THADOMAL SHAHANI
TSEC
ENGINEERING COLLEGE

EXPERIMENT NO. 10

Aim :- Write a program to implement the A3/A5/A8 GSM security algorithm.

Theory :-

Security Algorithm :

A security algorithm refers to a cryptographic method used to ensure the confidentiality and integrity of data transmitted over the GSM network.
The GSM network employs various security algorithms to protect communication between mobile devices and the n/w infrastructure.

GSM uses three different security algorithms called A3, A5 and A8. In practice, A3 and A8 are generally implemented together (known as A3/A8).

An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM n/w Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic. These protocols ensure that only authorized users can access the network and communicate securely.

- **A3 algorithm (Authentication):**

→ The A3 algorithm is responsible for the authentication of user's identity during the establishment of a connection with the GSM network.
It calculates the SRES (Signed Resource) based on the secret key K_i (stored on SIM card and in HLR and the Random challenge RAND sent by MSC).
SRES is then compared with expected SRES stored in the n/w's databases to verify the user's identity.
The algorithm is not standardized, meaning each GSM operator can choose its own implementation.

- **A8 algorithm (Key Generation):**

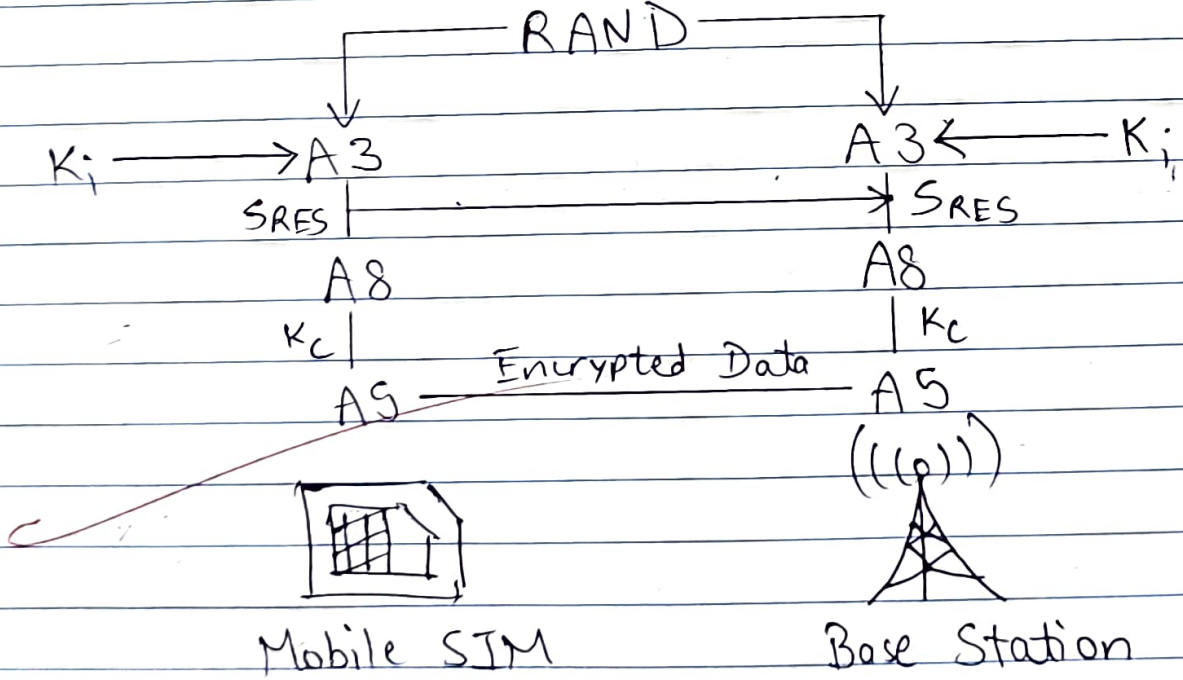
→ This algorithm is used to generate a session key K_c (cipher key) needed for encrypting the voice and data traffic between the mobile device and GSM network. It calculates the session key K_i and the random challenge RAND.
Session key K_c is unique for the each connection and ensures that communication b/w the mobile device and the n/w is fully secured.

A5 algorithm (Encryption)

→ A5 algorithm is used for encrypting the user's voice and data traffic over the air interface between the mobile handset and the base station subsystem (BSS) to ensure privacy and confidentiality.

- It operates as a stream cipher, where each bit of the data stream is encrypted very independently based on the session key K_c and the frame number.

A5 encryption is specified at international level to enable interoperability and roaming between different GSM networks.



- Flow Chart :

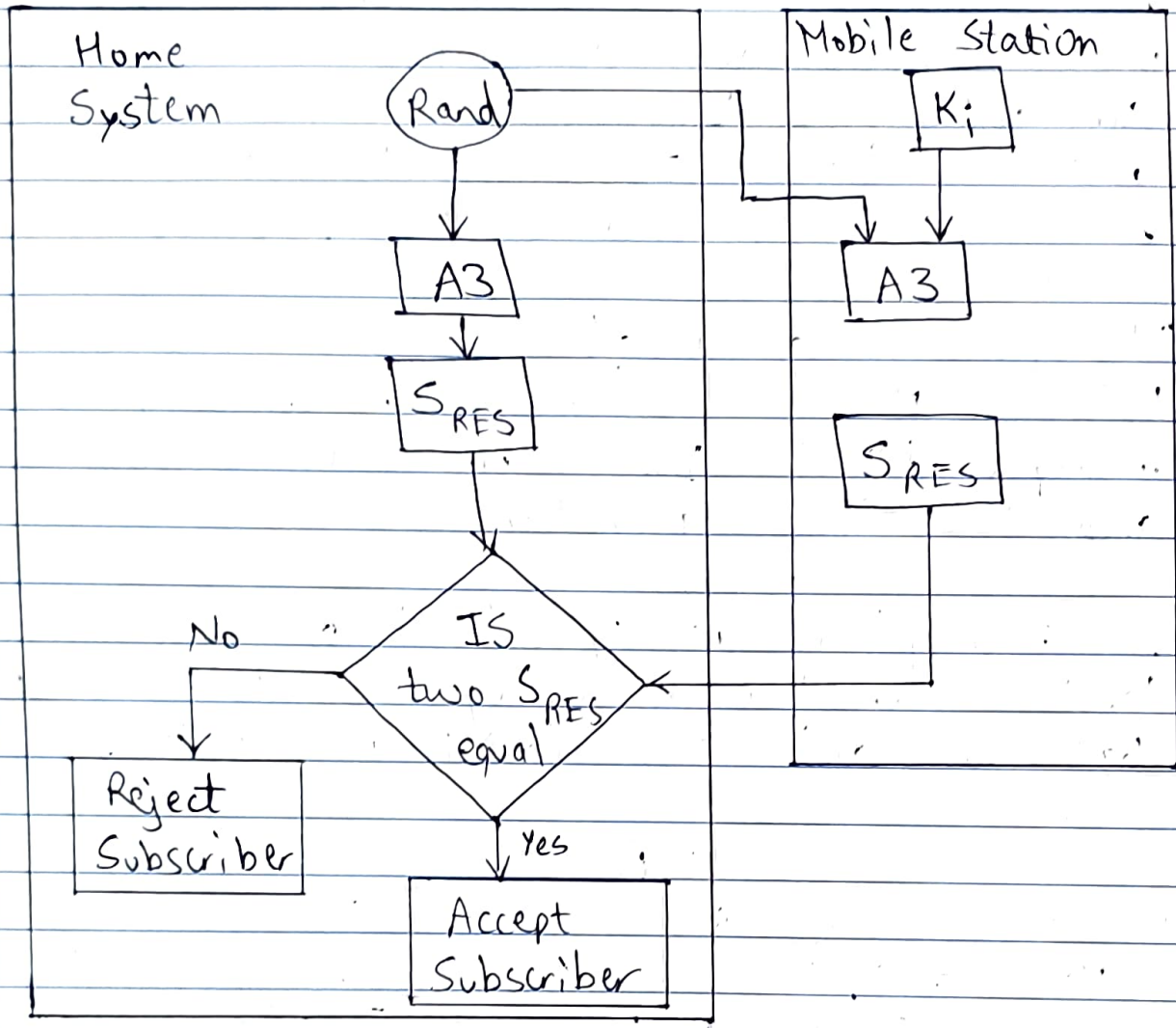


Fig. Authentication in GSM

Conclusion :-

Thus, implemented the GSM security algorithms A3 / A5 / A8.