ISSN (Online): 2230-7893
www.IJCEM.org

# Confidentiality & Privacy of Signaling Information elements on GSM Network by using Different Security Algorithms

**Preeti[1], Nitin Jain[2], Neeraj Singla[3] and Yogesh Kalra[3]**

[1,2]Asst Professor in Department of Computer Science, Gurgaon College Of Engineering,Gurgaon
pittivts@gmail.com, nitin.87.jain@gmail.com

[3]Asst Professor in Department of Computer Science, Vaish College Of Engineering, Rohtak
neerajsin30@gmail.com

[4]Asst Professor in Department of Computer Science, Savera Group Of Institutions,Gurgaon
yogeshkalra4@gmail.com

## Abstract
GSM security algorithms are used to provide authentication and radio link privacy to users on a GSM network .The encryption algorithm used in the GSM system is a stream cipher known as the A5 algorithm. In this Paper ,we will study about the security mechanisms incorporated in GSM that make it the most secure mobile communication, particularly in comparison to the analog systems . The use of authentication, encryption, and temporary identification numbers ensures the privacy and anonymity of the system's users.

**Keywords** –Ciphering, RAND, Signed response, IMSI, USIM, PIN ,Authentication Centre, triplets.

**Introduction:** GSM (group special mobile or general system for mobile communications) is the Pan-European standard for digital cellular communications which was established in 1982 within the European Conference of Post and Telecommunication Administrations (CEPT). The GSM standard originally described a digital, circuit switched network optimized for full duplex voice telephony.

## Need of Network Security:
The GSM speech service is secure up to the point where speech enters the core network but over the core network it has no security. In order to have an end-to-end security, speech must be encrypted before it enters the GSM network.

**Encryption** - In GSM, encryption refers to the process of creating authentication and ciphering crypto-variables using a special key and an encryption algorithm. Encryption program uses an encryption algorithm (complex mathematical processes) to encrypt and decrypt the data. Encryption algorithm creates specific strings of data used for encryption - keys that consist of long strings of bits or binary numbers.

**Symmetric Encryption:** Symmetric Encryption (also known as symmetric-key encryption, single-key encryption, one-key encryption and private key encryption) is a type of encryption where the same secret key is used to encrypt and decrypt information. Symmetric algorithms (Symmetric-key algorithms) use the same key for encryption and decryption. Symmetric-key algorithms can be divided into Stream algorithms (Stream ciphers) and Block algorithms (Block ciphers).

**1.Stream Ciphers**
Stream ciphers encrypt the bits of information one at a time - operate on 1 bit (or sometimes 1 byte) of data at a time (encrypt data bit-by-bit). Stream ciphers are faster and smaller to implement than block ciphers, however, they have an important security gap. If the same key stream is used, certain types of attacks may cause the information to be revealed.

**2 Block Ciphers**:
Block cipher (method for encrypting data in blocks) is a symmetric cipher which encrypts information by breaking it down into blocks and encrypting data in each block.

### 1.1.1 GSM Encryption Algorithms:
GSM uses three different security algorithms called A3, A5, and A8.

- An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centers. It is used to authenticate the customer and generate a key for encrypting voice and data traffic.
- An A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem (BSS).

## GSM Security Features:
Security in GSM consists of the following aspects:
**1. Subscriber Identity Authentication**: The GSM network authenticates the identity of the subscriber through a 128-bit random number (RAND) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki).
**2. Subscriber Identity Confidentiality**: The SIM contains the ciphering key generating algorithm (A8) which is used to produce

ISSN (Online): 2230-7893
www.IJCEM.org

the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

**3. Signaling Data Confidentiality:** To ensure subscriber identity confidentiality**,** the Temporary Mobile Subscriber Identity (TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued.

## IMPLEMENTATION:

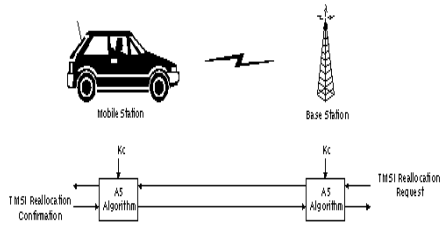
The security mechanisms of GSM are implemented in three different system elements:

1. Subscriber Identity Module (SIM)
2. GSM handset or MS
3. 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.

- Within the GSM network, the security information is further distributed among the authentication center (AUC), the home location register (HLR) and the visitor location register (VLR). The AUC is responsible for generating the sets of RAND, SRES, and Kc which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.




**GSM Security Model**:

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 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.

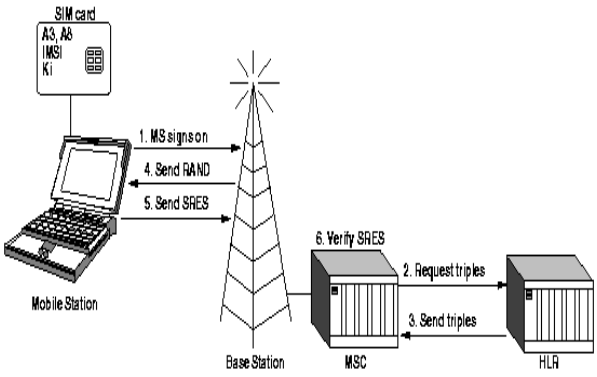



**Figure 1.Mobile station authentication**

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

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

ISSN (Online): 2230-7893
www.IJCEM.org

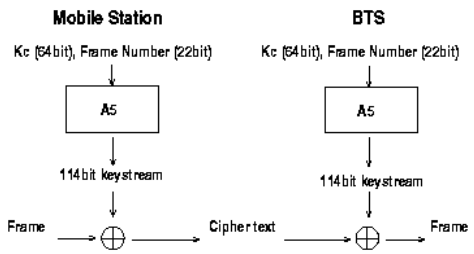



**Figure2 : Frame encryption and decryption**

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.

- **A3:The MS Authentication Algorithm:**
  The A3 is the authentication algorithm in the GSM security model. Its function is to generate the SRES response to the MSC's random challenge, RAND, which the MSC has received from the HLR. The A3 algorithm gets the RAND from the MSC and the secret key Ki from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the Ki secret are 128 bits long.

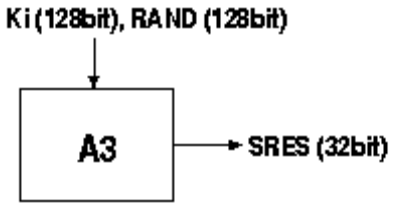



**Figure 3:Signed response (SRES) calculation**

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 .

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

- **A8:The Voice-Privacy Key Generation Algorithm**

The A8 algorithm is the key generation algorithm in the GSM security model. The A8 generates the session key, Kc, from the random challenge, RAND, received from the MSC and from the secret key Ki. The A8 algorithm takes the two 128-bit inputs and generates a 64-bit output from them. This output is the 64-bit session key Kc [6]. The BTS received the same Kc from the MSC. HLR was able to generate the Kc, because the HLR knows both the RAND (the HLR generated it) and the secret key Ki, which it holds for all the GSM subscribers of this network operator. One session key, Kc, is used until the MSC decides to authenticate the MS again. This might take days.

- **A5: 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 key stream for every frame**.** There are three versions of the A5 algorithm:

**A5/1** - The current standard for U.S. and European networks. A5/1 is a stream cipher.

**A5/2** - The deliberately weakened version of A5/1 that is intended for export to non-western countries. A5/2 is a stream cipher.

**A5/3** -A newly developed algorithm not yet in full use. A5/3 is a block cipher.

## AUTHENTICATION PROCEDURE

**1.** 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**. The network can have the MS authenticate whenever it wants and this can vary from network to network. The network can require the MS to authenticate every time an event is initiated (location update, mobile-originated call, mobile-terminated call, etc.), every so many events, or even after a certain time period has elapsed. The network will almost always require authentication whenever the MS moves into a new Location Area and does a Location Update.

**2**. 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).

**3.** 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.

**4.** 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.
**5.** 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.
**6.** The RAND, SRES, and Kc are collectively known as the Triplets. The AuC may generate many sets of Triplets and send them to the requesting MSC/VLR. This is in order to reduce the signaling overhead that would result if the MSC/VLR requested one set of triplets every time it wanted to authenticate the MS. It should be noted that a set of triplets is unique to one IMSI, it cannot be used with any other IMSI.
**7.** 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.
**8.** The MSC stores the Kc and the SRES but forwards the RAND to the MS and orders it to authenticate.
**9.** 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.

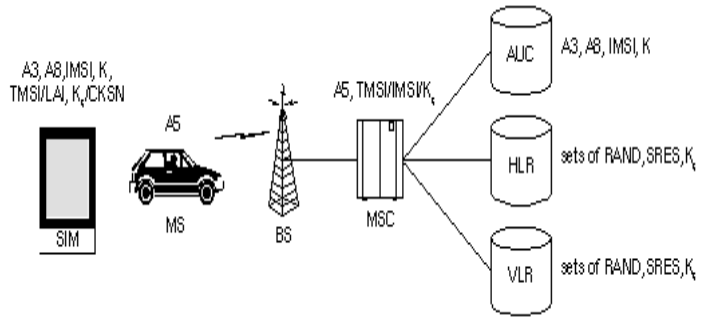



**Fig: Authentication Procedure**

## *1.2* Conclusion:

***1.3*** Security is a key issue in mobile communication. So there are different algorithms that are used to maintain Privacy and Confidentiality in GSM. A3/A5 are the algorithms that are used for providing authentication and A5 algorithms is used for providing Privacy/Confidentiality to GSM data elements sent over the network. But still there are many more security algorithms that prevents even the smaller attacks that A5 algorithms are unable to prevent.

## *1.4* References:

**1.** 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.

**2.** Biala, J., "Mobilfunk und Intelligente Netze," Friedr., Vieweg & Sohn Verlagsgesellschaft, 1994.

**3.** Cooke, J.C.; Brewster, R.L., "Cyptographic Security Techniques for Digital Mobile Telephones," Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications, Vancouver, B.C., Canada, 1992.

**4.** European Telecommunications Standards Institute, Recommendation GSM 02.09, "Security Aspects".

**5.** European Telecommunications Standards Institute, Recommendation GSM 02.17, "Subscriber Identity Module".

**6.** European Telecommunications Standards Institute, Recommendation GSM 03.20, "Security Related Network Functions".

**7.** Hodges, M.R.L., "The GSM Radio Interface," British Telecom Technology Journal, Vol. 8, No. 1, January 1990, pp. 31-43.

**8.** Hudson, R.L., "Snooping versus Secrecy," Wall Street Journal, February 11, 1994, p. R14

**9.** Schneier, B., "Applied Cryptography," J. Wiley & Sons, 1994.

**10.** Williamson, J., "GSM Bids for Global Recognition in a Crowded Cellular World," Telephony, vol. 333, no. 14, April 1992, pp. 36-40.