Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.379 – 392

RESEARCH ARTICLE

Evaluation of Authentication and Ciphering Algorithms in GSM

Payal, Vikram Nandal
M.Tech Student, Department of CSE, R.N. College of Engineering & Management
Assistant Professor, Department of CSE, R.N. College of Engineering & Management
payalgaurengg1@gmail.com, vikramcse@live.com

Abstract: The Mobile communications has experienced a great acceptance among the human societies. It has influenced and revolutionized different aspects of the human life. With a mobile handset, anyone can be accessed anywhere. This paper briefly presents the most important security flaws of the GSM network and its transport channels. It also provides some practical solutions to improve the security of currently available GSM systems. The Mobile communications has experienced a great acceptance among the human societies. It has influenced and revolutionized different aspects of the human life. With a mobile handset, anyone can be accessed anywhere.
Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world, accounting for 70% of the world's digital mobile phones. GSM service started in 1991. According to a press release by the GSM Association in May 2001; there are more than half a billion GSM mobile phones in use in over 168 countries today.

Keywords: GSM, HSCSD, GPRS, EDGE, UMTS

I. INTRODUCTION

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership.

Cellular is one of the fastest growing and most demanding telecommunications applications. Throughout the evolution of cellular telecommunications, various systems have been developed without the benefit of standardized specifications. This presented many problems directly related to compatibility, especially with the development of digital radio technology. The GSM standard is intended to address these problems.

The GSM has experienced gradual improvements that leaded to several versions such as GSM1800, HSCSD (High Speed Circuit Switched Data), EDGE (Enhanced Data rates for GSM Evolution), and GPRS (General Packet Radio Service). The GSM improvements are continued to 3G systems such as UMTS. It is believed that the GSM has many inherent security flaws and some of its security flaws are addressed in the upper generations such as UMTS. However, many operators especially in the developing countries are still using the traditional GSM network that succumbs to several security flaws.

II. GSM ARCHITECTURE

The GSM network can be divided into three parts. The Mobile Station carries the subscriber; the Base Station Subsystem controls the radio link with the Mobile Station; the Network Subsystem, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. Not shown is the Operations and Maintenance center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the air interface or radio link. The Base Station Subsystem and the Network Subsystem are also called the fixed network.

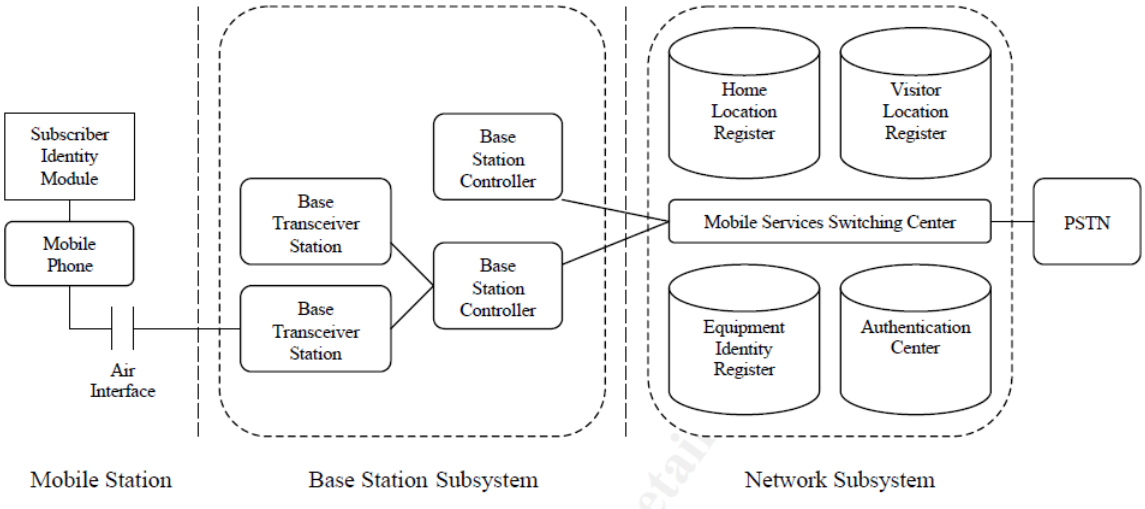


Fig. 1: GSM Architecture

Mobile Station:

The mobile station (MS) consists of mobile equipment and a Subscriber Identity Module (SIM) card. The most common mobile equipment is the mobile phone. By inserting the SIM card into a cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services. The mobile equipment uniquely identifies the International Mobile Equipment Identity (IMEI). The SIM is like a key, without which the mobile phone can't function. The SIM card stores the sensitive information such as the International Mobile Subscriber Identity (IMSI), Ki(a secret key for authentication), and other user information. All this information may be protected by personal identity number (PIN).

The SIM card itself is a smart card and is in accordance with the smart card standard (ISO 7816-1, -2). It is capable of storing personal phone numbers and short messages. It also stores security related information such as the A3 authentication algorithm, the A8 ciphering key generating algorithm, the authentication key (Ki) and IMSI. The mobile station stores the A5 ciphering algorithm.

Base Station Subsystem (BSS):

The role of the Base Station Subsystem (BSS) is to connect the user on a mobile phone with other landline or mobile users. The Base Transceiver Station (BTS) is in direct contact with the mobile phones via the air interface and can be thought of as a complex radio modem. The Base Station Controller (BSC) is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manages radio frequencies allocated for the calls through the BTS.

Network Subsystem (NSS):

It is a complete exchange, capable of routing calls from a fixed network via the BSC and BTS to an individual mobile station. The Mobile Services Switching Center (MSC) interconnects the cellular network with the Public Switched Telephone Network (PSTN). The MSC also serves to co-ordinate setting up calls to and from GSM users.

Mobile services Switching Center (MSC):

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem.

Home Location Register (HLR):

The Home Location Register (HLR) is a database of a mobile network in which information of all mobile subscribers is stored.

Visitor Location Register (VLR):

The Visitor Location Register (VLR) is a database in a mobile communications network associated to a Mobile Switching Centre (MSC). The VLR contains the exact location of all mobile subscribers currently present in the service area of the MSC.

Equipment Identity Register (EIR):

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved.

Authentication Center (AUC):

Authentication Center where all authentication algorithms are defined. The Authentication Centre (AUC) is a function in a GSM network used for authenticating a mobile subscriber that wants to connect to the network. Authentication is done by identification and verification of the validity of the SIM.

Temporary Mobile Subscriber Identity (TMSI):

The Temporary Mobile Subscriber Identity (TMSI) is a temporary identification number that is used in the GSM network instead of the IMSI to ensure the privacy of the mobile subscriber and is provided by the VLR associated with that MSC.

III. SECURITY MODEL (GSM)

Purpose of GSM Security:

As we know that security is the essential feature in any service. Hence, GSM network also follows certain level of security in the services which it provides. As we know that GSM uses radio communications for its mobile subscribers' this makes it a sensitive service for the persons who are unauthorized users and are accessing through the different mobile stations. These unauthorized users pretend that they are usual subscribers' and listen to the private conversations which are being exchanged on the radio paths.

Hence, there are mainly two security purposes which are kept in mind when it is concerned of the GSM network:-

First of all, to protect the Accessibility to the mobile services and secondly to prevent disclosure of any crucial information/data at the radio path to achieve the privacy regarding that particular data.

Security Architecture of the GSM:

The security architecture of GSM was originally intended to provide security services such as anonymity, authentication, and confidentiality of user data and signaling information. The security goals of GSM are as follows:

- Authentication of mobile users for the network,
- Confidentiality of user data and signaling information,
- Anonymity of subscriber's identity,
- Using SIM (Subscriber Identity Module) as a security module.

The Mobile Station (MS) consists of the Mobile Equipment (ME), and the SIM card. The SIM is a cryptographic smart card with the GSM specific applications loaded onto it. As a smart card, it has some inherent security functions specified to smart cards. Its operating system and chip hardware have several security attributes. SIM includes all the necessary information to access the subscriber's account. IMSI and Ki are stored on every SIM. IMSI is the International Mobile Subscriber Identity with at most 15 digits uniquely devoted to every mobile subscriber in the world. Ki

(Individual subscriber authentication Key) is a random 128-bits number that is the root cryptographic key used for generating session keys, and authenticating the mobile users to the network. Ki is strictly protected and is stored on the subscriber's SIM, and AuC. The SIM is itself protected by an optional Personal Identification Number (PIN). Each user is requested to enter the PIN unless this feature is deactivated by the user. After a number of invalid attempts that is usually 3 times, the SIM locks out the PIN, and the PUK (PIN UnlocK) is then requested. If the PUK is also incorrectly entered for a number of times that is usually 10 times, the SIM refuses local accesses to its privileged information and authentication functions, and makes it useless.

Authentication and confidentiality of user data are in deposit of the secrecy of IMSI and Ki. With disclosure of such numbers, anyone can impersonate a legitimate user. A3 and A8 algorithms are also implemented on every SIM. This means that each operator can determine and change such algorithms independent of other operators and hardware manufacturers. Therefore, the authentication will work when a user is roaming on other countries or operators since the local network will query the HLR of the home network for the results and does not need to know the A3/A8 algorithm of the home network. A3 is mainly used for authenticating users to the network while A8 is used for generating the session key of encryption Kc. The network sends a random challenge to the user so that SIM produces Kc and SRES. After user authentication, the network can order the phone to start the encryption by using the generated session key Kc. The cryptographic algorithms are implemented on the hardware of mobile phones. The network can choose from up to 7 different encryption algorithms (or the mode of no ciphering) but it should choose an algorithm that is implemented on the phones. A class mark message has been earlier specified the phone's capabilities to the network. Three algorithms are generally available: A5/1, A5/2, and A5/3. A5/1 and A5/2 are two stream ciphers originally defined by the GSM standards. A5/1 is stronger but it is subject to export control and can be used by those countries that are members of CEPT. A5/2 is deliberately weakened to be deployed by the other countries. The use of such algorithms is controlled by the GSM Memorandum of Understanding (MoU). A5/3 is a block cipher based on the Kasumi algorithm that is defined by the 3GPP at 2002 and can be supported on dual-mode phones that are capable of working on both 2G and 3G systems. The GSM authentication, session key generation, and encryption processes are depicted in the Figure.

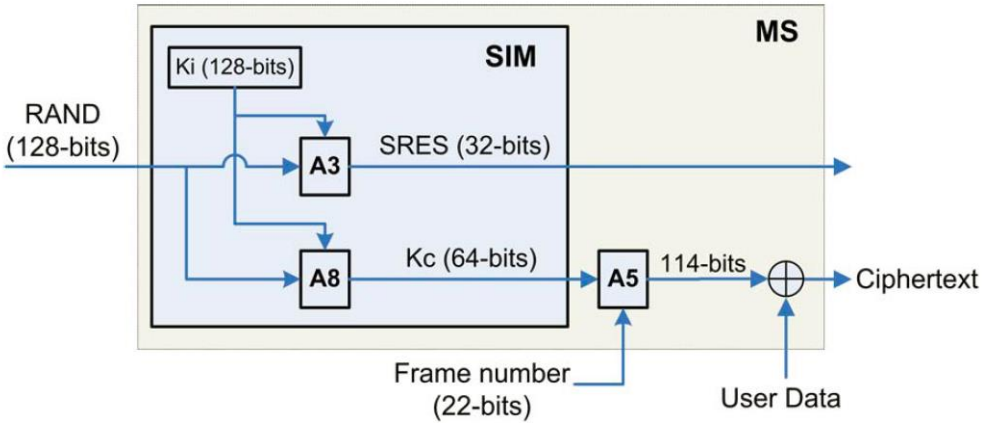


Fig. 2: GSM Authentication, Session key generation and Ciphering

SIM includes all the necessary information to access the subscriber's account. IMSI and Ki are stored on every SIM. Authentication and confidentiality of user data are in deposit of the secrecy of IMSI and Ki. A3 and A8 algorithms are also implemented on every SIM. A3 is mainly used for authenticating users to the network while A8 is used for

generating the session key of encryption Kc. After user authentication, the network can order the phone to start the encryption by using the generated session key Kc.

IV. PROTOCOL WALKTHROUGH

When a MS requests access to the network, the MSC/VLR will normally require the MS to authenticate. The MSC will forward the IMSI to the HLR and request authentication Triplets.

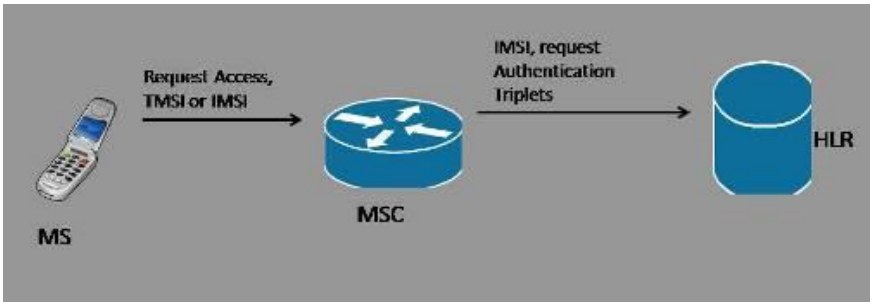


Fig. 3

When the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and belongs to the network. Once it has accomplished this, it will forward the IMSI and authentication request to the *Authentication Center* (AuC).

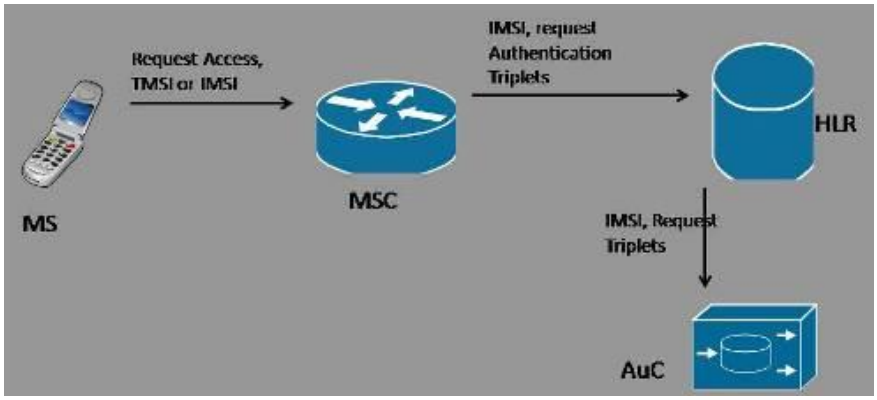


Fig. 4

The AuC will use the IMSI to look up the Ki associated with that IMSI. The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The Ki is only stored on the SIM card and at the AuC. The Auc will also generate a 128-bit random number called the RAND.

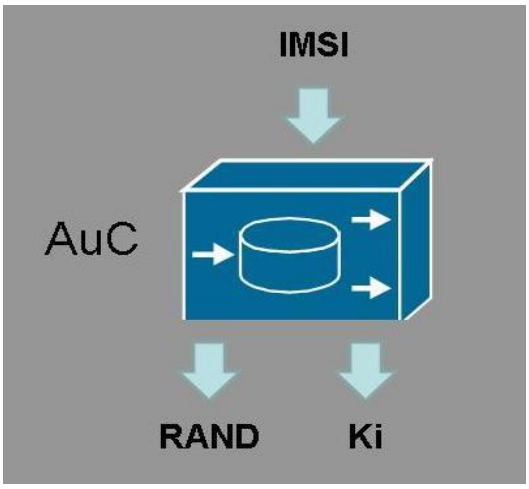


Fig. 5

The RAND and the Ki are inputted into the A3 encryption algorithm. The output is the 32-bit *Signed Response* (SRES). The SRES is essentially the "challenge" sent to the MS when authentication is requested.

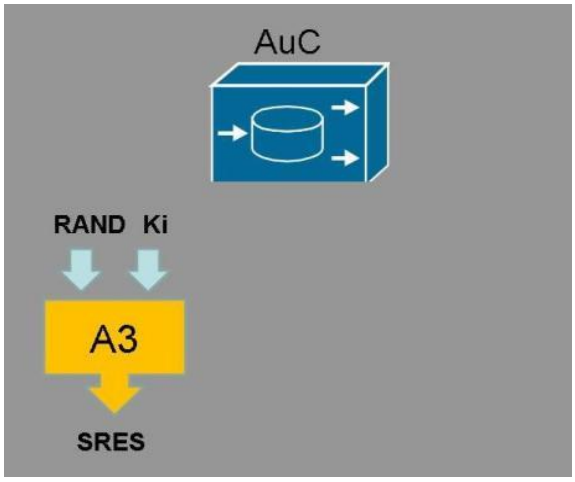


Fig. 6

The RAND and Ki are input into the A8 encryption algorithm. The output is the 64-bit Kc. The Kc is the ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.

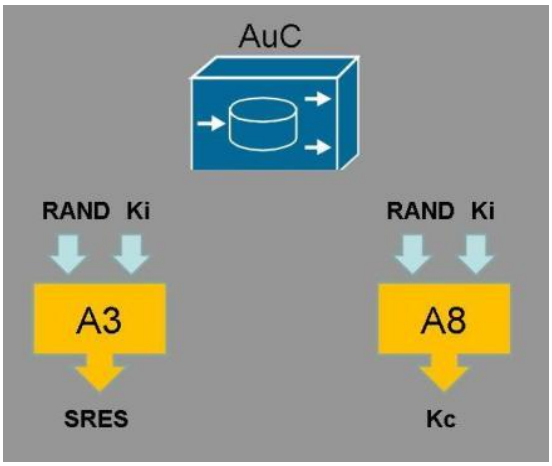


Fig. 7

The RAND, SRES, and Kc are collectively known as the *Triplets*. The AuC will generate Triplet and send them to the requesting MSC/VLR. It should be noted that a set of triplets is unique to one IMSI; it cannot be used with any other IMSI.

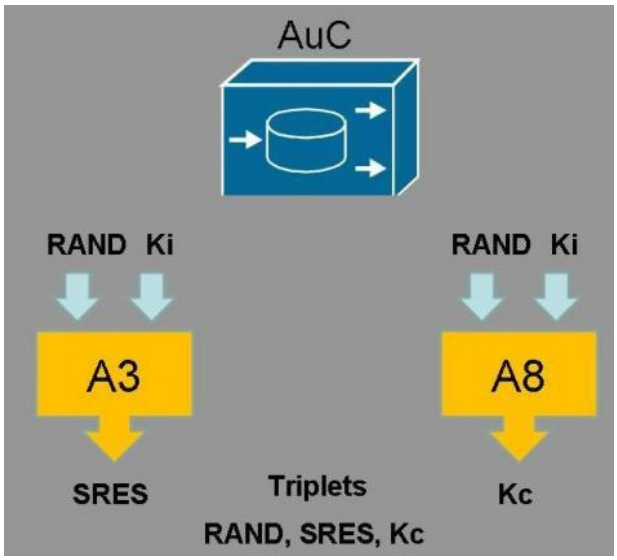


Fig. 8

Once the AuC has generated the triplets (or sets of triplets), it forwards them to the HLR. The HLR subsequently sends them to the requesting MSC/VLR.

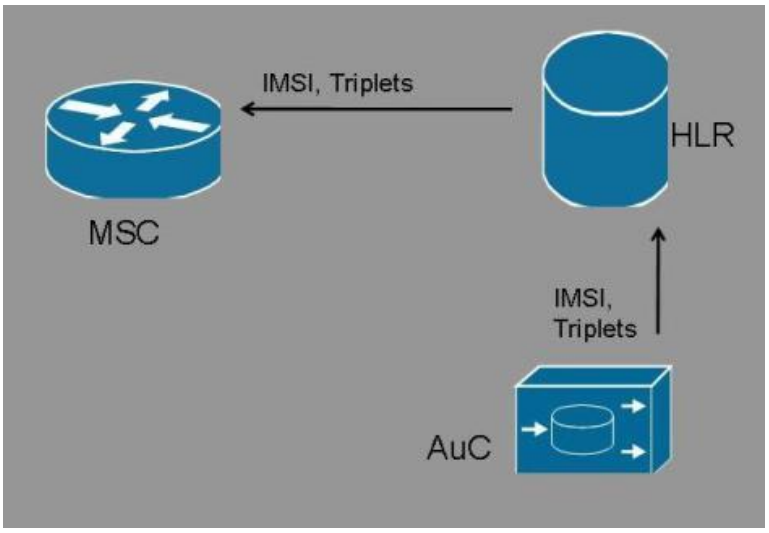


Fig. 9

The MSC stores the Kc and the SRES but forwards the RAND to the MS and orders it to authenticate.

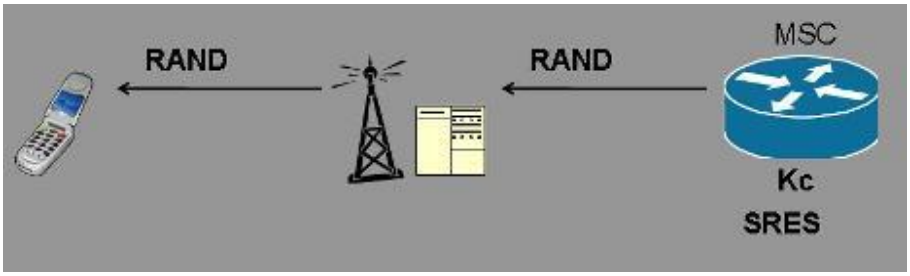


Fig. 10

The MS has the Ki stored on the SIM card. The A3 and A8 algorithms also reside on the SIM card. The RAND and Ki are inputted into the A3 and A8 encryption algorithms to generate the SRES and the Kc respectively.

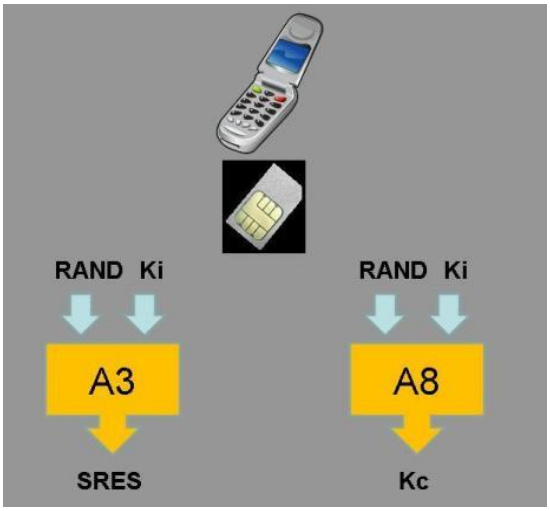


Fig. 11

The MS stores the Kc on the SIM card and sends the generated SRES back to the network. The MSC receives the MS generated SRES and compares it to the SRES generated by the AuC. if they match, then the MS is authenticated.

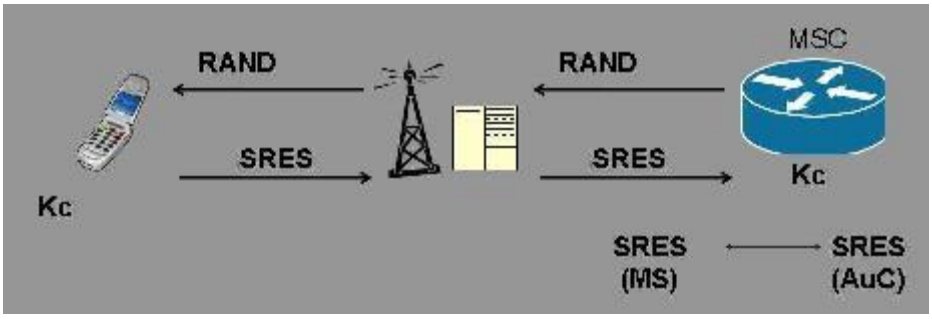


Fig. 12

V. Implementation of the System & Algorithm

GSM algorithms for authentication and encryption are strictly confidential and not publicly available. Hence, to achieve authentication and encryption a model has been defined. It will be a client server application communicating via TCP sockets. The server shall handle multiple clients simultaneously. The client and server applications are configurable via command line arguments.

5.1 Implementation of the system:

5.1.1 Assumptions:

- The application shall be there on MS, BTS ,MSC and HLR
- MS will be simulated using client on Linux.
- Multiple clients (MS) shall connect to the server (MSC).
- Concurrent Server will do authentications with the involvement of MSC and HLR.
- BTS will also be simulated using client on Linux.

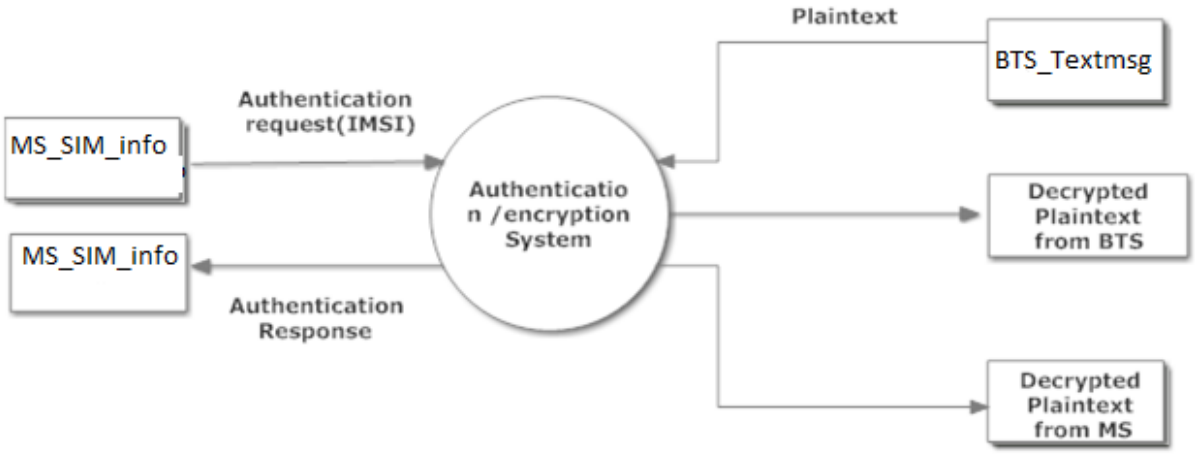
UDP can also be used instead of TCP but TCP is preferred because:

- A TCP Socket is a**connection oriented protocol**. This simply means that we make a connection between two machines and send data between the two computers much like we are writing to a file on one side, and reading from a file on the other.

- This connection is **reliable and ordered**, meaning that all data you send is guaranteed to arrive at the other side in the same order that you wrote it. It also a stream of data, meaning that TCP takes care of splitting up your data into packets and sending those across the network for us.

5.1.2 Authentication:

- Authentication is required in every mobile radio system
  - ✓ To establish the authenticity of a user/equipment
  - ✓ Establish whether the user is allowed to access the service
- Authentication consists of a challenge and a response
  - ✓ Network provides a challenge in form of a random number RAND
  - ✓ Response SRES is derived based on algorithm A3 from challenge (RAND), authentication key K_i and IMSI
  - ✓ MS replies to challenge by sending SRES back to network, which then compares MS's SRES with its own SRES .



Algorithm for Authentication and Ciphering:

A3 Algorithm:

- **What this function is Doing:**
  - This function receives random number (RAND), authentication key(Ki) .
  - Generate Signed Response (SRES) at MSC_authentication_server for the purpose of authentication of MS_Client.

- **Who is calling this function:**
  - triplet_request_to_auc

- **Pseudo Code**

Local Variablesi=0,j=Ki_LENGTH/2

Start SRES_generation_A3_algo

Call log_function to write to Log file

1. Read random number (RAND) and Ki as parameters
2. If error in reading inputs then

Call log_fiunction to write to Log file

Return 2

Call log_fiunction to write to Log file

3. Repeat steps 4 and 5 until i > RAND_LENGTH/2 and j > Ki_LENGTH
4. Ex-Or RAND[i] and Ki[j]
5. Store it in lhs[ ]
6. j=0

Call log_fiunction to write to Log file

7. Repeat steps 8 and 9 until i > RAND_LENGTH and j > Ki_LENGTH/2
8. Ex-Or RAND[i] and Ki[j]
9. Store it in rhs[ ]
10. i=0 , j=0

Call log_fiunction to write to Log file

11. Repeat steps 12 and 13 until i > RAND_LENGTH/2 and j > Ki_LENGTH/2
12. Ex-Or lhs[i] and rhs[j]
13. Store it in combine[i]

Call log_fiunction to write to Log file

14 i=0

14. Repeat steps 15 and 16 until i > RAND_LENGTH/4
15. Ex-Or lhs[i] and rhs[j]
16. Store it in combine[i]

Call log_fiunction to write to Log file

17 i=0,j=Ki_LENGTH/4

18. Repeat steps 19 and 20 until i > RAND_LENGTH/4
19. Ex-Or combine[i] and combine[j]

20.Store it in SRES[i]
Call log_fiunction to write to Log file

21 Return 0
Stop SRES_generation_A3_algo

VI. CONCLUSION AND FUTURE WORK

CONCLUSION:
Existing protocols and algorithms are not available to world. And Although the GSM architecture allows operator to choose any algorithm for A3 and A8, many operators used COMP128 (or COMP128-1) that was secretly developed by the GSM association. The structure of COMP128 was finally discovered by reverse engineering and some revealed documentations, and many security flaws were subsequently discovered. In addition to the fact that COMP128 makes revealing Ki possible especially when specific challenges are introduced, it deliberately sets ten rightmost bits of Kc equal to zero that makes the deployed cryptographic algorithms 1024 times weaker and more vulnerable, due to the decreased keyspace. Also, Both A5/1 and A5/2 algorithms were developed in secret. Also, this application will work only on LINUX supported operating system. The concurrent server can handle at most 10 clients at a time.
To achieve more secure GSM network, all the bits of Kc has been used to make a more complex and secured ciphering algorithm. The algorithm provides better solution to handle authentication and encryption of mobile communication.

Future Directions:

In this proposed work, Authentication and Encryption algorithms are redefined. And our work can be enhanced in several ways:
1) The Encryption and Decryption of images, audio and video files can also be done after the authentication procedure.
2) TMSI number can be used for more security purposes.
A key use of the TMSI is in paging a mobile. "Paging" is the one-to-one communication between the mobile and the base station. The most important use of broadcast information is to set up channels for "paging". Every cellular system has a broadcast mechanism to distribute such information to a plurality of mobiles.
3) Communication between two and more MS can be established further.

