithms
[25]

Input Size (KB)	**3DES**	**DES**	**CAST-128**	**BLOWFISH**	**IDEA**	**RC2**
51	120	42	45	16	49	14
249	170	61	48	31	69	45
501	232	82	73	62	101	67
911	381	120	91	70	135	73
5601	1240	490	450	302	641	371
11110	2705	1020	740	601	1150	750
12100	3001	1071	790	678	1210	801
Throughput (MB/Sec)	3.88	10.57	13.64	17.34	9.09	14.39

Table 4.3: Throughput with respect to other algorithms
[23]

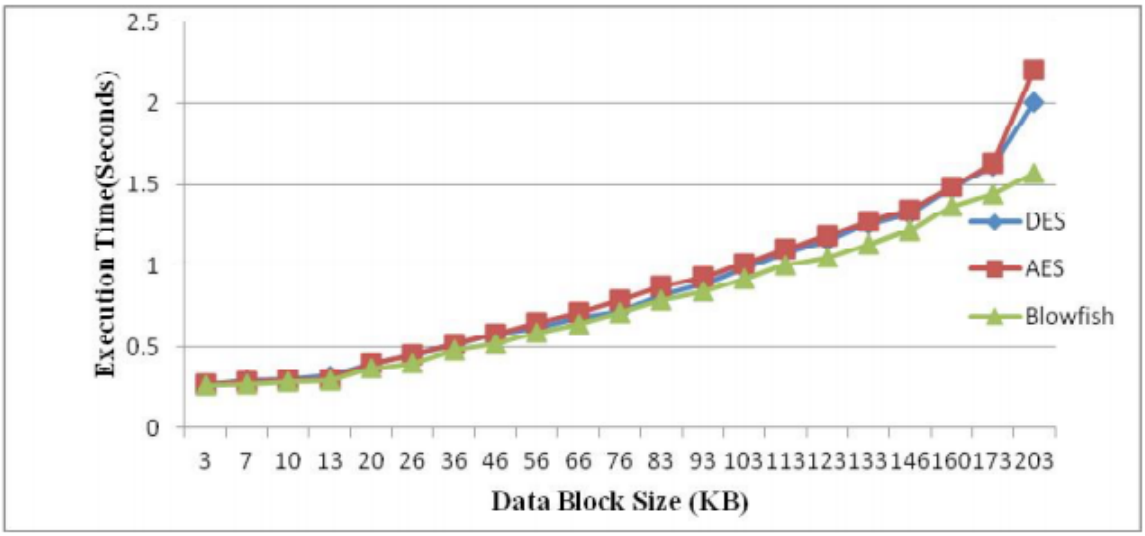

Figure 4.3: Execution Time with respect to other algorithms [26]

Chapter 5

Implementation

5.1 Android Application

In order to implement the application, the application was designed in such a way that when anybody opens it, the user is prompted for a username and password.

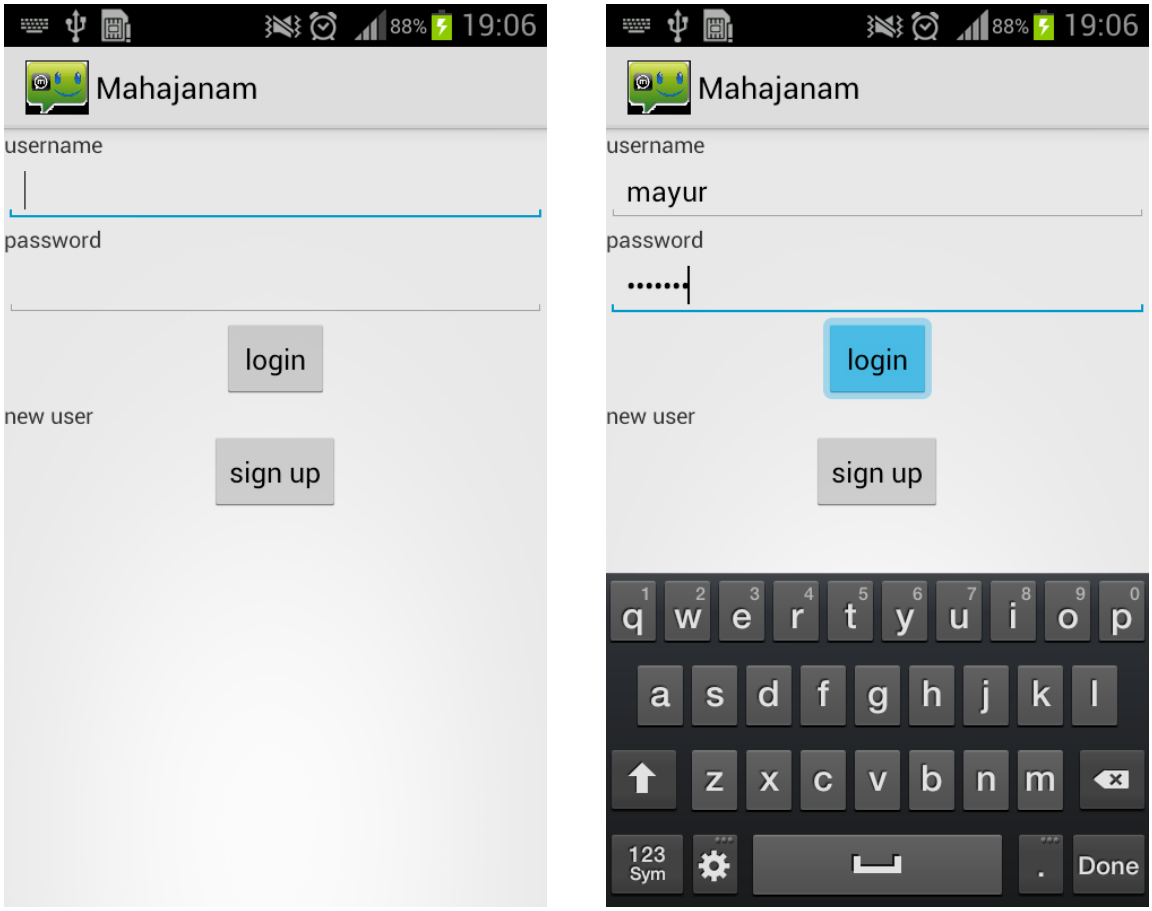

Figure 5.1: Prompting for details of username and password

When correct username and password is entered. A welcome screen appears. Welcome screen having some buttons, waiting for user needed action. It has two functionalities,

- Sending secure SMS
- Bluetooth Chat

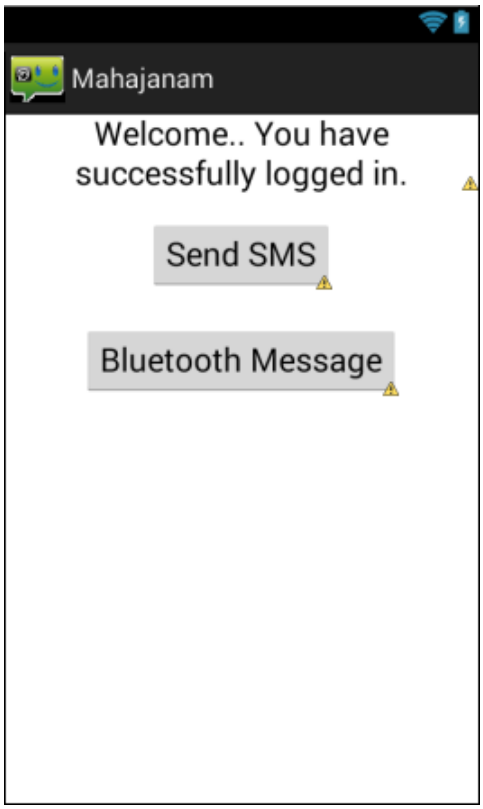

Figure 5.2: Welcome screen waiting for user's choice

But when wrong input password or username is entered, then it won't proceed further. On first installation the activation key will be provided through which username and password canl be generated. Using that registration key multiple users on the same device can be created.

5.2 Send SMS

When clicking on Send SMS, A new window appears in which the field for phone number, message and encrypted message are present.

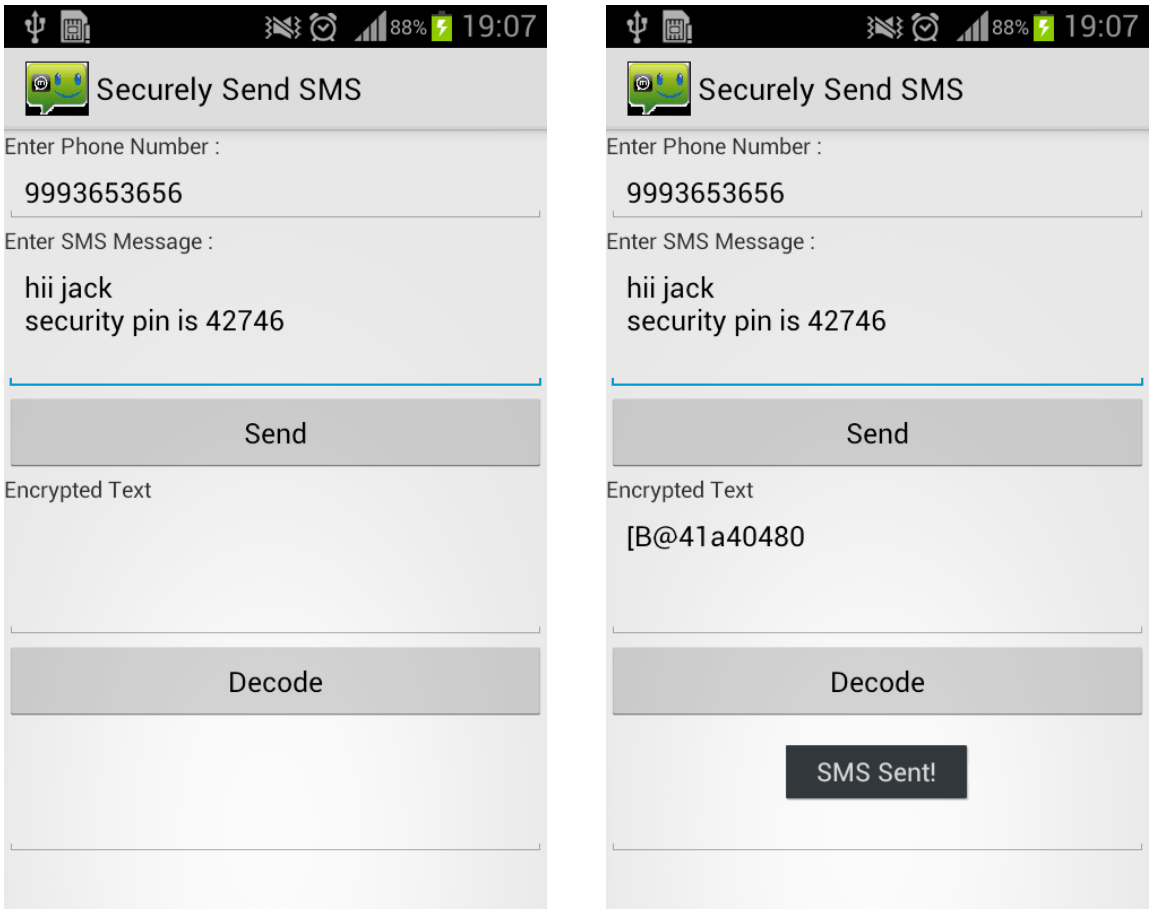

Figure 5.3: Asking for phone nu. and message. when message is send and decrypted

The phone number is the field in which the contact number of the receiver is entered. The Message field contains the message we want to send securely. The encryption field will be shown when the message is to be sent. Encryption field shows the actual message which is sent to receiver.

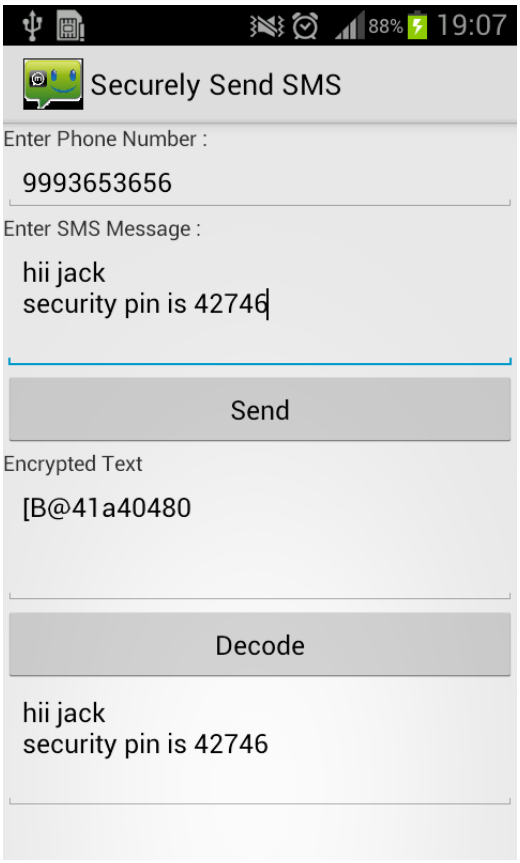

Figure 5.4: Decryption of message at receiver end

At the receiver end the message is to be decrypted by the user, so that he would be able to read the message.

5.3 Bluetooth Chat

When clicking on Bluetooth chat, A new windows appears in which blank screen appears. On the right-upper corner stated that "not connected". It means no bluetooth device is connected to the phone. When clicking on menu button, then it pop-ups two options :

- Make Discoverable
- Connect a device

When clicking on Make discoverable option. It asks for a permission to make our device visible to other devices for 300 seconds.

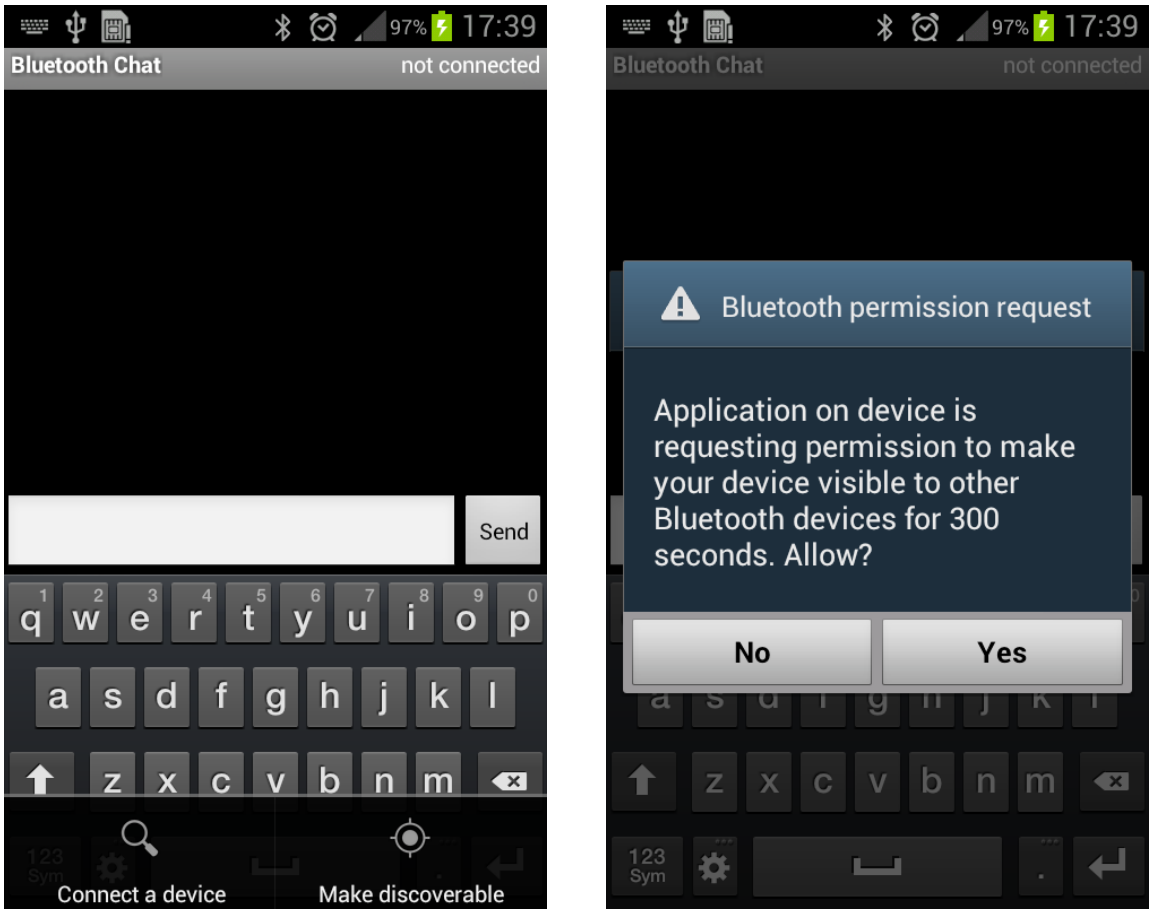

Figure 5.5: Menu options and prompting for Bluetooth permission for visibility

On the other hand, other phone who want to communicate via bluetooth searches for devices by clicking on Connect a device. When user click on connect a device, a pop menu appears having a list of bluetooth devices previously paired and newly searched devices. Out of this list user can choose with whom he wants to be connected.

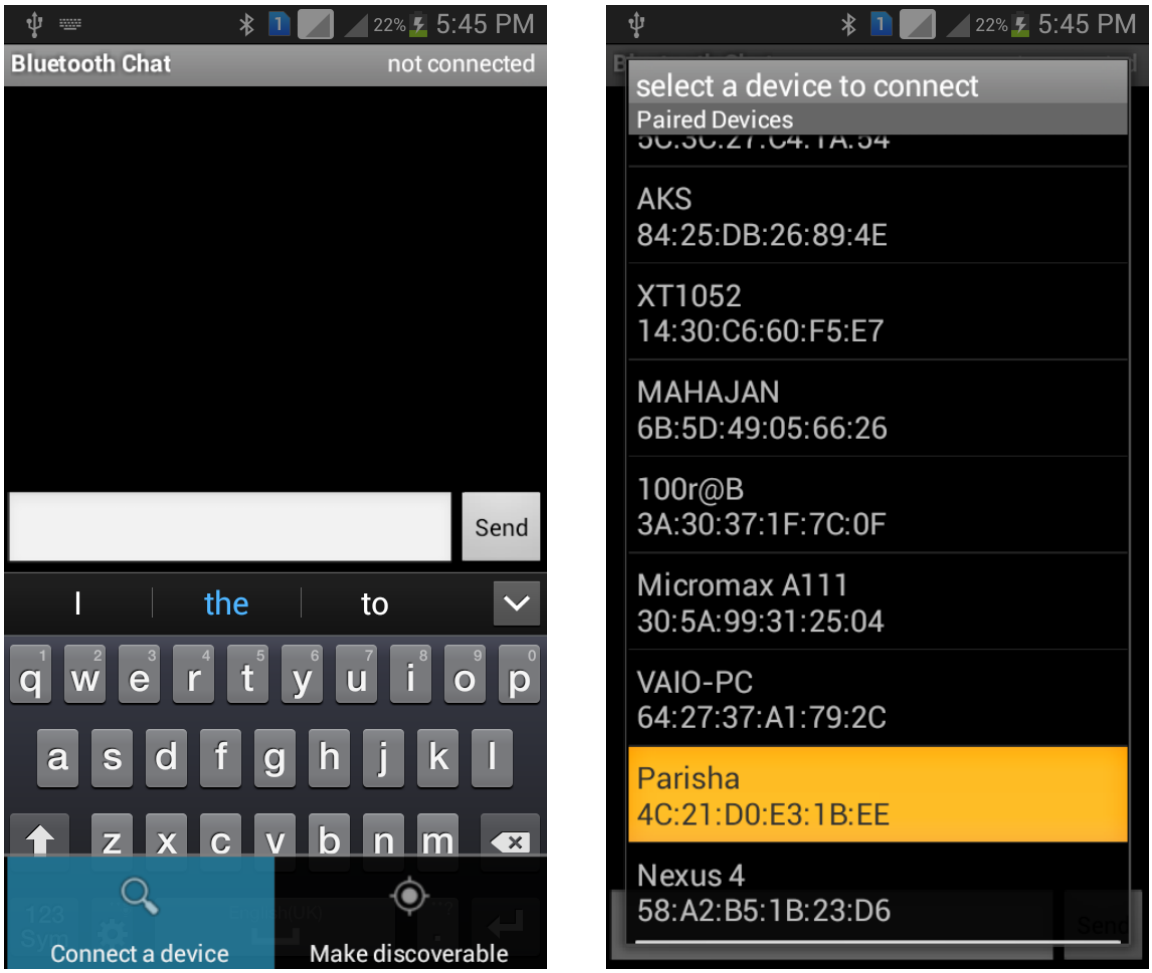

Figure 5.6: Menu options and pop up list of bluetooth devices

When choosing a user to communicate, then also it pop up a Bluetooth pairing request for that device from user's device. When this passkey on both the end is same then user can click on pair button.

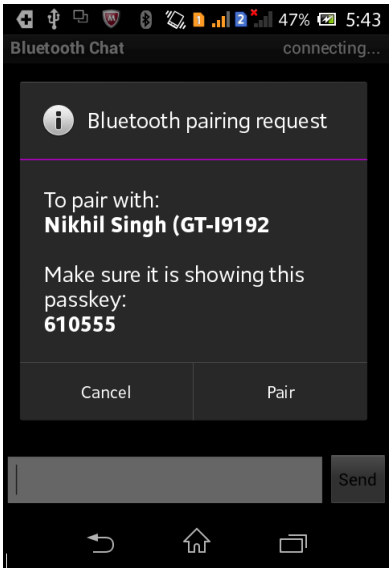

Figure 5.7: Prompting for passkey

When pairing on both the Mobile phone is done then both the phone gets connected.

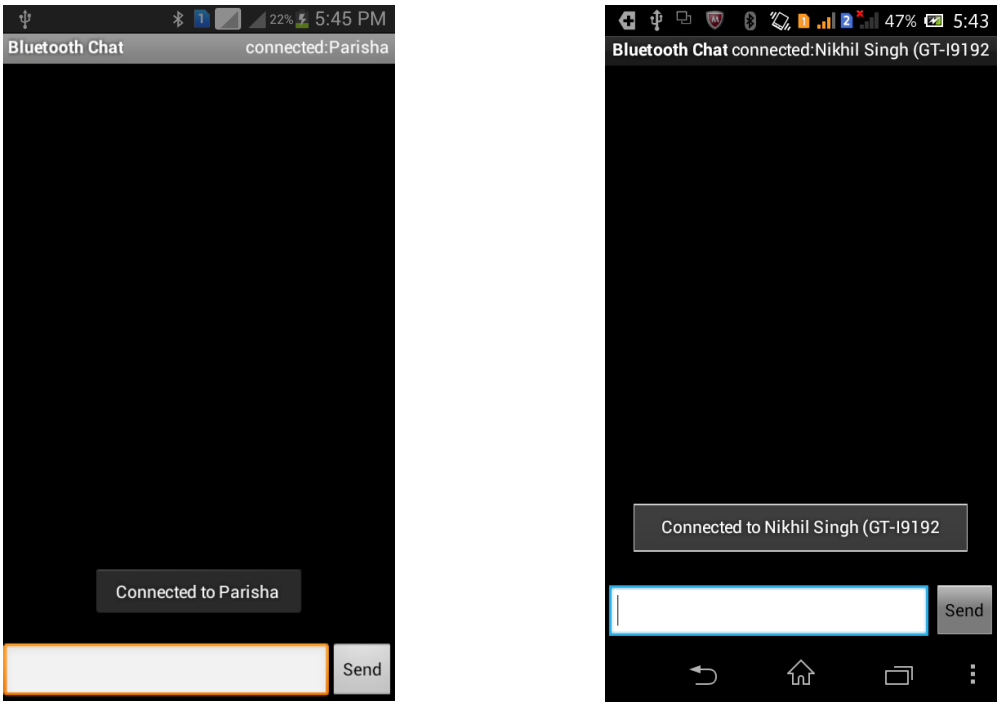

Figure 5.8: Both the device get paired with each other

Once devices via bluetooth are connected, they can communicate securely. The messages transferred between the users are shown below:

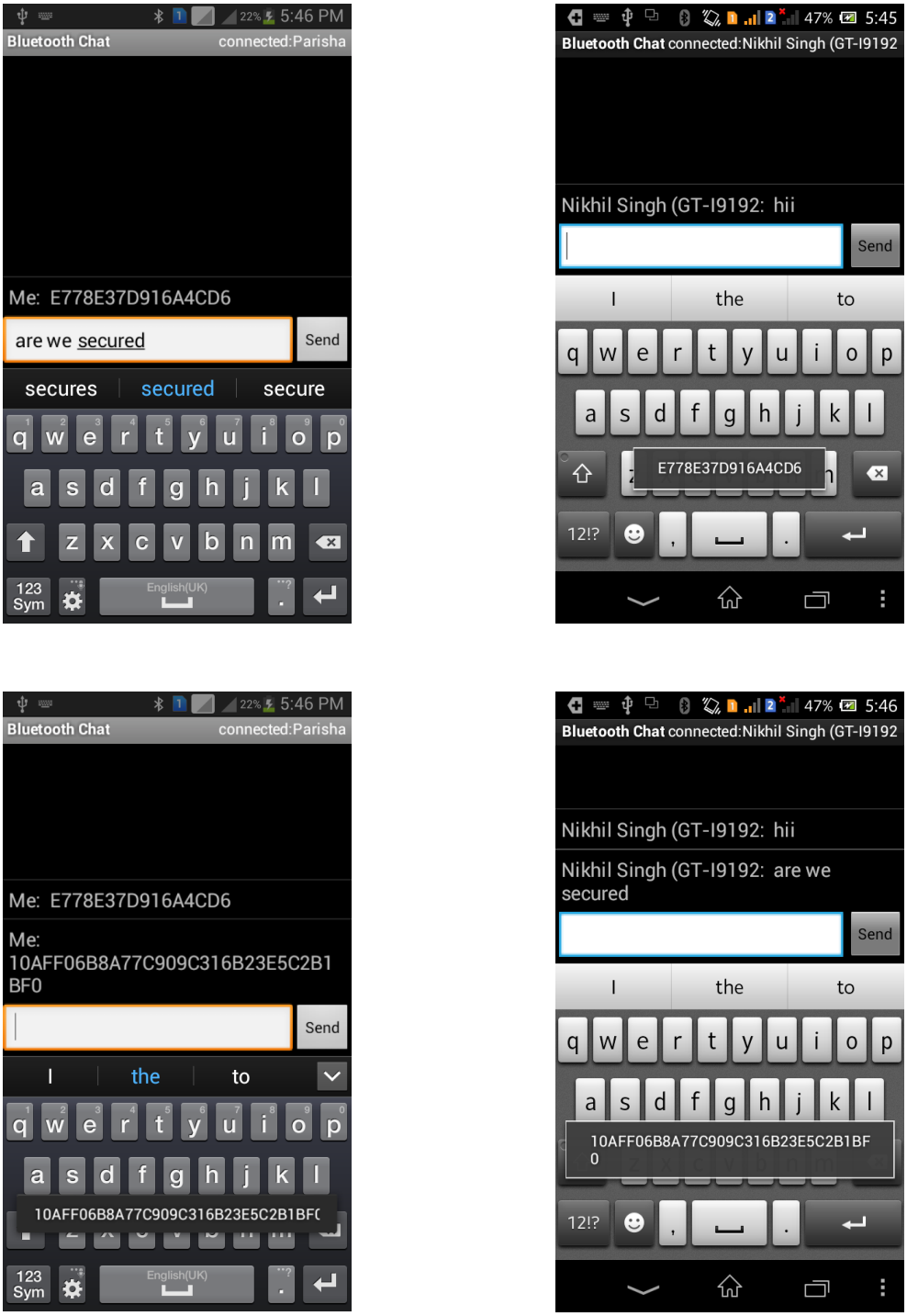

Figure 5.9: Communication between the users via secure bluetooth messages

Chapter 6

Conclusion and Future Work

In this work an android application is presented, through which we can securely send our SMS and also securely communicate via bluetooth. A GSM SMS is encrypted first and then it is allowed to be transmitted over network, at receiver end the messages is only decrypted by our application. Thus SMS remains secure and confidential.

In bluetooth chat system, bluetooth permits one device to be discoverable at certain time only so that after that time period no other device connect to it. Once the device is paired with secure pass key then it is stored in its device paired list, so while connecting next time we need not other device setting to be discoverable. It will be connected directly without asking for pass key to be matched.

In this application we are encrypting everything using same key, thus for future purspective, application will be made in such a way that every connection will share a random key and that session will use that key for encryption and decryption.

Bibliography

[1] Dorothy Skierkowski, Rebecca M. Wood *Computers in Human Behavior*
Department of Psychology, Central Connecticut State University, New Britain, CT 06053, United States *, 23 December 2011*

[2] Amanda Lenhart *Teens, Smartphones & Texting*
Pew Research Centers Internet & American Life Project, 1615 L St., NW Suite 700, Washington, D.C. 20036 *, May 12, 2010*

[3] Telecom Source Consulting Inc. *SMS*
SMS The Telecom Source *2008*

[4] Dan Veeneman *Cellular Cryptography.*
Sattellite Times *, December 26, 2009*

[5] David Margrave *GSM Security and Encryption*
George Mason University,

[6] Karsten Nohl, Kevin J. O'Brien *Cellphone Encryption Code Is Divulged.*
Available at: New York Times. *, December 28, 2009*

[7] Alex Biryukov, Adi Shamir, David Wagner *Real Time Cryptanalysis of A5/1 on a PC.*
Available at: Fast Software Encryption Workshop 2000, New York City *27 April 2000*

[8] Elad Barkhan, Eli Biham and Nathan Keller *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication.*
Available at: Department of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel, 2006-2007

[9] Steve Dhulton *Intercepting GSM traffic.*
Washington D.C., Black Hat Briefing *, February 2009*

[10] Elad Barkan, Kfar Sirkin (IL), El Biham, Haifa (IL) *CRYPTANALYSIS METHOD AND SYSTEM.*
Patent N0.: US 8,295,477 B2, Date of Patent: *Oct. 23, 2012

[11] Khaled Merit and Abdelazziz Ouamri, *Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm.*
International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012

[12] Majithia Sachin, Dinesh Kumar, *Implementation and Analysis of AES, DES and Triple DES on GSM Network.*
IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010

[13] F.J. Gonzalez-Castano, J. Vales-Alonso, J.M. Pousada- Carballo, F.I. de Vicente, and M.J. Fernandez-Iglesias, *Real-Time Interception Systems for the GSM Protocol* IEEE Transactions on Vehicular Technology, Vol.51, No.5, pp. 904-914 *, Sept. 2002*

[14] J.R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, *Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards* IEEE Symposium on Security and Privacy (S&P'02), pp.31-41, 2002.

[15] G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Shenoi, *Securing SS7 Telecommunications Networks* IEEE Workshop on Information Assurance and Security, pp.273-278, *June 2001.*

[16] V. Bocan, and V. Cretu, *Mitigating Denial of Service Threats in GSM Networks* 1st IEEE International Conference on Availability, Reliability and Security (ARES'06), *April 2006.*

[17] Copyright ©Nokia Networks *GSM Air Interface & Network Planning.*
Available at: TC Finland *, January, 2002*

[18] M. Toorani, and A. A. Beheshti Shirazi, *Solutions to the GSM Security Weaknesses* 2nd International Conference on Next Generation Mobile Applications, Services,

and Technologies (NGMAST'08), pp.576-581, University of Glamorgan, Cardiff, UK, Sep. 2008 [DOI 10.1109/NGMAST.2008.88]. *, Sep, 2009*

[19] European Telecommunications Standards Institute. Digital cellular Telecommunications system (Phase 2+); *Security mechanisms for the SIM Application Toolkit*; Stage 1. GSM 02.48 version 6.0.0 Release 97. *April 1998.*

[20] N.N. Katugampala, K.T. Al-Naimi, S. Villette, and A.M. Kondoz,*Real-time End-to-end Secure Voice Communications Over GSM Voice Channel*, 13th European Signal Processing Conference (EUSIPCO'05), Turkey, *Sep. 2005.*

[21] A.B. Rekha, B. Umadevi, Y. Solanke, and S.R. Kolli, *End-to-End Security for GSM Users*, IEEE International Conference on Personal Wireless Communications, pp.434-437, *Jan. 2005.*

[22] Monika Agrawal, Pradeep Mishra *A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm*
Available at: (IJEAT) ISSN: 2249 8958, Volume-1, Issue-6, August 2012

[23] Md Imran Alam, Mohammad Rafeek Khan *Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography*
Available at: (IJEAT) ISSN: 2277 128X, Volume 3, Issue 10, October 2013

[24] Pratap Chandra Mandal *Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish*
Available at: ISSN: 2229 371X, Volume 3, No. 8, August 2012 Journal of Global Research in Computer Science

[25] Sweta K. Parmar, Prof. K. C. Dave *A Review on Various Most Common Symmetric Encryptions Algorithms*
Available at: IJSRD, Vol. 1, Issue 4, 2013 — ISSN (online): 2321-0613

[26] Nagesh Kumar, Jawahar Thakur, Arvind Kalia *PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS: DES, AES and BLOWFISH*
Available at: An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4

Appendices

Appendix A

Implementation Plateform

The platforms which are required to implement include:

- **Android SDK(Software Development Kit):** To develop application program, we will require Eclipse IDE, Android plugins, Android Emulator.

- **A linux or MAC system:** To build Android OS itself. i.e. custom roms, we will require Ubuntu LTS of 12.04 or later version with 16 GB RAM and 30 GB harddisk space.

Appendix B

Applications Used

The other Android applications which are used for guidence and other type of help, are as follow :

- **SmsEncoder**
- **SampleBluetooth**
- **SendSMS**
- **BroadcaseReceiverNewSMS**
- **AutoCompleteEditText**
- **ContentProviderEmail**
- **DataEncryption**
- **SMS_APP**
- **RedPhone**
- **SpyCallRecorder**
- **MythDroid**
- **CSipSimple**
- **SdkControllerApp**