GSM (2G) Security

There are two principal tasks involved in providing security in GSM a) entity Authentication and key agreement b) Message protection.

a) Entity Authentication and key Agreement-

Authentication verifies the identity and the validity of the SIM card to the n/w and that the subscriber has authorized access to the n/w.

Ki - is the individual authentication subscriber key its a 32-bit no. it is paired with Ki when the SIM card is created. Ki is only stored on the SIM card and the authentication center

RAND - it is a random 128 bit no. that is generated by the when the n/w req to authenticate to a subscriber. RAND is used to generate the SRES and kc cryptovariables

SRES ~~Esa~~ 32 bit. used in authentication 1 its not passed but kept by the MSC/VLR (signed Response)

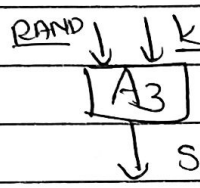
kc - 64 bit ciphering key that is used in the A5 encryption alg that is used to

DATE

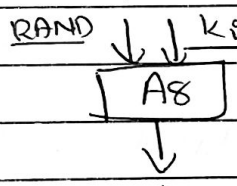
Page No 14

encipher and decipher the data that is being transmitted over the interface

- A_3 Alg - it resides in the SIM card



- A8 Alg - Computes the 64 bit ciphering key
  it resides in the IMSI sim card



- Authentication is performed when a subscriber moves into a new n/w

Steps (overview) for easy understanding

step 1 Authorization when the MS (Mobile station) request access to the n/w [Request Access IMSI] the MSC / VLR will request the Auc to authenticate

step 2 The MSC will forward the IMSI to the HLR and request authentication. When the HLR receives the IMSI and the subscriber req it first checks its DB to make sure the MC is

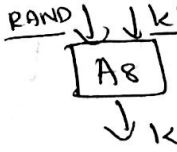
RAMSONS

valid and belong to the nlw it then fawaad it to the Authentication Center (AUC) and request fael authentication Triplets

Step3 : The AuC will use the IMSI to look up into the associated k_i with the available IMSI. The AUC will also generate a 28 bit Random NO. (RAND) and a key. The RAND and key (kp) is inseted into the A3 Alg the o/p is 32 bit SRES.

Step4 : The SREG is the challonge that is send to the mobile Station (MS) when authentication is requested

step 5 : The RAND and k_i are send to A8 Alg the o/p is 64-bit k_c (Ciphering key). That is used in the A5 Alg to cipher and decipher the data that is being transmited on the interface



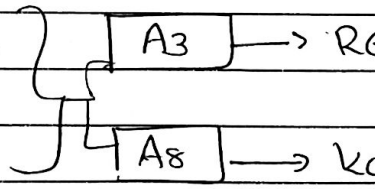
Step 6 : The RAND, SREG and k_c = Triplets

Once the AUC has generated the Triplets it will fawaad them to HLR

Step7: HLR sends this request to the MSC/VLR

The MSC stores the SRES and Kc but forwards the RAND to the mobile station (MS) inorder to authenticate

Step8: The MS has the K_i stored on the SIM. The A3 and A8 alg also resides on the SIM card. The RAND and K_i are send to the A3 and A8 alg to generate the Response (RES) or XRES and Kc



Step 9: The RES or XRES is send to MSC/VLR. Here the MSC will match the RES with the SRES coming from the authentication center

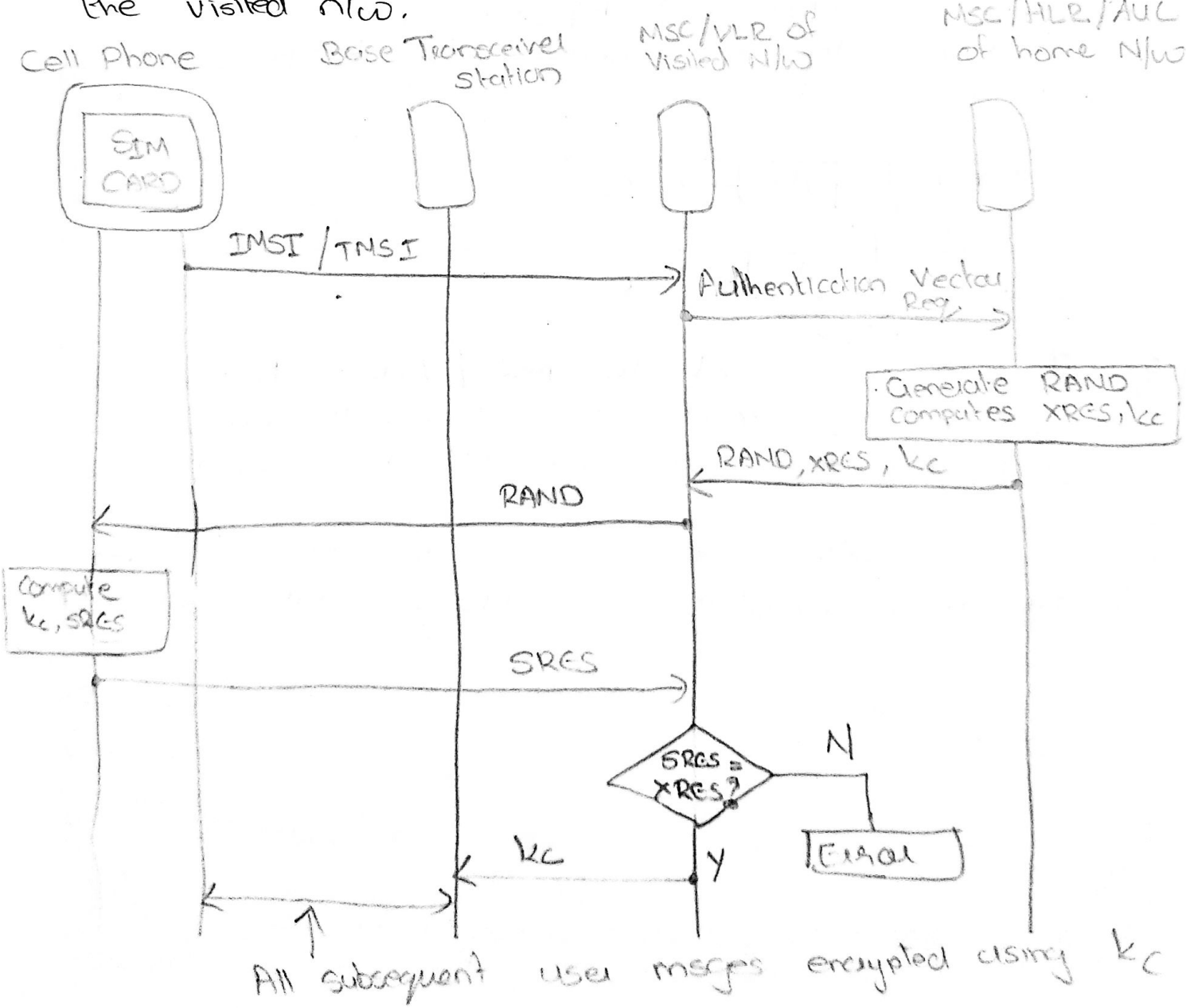
RES = SRES or XRES = SRES

if the two matches the MS is authenticated

[From Text]

Step 1 : Authorization Request from Cellphone

- Cellphone sends to the Base station the encryption alg that it can support.
- sends its IMSI / TMSI to the MSC.
- If the cellphone is away from the home n/w the IMSI will be received by the MSC of the visited n/w.



Step 2: Creation and Transmission of Authentication Vectors -

- The MSC for the home n/w receives the IMSI of the cellphone. It is used to index into the HLR when it obtains the key k_i.

- The MSC/HLR generates a 128-bit random no., RAND, which functions as the challenge in the challenge-response authentication protocol.

- It computes two quantities XRES and k_c

$$XRES = A_3(RAND, k_i)$$
$$k_c = A_8(RAND, k_i)$$

A_3, A_8 – keyed hash fn.
XRES – expected response in the challenge-response authentication protocol.
k_c – encryption key.

- The HLR creates five authentication triplets,

$$\langle RAND, XRES, k_c \rangle$$

- The triplets are sent to the MSC of the home n/w by the HLR.

- The MSC then sends the challenge (RAND) from the first triplet to the base station who forwards it to the SIM on the cellphone.

Step3 : Cellphone Response.

Once the SIM receives RAND, it computes SRES

- The cellphone sends SRES to the base station who forwards it to MSC.
- The MSC checks if SRES is equal to XRES - its expected response if equal MSC identifies it as a genuine subscriber.

Step4 : Computation / Receipt of Encryption key

- SIM computes Kc
- On the nlw side the MSC extracts Kc from its authentication triplet and communicates it to the base station ∴ all user msgs blw the cellphone and base station are encrypted using Kc

Encryption

Encryption of msgs b/w the cellphone and BS is performed by a stream cipher.

The keystream generated for this cipher is denoted by A_5. The keystream is a function of the 64-bit encryption key, k_c, and a 22-bit frame number.

$$\text{KEYSTREAM} = A_5(k_c, \text{FRAME\#})$$

The frame no. is incremented for each frame that is transmitted. The keystream changes for each frame sent during a call.

Ciphertext = Plaintext $\oplus$ keystream

Computations of the keystream and encryption do not require i/p from any of the static secrets stored in the SIM.

The operations are performed by the cellphone and not the SIM.

The computation of XRES and k_i requires the