UNIT - II

GSM

Security services :

1) Access control and authentication :

This ensures the authentication of a valid user for the SIM.

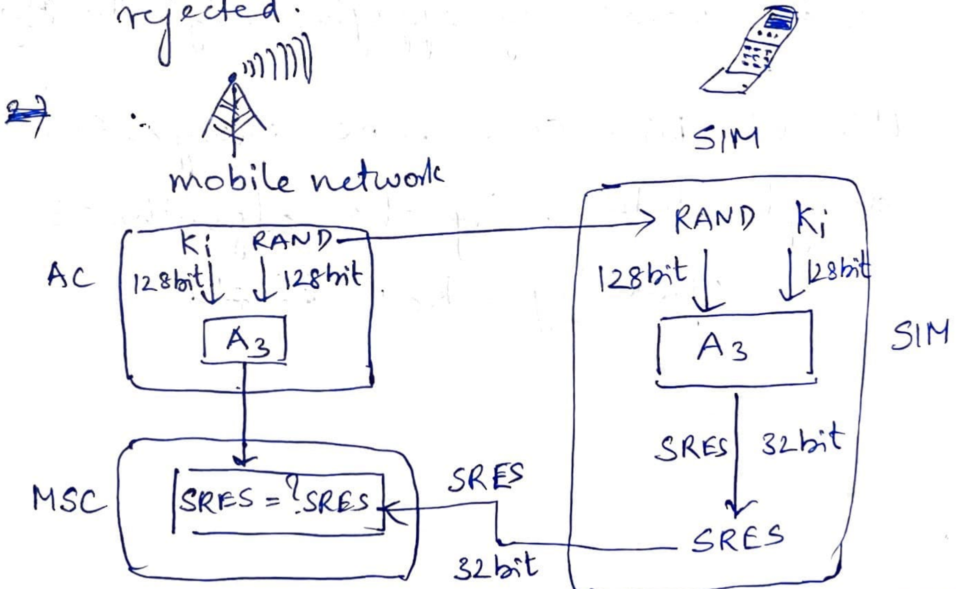
Authentication is based on the SIM which stores the individual authentication key k_i, user identification IMSI (international mobile subscriber identity) and the algorithm A_3.

challange response method for authentication:

- The access control AC generates a random number RAND as challenge and the SIM within MS answers with SRES (signed response) as response.

- AUC performs basic generation of random values RAND, signed responses SRES and cipher keys k_c for each IMSI and then forwards this information to the HLR. (home location register). The current VLR (Visitor location register) requests the needed values for RAND, SRES, k_c from HLR.

- For authentication, VLR sends the RAND to the SIM. Both sides, subscriber and network modules perform the same operation with RAND and key called A_3. MS (Mobile station) sends back the SRES generated by the SIM. VLR can compare both values and if they are same, VLR accepts subscriber else subscriber is rejected.



2) Confidentiality

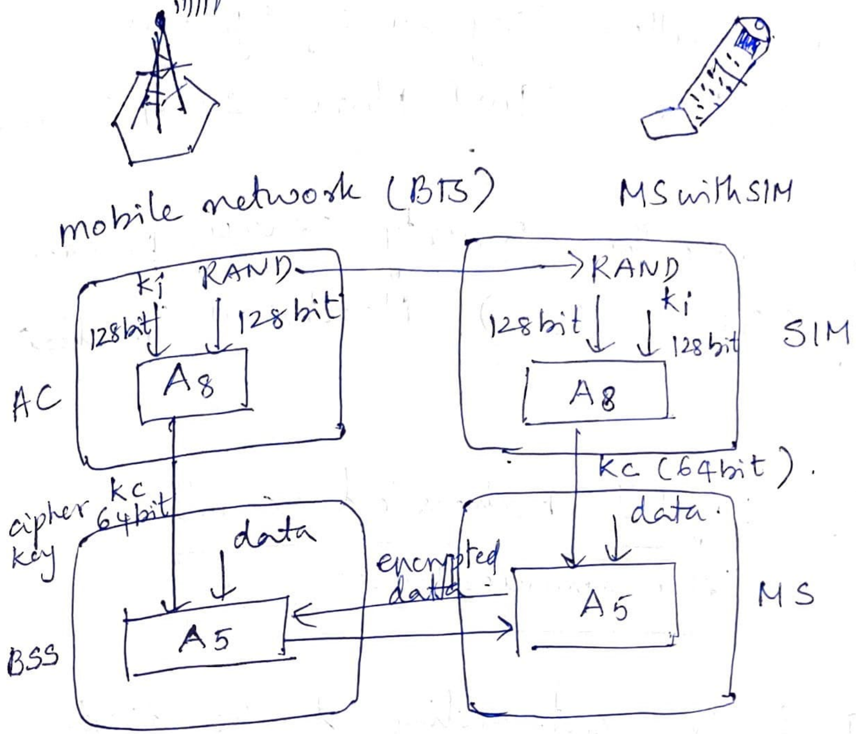
All user-related data is encrypted. After authentication, BTS (Base Transceiver station) and MS apply encryption to voice, data and signaling.

Encryption: All messages related to the user are encrypted in GSM over the air interface.

- MS and BSS (Base station subsystem) apply cipher, key, Kc. K_c is generated using the individual key k_i and a random value by applying algorithm A_8.

- MS and BTS can now encrypt and decrypt data using the algorithm A5 and cipher key, Kc. ~~kc the~~

Data Encryption



3) Anonymity: All data is encrypted before transmission and user identifiers are not used over the air.

GSM transmits a temporary identifier (TMSI) which is newly assigned by the VRL after each location update.

- Explain briefly about DECT with a neat labelled diagram of system architecture (9m) March 2021 (Backlog)

- What are the security services provided by GSM. (3m) March 2021 (Backlog)

DECT Digital Enhanced cordless Telecommunications

- DECT is an alternative to the digital system.
- DECT is mainly used in offices, on campus, at tradeshows.
- DECT can be used to bridge the last few hundred meters between a new network operator and customers.
- Using this small range, new companies can offer their service without having their own lines.

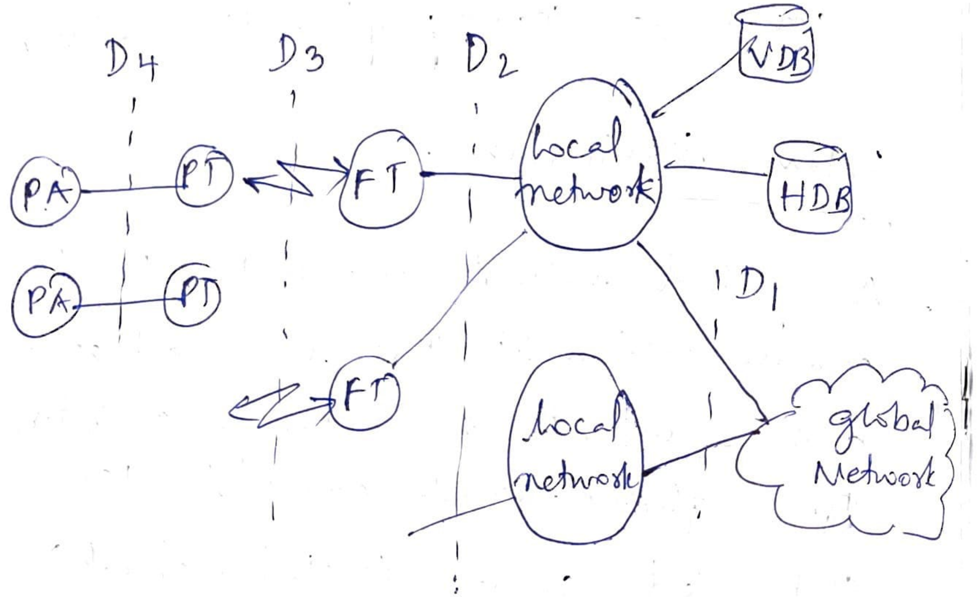
- DECT systems offer many internetworking units eg: with GSM, ISDN or data N/Ws.
- DECT is limited to about 300m range from the base station and with additional multiplexing techniques, DECT offers service to 10,000 people within one km^2.

System Architecture :

- A global network connects the local communication structure to the outside world and offers its services through an interface D$_1$. global networks could be ISDN (integrated services digital network), PSTN (Public switched telephone networks), PLMN (public land mobile networks) eg GSM or PSPDN (~~public~~ packet switched public data network).
- Services offered by these networks are

transportation of data, translation of addresses and routing of data between the local networks.

- DECT system architecture reference model



- local networks in DECT offer local telecommunication services like simple switching, intelligent call forwarding, address translation.

eg: analog or digital private branch exchanges (PBX) or LAN's.

- All network functions will be integrated in the local or global network where the databases, home database (HDB) and visitor data base (VDB) are located.

HDB, VDB support mobility similar to HLR, VLR in GSM.

Incoming calls are automatically forwarded to the current subsystem and current subsystem informs the HDB about the changes in the location.

- DECT core network consists of (FT) Fixed radio termination and (PT) Portable radio termination and provides multiplexing service.

FT, PT are at the fixed network side and mobile network side respectively.

- Several portable Applications (PA) can be implemented on a device.

Discuss Routing in Satellite networks
[(9m) April 2021 , Backlog.]

Routing in Satellite N/W's

- One way to route data transmission from one user to another is through ISL (intersatellite links).

- Through ISL's , traffic can be routed between the satellites.

- Assume two users of a satellite exchange data. One user sends data upto satellite and the satellite forwards it to the receiver ~~The last satelli~~ through other satellites. The last satellite now sends the data down to the earth. So one uplink and one downlink per direction is needed.

- This ability of routing within the satellite N/W reduces the no. of gateways needed on the earth.

Second method of routing is to relay all traffic to earth, route there and relay back to a satellite.

- Here the data sent by user is sent to a satellite and then forwarded to a gateway on earth.

- Routing takesplace until another gateway is reached. Again data is sent up to the satellite which forwards it down to the receiver. Here two uplinks and two downlinks are needed.

drawbacks of ISL's :

- depending on speed of routing ~~and on the orbit~~ in satellite network compared to the terrestrial N/W , ISL's might have lower latency

- More complex due to additional antennas and routing hardware for the satellite.

- higher fuel consumption and thus shorter lifetime.

What is uplink and downlink frequency band in GSM? (2m.)

- In satellite communication, a downlink is the link from a satellite down to one or more ground stations or receivers.
Uplink is the link from a ground station up to the satellite.

- GSM - 900 and GSM-1800 (digital cellular system) are mostly used.
GSM-900 uses 890 - 915 MHz to send information from the Mobile station to the Base Trancciver station (BTS). This is called the uplink and 935 - 960 MHz for the other direction which is called the downlink.