SECURITY IN GSM

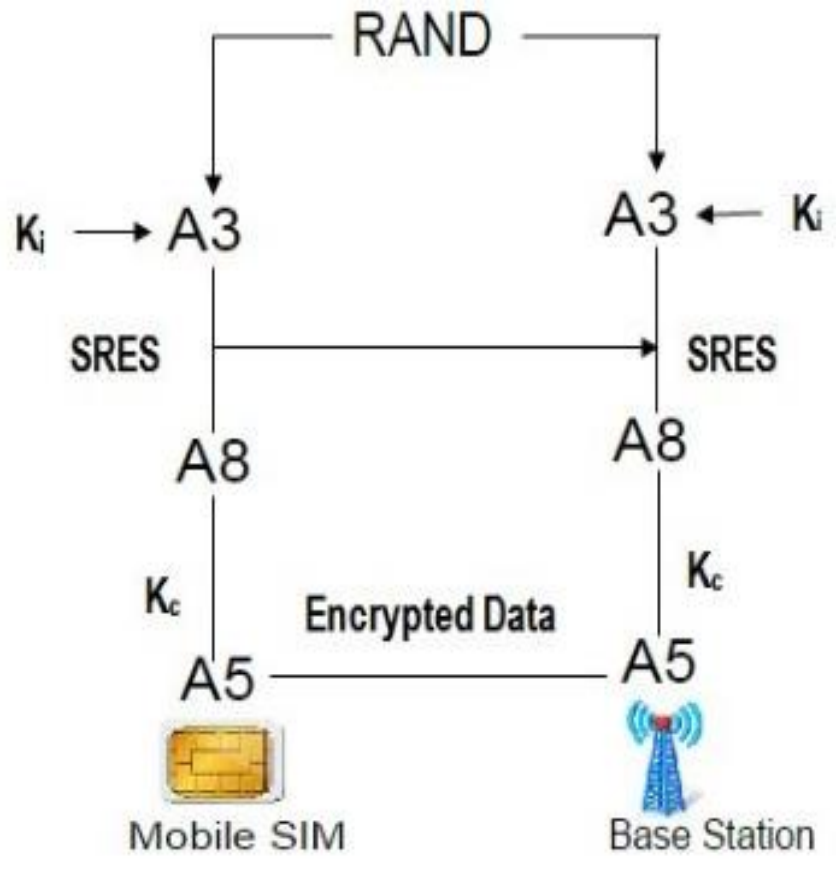
Authentication & Encryption

ECE 525E – WIRELESS & MOBILE COMMUNICATION

Monday, March 10, 2025

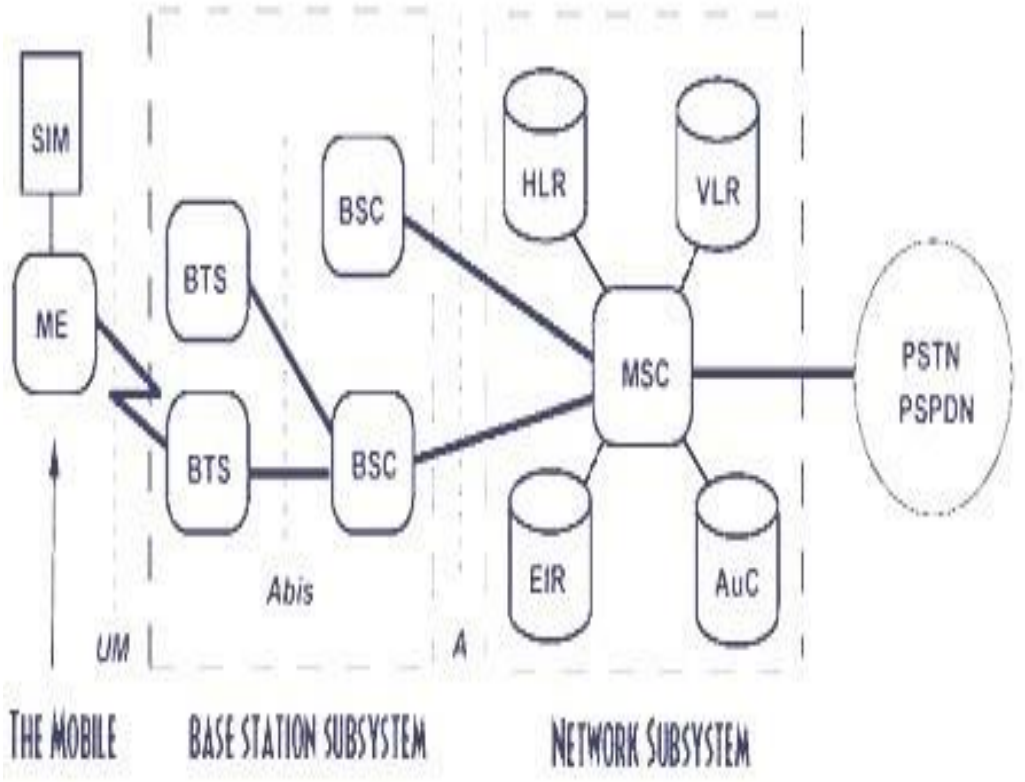
WHAT ARE THE INBUILT SECURITY FEATURES IN GSM?

1. **Key security features in the Global System for Mobile Communication (GSM) are:**
   a) **Authentication using inbuilt algorithms to verify the identity of the mobile subscriber** before allowing them to access the network.
   b) **Encryption of voice & data over radio links** between MSs and base transceiver stations
   c) **Ensuring user anonymity by using temporary user identification instead of IMSI.**



WHAT IS AUTHENTICATION CENTRE?

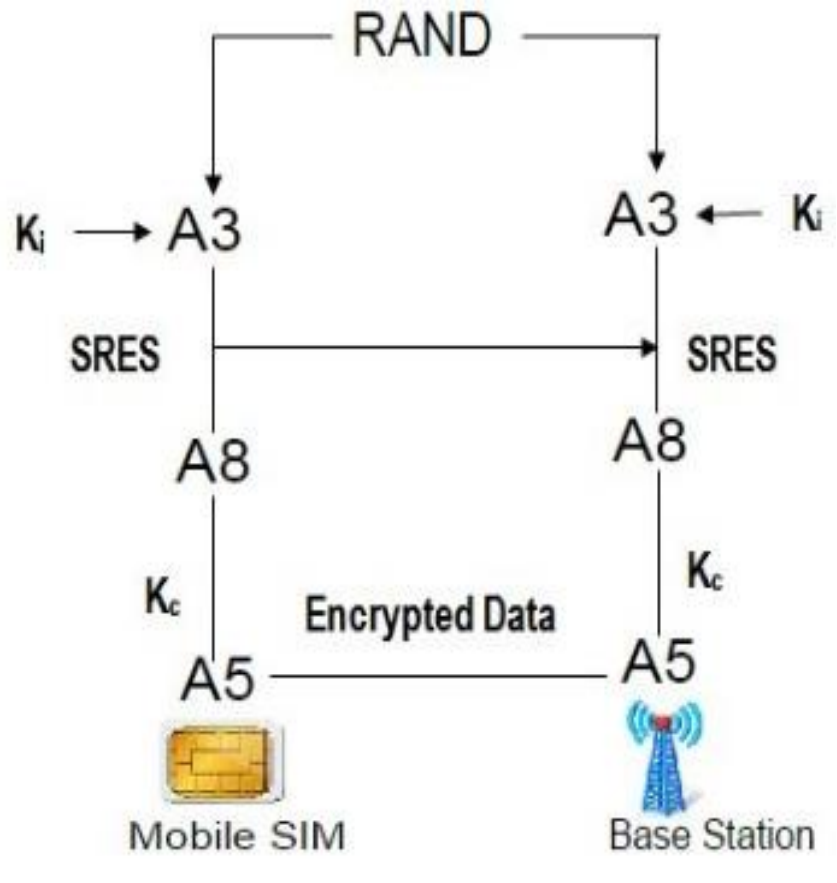
1. **Authentication Center (AuC) is a component of the Network Subsystem responsible for authenticating each SIM card** attempting to connect to the network and generating parameters for encryption and privacy, ensuring secure communication.
2. **The purpose of the AuC is authenticate mobile subscribers** by verifying the validity of their SIM cards and generating the data used for secure communication.



THE AUTHENTICATION CENTER (AUC)

a) The Authentication Centre (AuC) is a database that keeps the following parameters:
   a) The K_I,
   b) The A3 authentication algorithm,
   c) The A5 ciphering algorithm
   d) The A8 ciphering key generating algorithm.

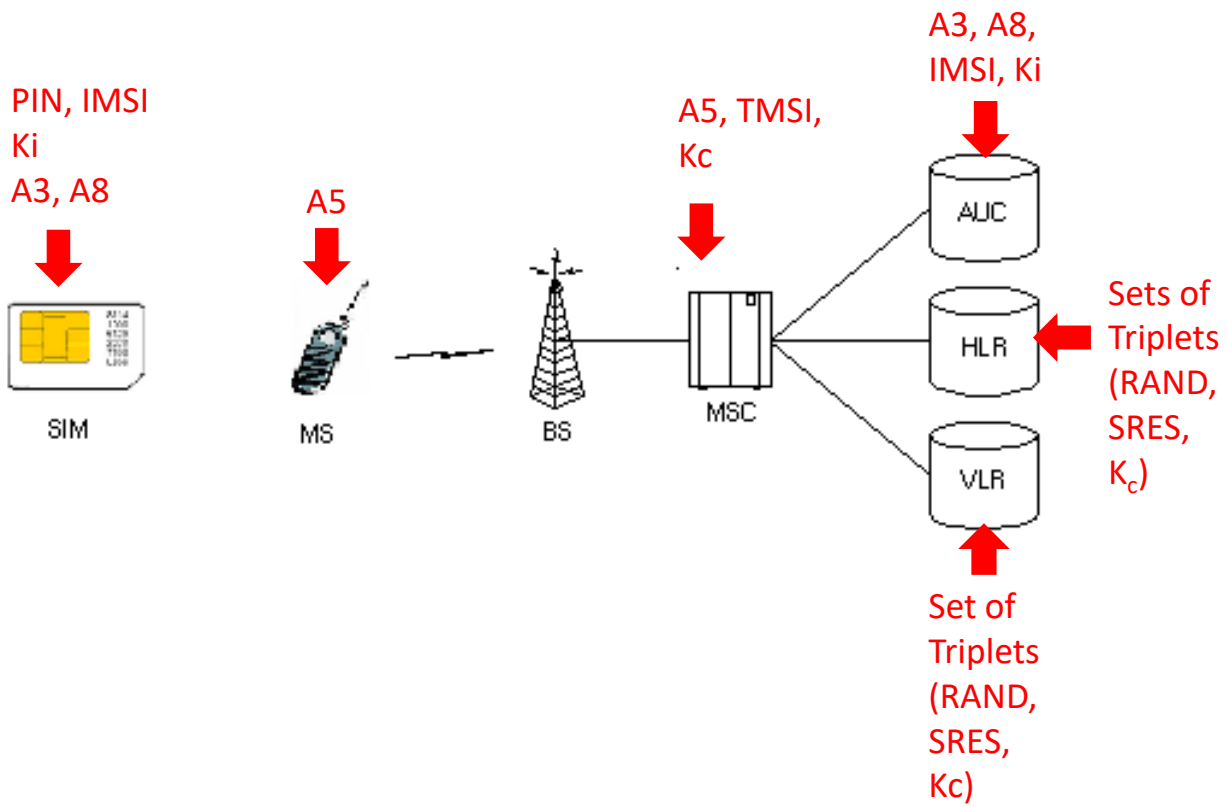
b) AUC is responsible for creating the sets of triplets:
   a) Random numbers (RAND),
   b) Signed Response (SRES) and
   c) The Cipher key (K_C)



HOW SECURITY IS ASSURED IN GSM

The security mechanisms of GSM are implemented in Mobile Station, SIM card and Network as follows:

1. **The Subscriber Identity Module (SIM)** contains
   a) Personal Identification Number (PIN)
   b) The International Mobile Subscriber Identity (IMSI)
   c) the Individual Subscriber Authentication Key (K_i),
   d) the Cipher Key Generating Algorithm (A8),
   e) the Authentication Algorithm (A3),
2. **The GSM handset (or MS)** contains
   a) Ciphering Algorithm (A5)
3. **The GSM network** contains
   a) Encryption algorithms (A3, A5, A8)
   b) IMSI,
   c) Temporary Mobile Subscriber Identity (TMSI)
   d) Location Area Identity (LAI),
   e) Individual subscriber authentication key (K_i)

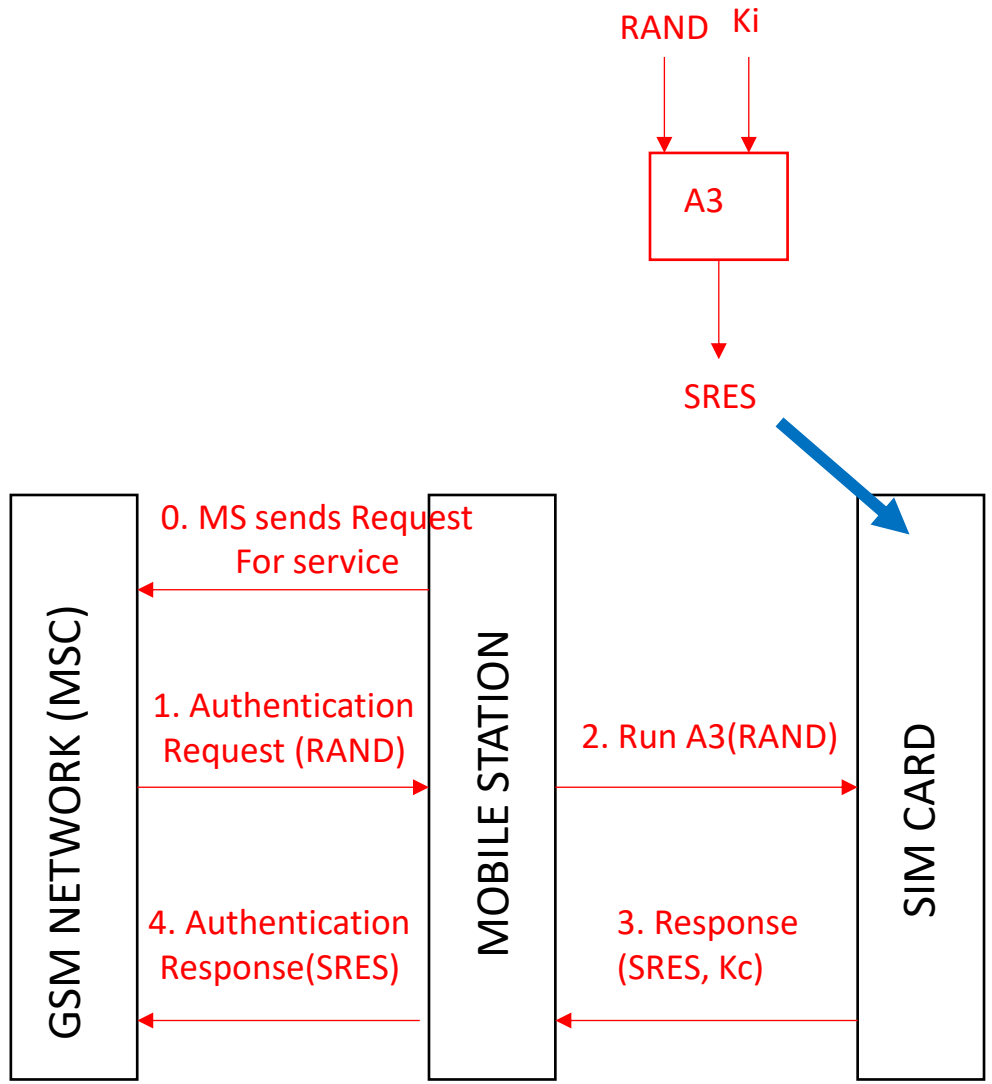


PURPOSE OF AUTHENTICATION

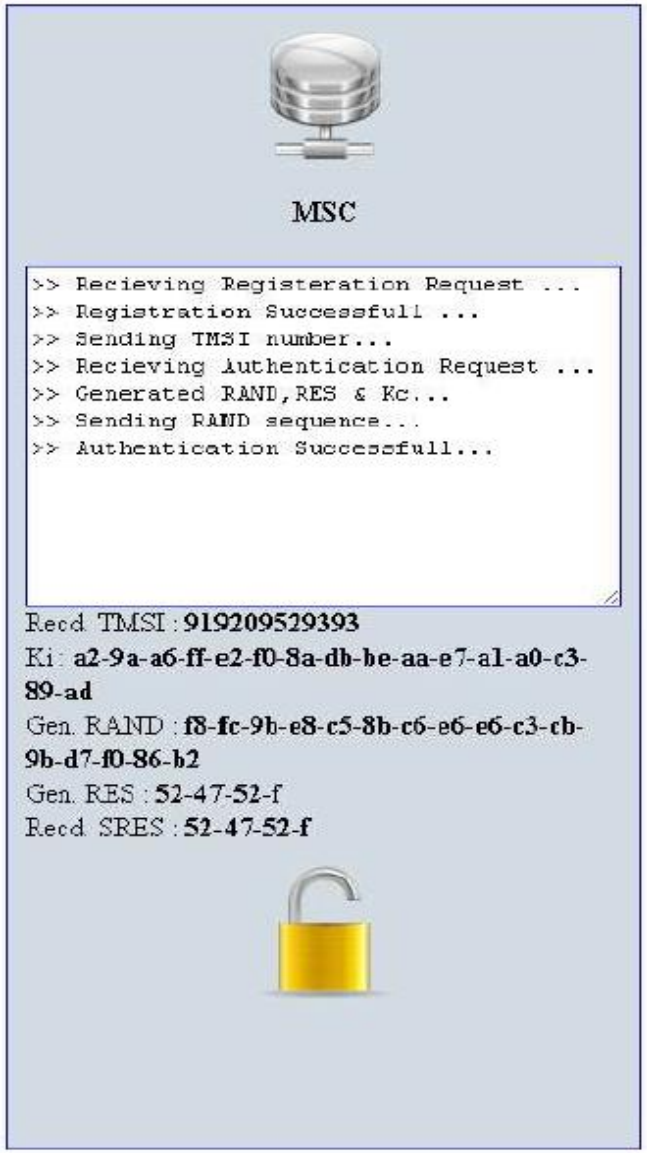
1. The GSM offers a mechanism for verifying the subscriber identity by ensuring that a **user has a valid Subscriber Identity Module (SIM) card.**
2. The purpose of authentication, is to **protect the network** against unauthorized use.
3. It also **protects GSM subscribers**, by making it practically impossible for intruders to impersonate authorized users- masquerading.

GSM AUTHENTICATION (GENERAL)

1. The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism.
2. **The aim** is to establish that the Ki stored in the AUC when first registering the subscriber is the same as that stored in the SIM card.
3. The process is as follows:
   1. A 128-bit random number (RAND) is generated by the AUC and sent to the MS.
   2. 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 (K_i).
   3. The SIM card responds with signed response (SRES) and Cypher Key (K_c)
   4. SRES is then transmitted to the network.
   5. Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.



MONITORING THE AUTHENTICATION PROCESS



AUTHENTICATION OF ROAMING MOBILE STATION

Step1: MS enters a new visiting area and requests for service, an authentication request is sent to MSC first, where the request includes TMSI and LAI.

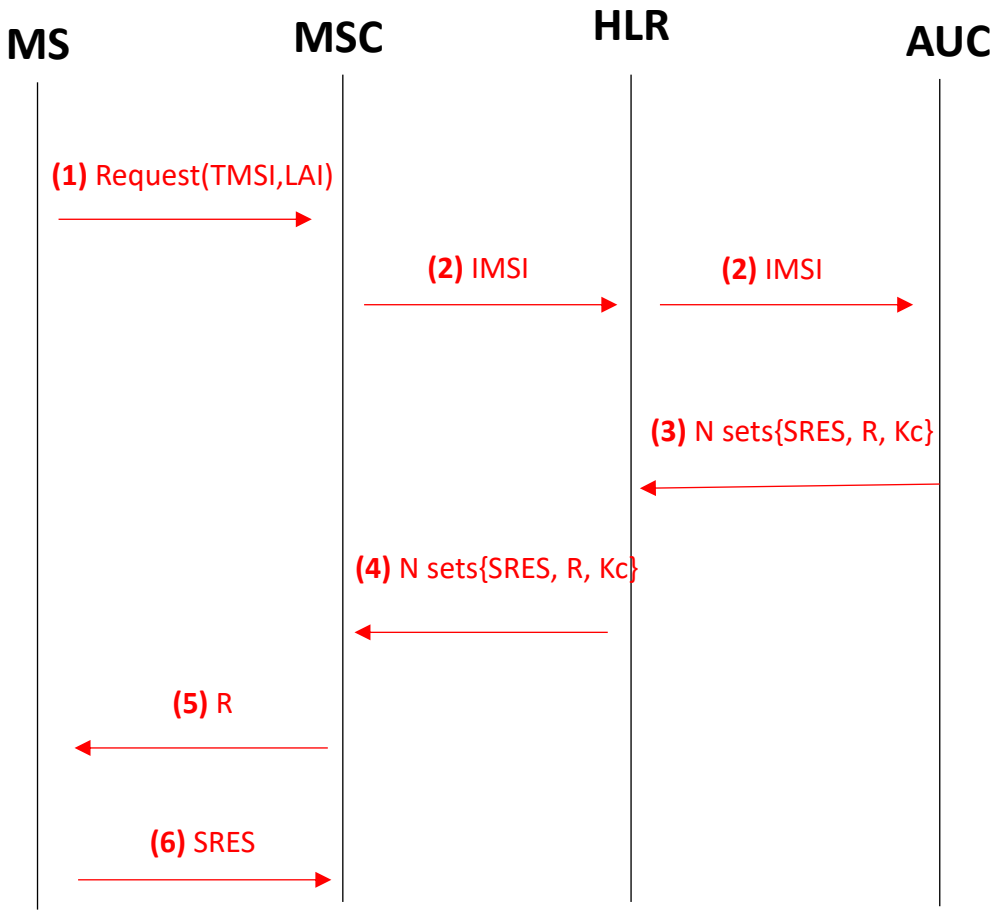
Step2: After receiving the request, the new MSC uses the received TMSI to get the IMSI from the old MSC and then sends IMSI to HLR and AUC.

Step3: The AUC generates n distinct sets of authenticating parameters {SRES, R, K_c} and sends them to HLR which transmits them to the MSC.

Step4: After receiving the sets of authenticating parameters, MSC keeps them in its own database and selects one set of them to authenticate the mobile station in subsequent calls and sends the selected R to MS.

Step5: Once MS receives R from MSC, it computes SRES = A3(R, K_i) and the temporary session key K_c = A8(R, K_i), respectively, where K_i is fetched from the SIM card. Then the SRES is sent back to MSC.

Step 6: Upon receiving SRES from MS, the MSC compares it with the corresponding SRES kept in its own database. If they are not the same, the authentication is failure and the MS is blocked from the network.



Authentication of a Roaming Phone

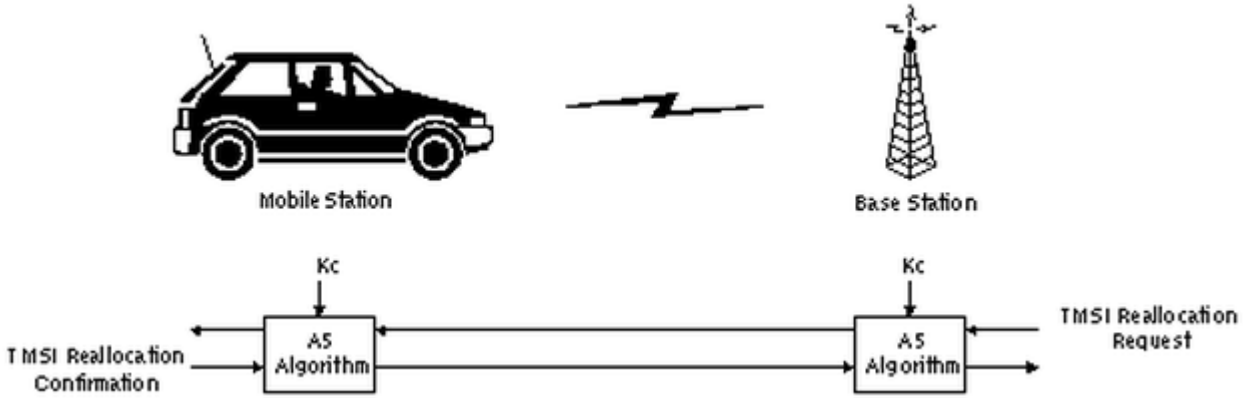
SUBSCRIBER IDENTITY CONFIDENTIALITY

1. **The Temporary Mobile Subscriber Identity (TMSI)** is used to ensure subscriber identity confidentiality.

2. **TMSI** is sent to the MS after the authentication.

3. The mobile station responds by confirming reception of the TMSI.

4. The TMSI is valid in the location area in which it was issued.



TMSI Re-allocation Process

ENCRYPTION OF VOICE AND DATA

1. **Encryption** is used in the GSM air interface (Um Interface) to protect the confidentiality of data and signalling on the air interface.

2. Two algorithms are essentially involved in the encryption process; i.e

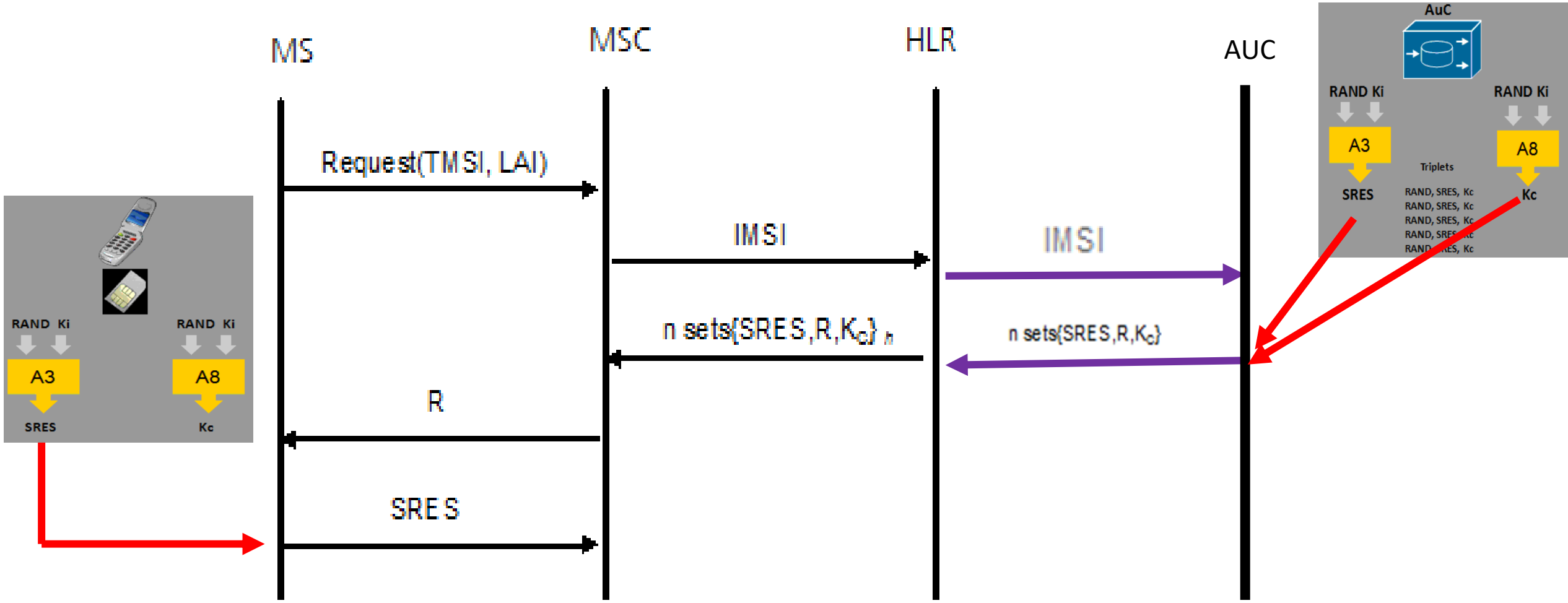
   a) The **encrypting algorithm (A5)** implemented in the MS and at the BTS.

   b) The **cipher key generation algorithm** (A8) implemented in the AuC and the SIM.

Telephone Eavesdropping

FLOW DIAGRAM OF THE GSM SECURITY PROCESS

1. After the user has been authenticated, the MS and the BTS can start using encryption by applying the cipher key Kc.
2. Kc is generated using the individual key K_i and a RAND by applying the A8 algorithm.
3. The SIM and the network both create the same value K_c based on the RAND.
4. The K_c itself is never transmitted over the air interface.

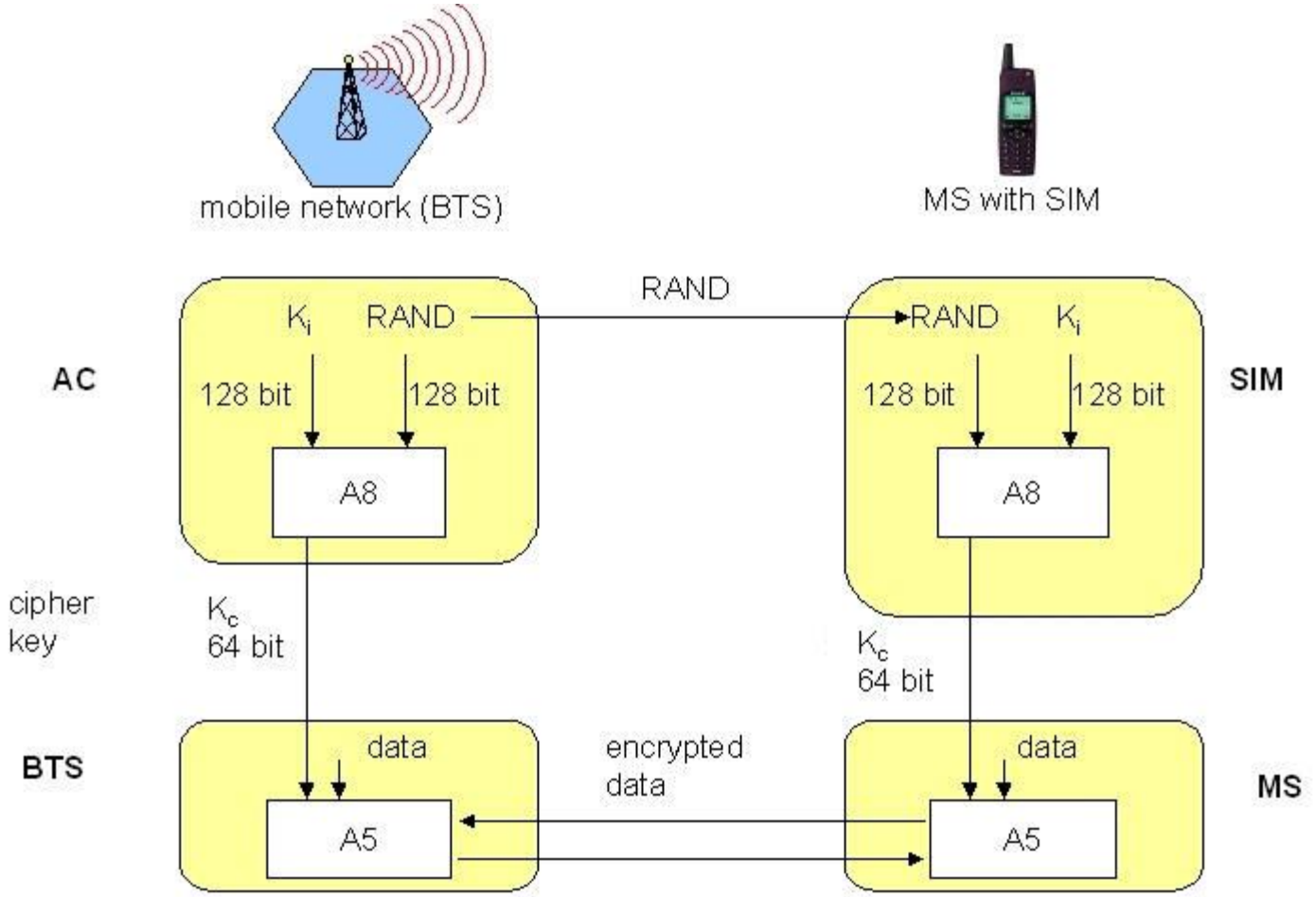


ENCRYPTION & DECRYPTION IN GSM NETWORKS

1. After authentication, the MSC passes the cypher key kc to the BTS and the SIM card passes kc to the Mobile phone.

2. The MS and the BTS can now encrypt and decrypt data using the A5 algorithm and the Kc.

3. Kc is a 64 bit key which is not very strong, but provides enough protection to stop simple eavesdropping.



WHERE DO YOU GET A3, A5, A8 SOFTWARE?