**20XW61 - Mobile Computing**

**Assignment Presentation**

**- By Kishor KR (20PW18)**

**Security in GSM**

**Security Services:**

1. Access control / authentication - Authentication process helps gsm network authenticate the right user. This process is based on exchanged secret key Ki which is known to AuC (Authentication Center) and SIM card. there is no provision to read the key Ki from the SIM
2. Anonymity **-** Here IMSI(International Mobile Subscriber Identity**)** is associated with a unique user (SIM), after the initial registration, a TMSI(Temporary Mobile Subscriber Identity) is assigned to the subscriber. The TMSI is stored along with the IMSI in the network HLR(Home location register).
3. Confidentiality - voice and signaling encrypted on the wireless link (after successful authentication)

**3 algorithms specified in GSM:**

1. A3 for authentication (“secret”, open interface)
2. A5 for encryption (standardized)
3. A8 for key generation (“secret”, open interface)

**Data services in GSM:**

* Data transmission standardized with only 9.6 kbit/s
  1. Advanced coding allows 14.4 kbits/s
  2. Not enough for internet and multimedia application
* **HSCSD (High-Speed Circuit Switched Data)**
* Already standardized
* High Speed Circuit Switched Data (HSCSD) is an enhancement in the data rate of circuit switched data in a GSM network.
* Building of several time-slots to get higher AIUR(Air Interference User Rate)
* Advantage : ready to use, constant quality, simple
* Disadvantage : channels blocked for voice transmission
* **GPRS (General Packet Radio Service)** : It is basically an up-gradation of the features of GSM (over the basic features). It allows a user to obtain a much better speed of data and provides them with simple and wireless access to the packet data networks as compared to the standard GSM technology.
* **GPRS network elements** :
  + The gateway GPRS support node (GGSN) converts the incoming data traffic coming from the mobile users through the Service gateway GPRS support node (SGSN) and forwards it to the relevant network, and vice versa. **The GGSN and the SGSN together form the GPRS support nodes (GSN)**.