GSM Security

1 GSM Security Introduction

GSM uses encryption based security which includes:

- Challenge-response authentication for the MS (Mobile Station)
- Shared key (private key) ciphering for traffic

Besides the GSM has other security features as well, which includes frequency hopping (physical layer security), IMSI and IMEI verifications, and use of TMSI. PIN (Personal Identity Number) and PUK (PIN Unlocking Key) pair for the SIM card.

2 SIM Security

PIN (Personal Identity Number) is a 4-8 digit SIM access code which can be used to secure the MS from use. When PIN is activated the user needs to enter PIN code in order to make a call. The PUK (Personal Unblocking Key) is used to unlock the PIN code.

PIN2 (Personal Identity Number 2) is a 4-8 digit SIM access code which can be used to secure the SIM from accessing the PDA (personal digital assistant) information such as address book, and also the call log. When PIN2 is activated the user needs to enter PIN2 code in order to access the information. The PUK2 (Personal Unblocking Key 2) is used to unlock the PIN2 code.

How do I change my PIN and PUK?

Change SIM Card PIN	** 04 * old PIN * new PIN * new PIN #
Change SIM Card PIN2	** 042 * old PIN2 * new PIN2 *new PIN2 #
Change SIM Card PUK	** 05 * old PUK * new PUK * new PUK #
Change SIM Card PUK2	** 052 * old PUK2 * new PUK2 * new PUK2 #

Note: These codes only work on some mobile stations offered by some providers.
http://www.gsm-security.net/faq/change-gsm-pin-pin2-puk-puk-personal-identity-number-personal-unblocking-key.shtml

3 IMSI/TMSI and IMEI Verification

The IMSI number is the ID of the subscription. Any service request must include IMSI (or TMSI) to identify the identity of the subscriber. The MSC verifies the subscription profile of that IMSI, which is saved in HLR and possibly in the VLR. Similarly, a GSM system also checks the IMEI number against White, Grey and Black list of IMEI in the EIR.

The allocation of TMSI (Temporary IMSI) is used in order to protect IMSI's privacy. The allocation and use of TMSI help avoid sending IMSI all the time over the radio interface.

4 Physical Layer Security on Radio Interface

Frequency hopping technique is employed in GSM systems in order to reduce carrier-to-interference ratio (CIR). An added benefit of the frequency hopping is physical layer security. With this technique a connection uses a sequence of frequencies (one after another) in order. The frequencies and their order is decided when the MS is assigned the radio channel. See the frequency hopping section for the further detail.

5 Authentication and Ciphering

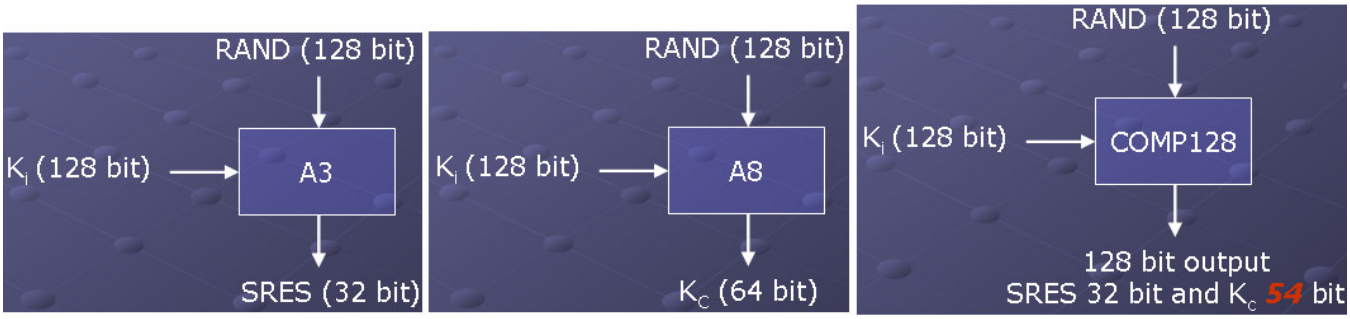
Individual Subscriber Authentication Key (K_I) is a 128-bit security key shared by the MS (stored in the SIM) and operating company's network (stored in HLR data base) for the purpose of authentication and ciphering. GSM has a number of standard algorithms (**A1 to A8**). These algorithms are also stored in the MS and the AuC (Authentication Center).

For the purpose of authentication and ciphering the MSC requests the HLR to provide security 'triples', which consists of

- A 128-bit random challenge (RAND)
- A 32-bit Signed Response (SRES)
- A 64-bit ciphering key (Kc) which is also called Session Key

The HLR provides the K_I of the MS to AuC (authentication Center) and asks for the triples. Usually AuC provides 5 triples at a time. AuC computes these numbers as follows:

- 128-bit RAND is from a simple random number generator
- 32-bit SRES is the result from Authentication algorithm (A3), using RAND and K_I as inputs (see the figure below).
- 64-bit Cipher Key (K_C) is the result from Ciphering Key algorithm (A8) using RAND and K_I as inputs (see the figure below).



Almost all the GSM operators use COMP128 algorithm for A3 and A8. COMP128 produces 128 bit output, which includes 32-bit SRES and 54-bit K_C. Ten zeros are appended to 54-bit K_C to make it a 64-bit K_C.

Upon reception of the triples from the AuC the HLR sends them to the MSC. The MSC saves the values in the VLR, and use them one at a time. When all of them are used the MSC asks the HLR for a new set.

When one of more 'triples are available in the VLR the MSC picks one triple as the current one. The MSC sends the RAND of the current triple to the MS.

Mobile Station Authorization Process

The mobile station authorization process is a challenge – response process. An MSC sends the RAND (from the active triple) to the MS, and challenge the MS to compute the correct SRES. The MS uses the same process as AuC does to compute SRES. That is, the algorithm A3 (stored in the SIM) takes the K_I (stored in the SIM) and the RAND (received from the MSC) as inputs and computes the SRES as the output. The MS sends the SRES to the MSC as the response to the challenge. The MSC compares the received SRES with its own one. When found equal the MSC considers the MS passed the test.

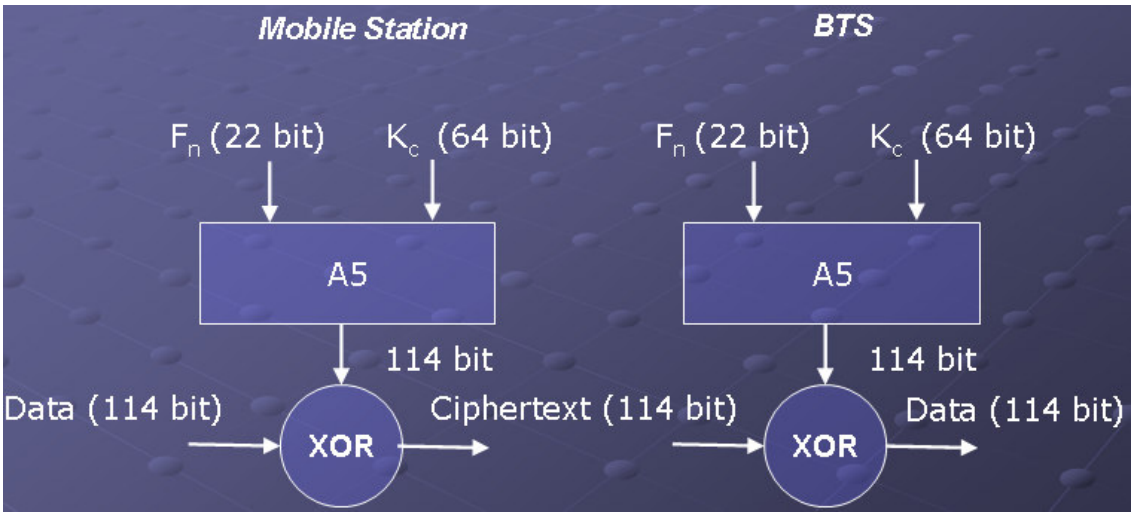
Session Key Generation Process in the MS

The active triple in the MSC/VLR contains K_C which is the session key for ciphering the payload. The MS needs the identical one. The MS uses the same process as AuC does to compute K_C. That is, the algorithm A8 (stored in the SIM) takes the K_I (stored in the SIM) and the RAND (received from the MSC) as inputs and computes the K_C as the output. The MS stores the key in the SIM. Since MS is already successful in authentication the computation of the session key should be correct.

At this stage the MS and the MSC have the copies Session Key (K_C). Note that MSC already has this key as a part of the triple. When required, the MSC sends the key to the BTS (via BSC) for the purpose of ciphering. Thus the MS and the BTS exchange ciphered traffic.

Payload Ciphering Process

The ciphering algorithm (A5) uses the cipher key (K_C) and the 22-bit TDMA frame number (F_N) as the input parameters in order to cipher/decipher the data/digitized voice (see the diagram below)



http://www.gsm-security.net/gsm-security-papers.shtml

Multiple versions of the A5 algorithm exist which implement various levels of encryption. Examples:

- A5/0 utilizes no encryption
- A5/1 is the original A5 algorithm used in Europe
- A5/2 is a weaker encryption algorithm created for export and used in the United States
- A5/3 is a strong encryption algorithm created as part of the 3rd Generation Partnership Project (3GPP)

In order to reduce the overhead of authentication and key generation process the GSM takes a middle road. This process is required only once per MS attachment. When the MSC sends the RAND value to the MS for authentication the MSC also passes ciphering key sequence number (CKSN). This is a serial number given to the 'triple' by the MSC and stored in VLR along with the MS's data. When the MS makes the next service requests it sends the CKSN in its service request. The MSC verifies the CKSN and bypass the authentication and key distribution process by simple using the old one.