Chapter 2

1. What is function of NSS in GSM?

Ans. **Network switching subsystem (NSS)**(or GSM core network) is the component of a GSM system that carries out call switching and mobility management functions for mobile phones roaming on the network of base stations.

2 Write types of TCH channels of GSM?

Ans. GSM has two types of traffic channels **TCH/FS** and **TCH/HS**. It is used both in the uplink and downlink after mobile has established connection with the GSM cell (BTS). It uses 26 frame multi frame structure.

TCH/FS stands for traffic channel at Full rate speech and TCH/HS stands for traffic channel at half rate speech. It uses normal burst structure .

3 Define a Interface?

Ans. A  *interface* is the point of interconnection between one entity like ms, bts etc… and to another entity as such. It works at different layers and in different form like air interface or PLMN interface etc.

4 List out subsystem of GSM

Ans. Radio subsystem

Network and switching subsystem and

Operation subsystem

5 Define term Base station subsystem (BSS).

Ans. Base Station Subsystem (BSS) connects the Mobile Station and the Network and Switching Subsystem (NSS).

6 What is Base transceiver station (BTS).

Ans. Base Transceiver Station corresponds to the transceivers and antennas used in each cell of the network. BTS is usually placed in the center of a cell and its transmitting power defines the size of a cell.

Function of BTS:

Provides 2 channels: signalling and Data channel.

Performs error protection coding for the radio channel

7 Define Base station controller(BSC).

Ans. Base Station Controller is the connection between the BTS and the Mobile service Switching Center (MSC) and manages the radio resources for one or more BTSs. BSC handles handovers, radio-channel setup, control of radio frequency power levels of the BTSs, exchange function, and the frequency hopping.

Function of BSC

Performs radio resource management.

Time and frequency synchronization signals to BTSs.

Time Delay Measurement and notification of an MS to BTS Power Management of BTS and MS.

8 What is Mobile station

Ans. Mobile Station (MS) consists of two main elements: mobile equipment or mobile device (that is the phone without the SIM card) and Subscriber Identity Module (SIM).

9 What are the functions of VLR?

Ans.  It is a database which consists of temporary information about subscribers which is used by MSC in order to provide services to visiting subscriber.

MSC updates the VLR by determining which users are in roaming.

Once, the roaming mobile information is updated, then MSC sends necessary information to roaming mobile subscribers so that roaming mobile call can be properly routed.

10 What are functions of equipment identity register?

Ans. The ***Equipment Identity Register*** (EIR) is a database that contains a record of the all the mobile stations (MS)that are allowed in a network as well as an database of all equipment that is banned, e.g. because it is lost or stolen.

The identity of the mobile station is given by the International Mobile Equipment Identity ([IMEI](http://www.telecomabc.com/i/imei.html)). Each time a call is made, the [MSC](http://www.telecomabc.com/m/msc.html) requests the IMEI of the mobile station, which is then send to the EIR for authorisation.

11 What is the function of Operation and maintenance center in GSM?

Ans. Operations and Support Subsystem (OSS) controls and monitors the GSM system.

OSS is connected to the different components of the NSS and to the BSC and also in charge of controlling the traffic load of the BSS.

12 Define term MSISDN.

Ans. Mobile Subscriber ISDN Number (MSISDN):

The MSISDN number is the real telephone number as is known to the external world.

13 List out types of handover.

Ans. There are four different types of handover in the GSM system, which involve transferring a call between:

1. Channels (time slots) in the same cell (Intra-cell handover).
2. Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC) (Inter-cell, intra-BSC handover)
3. Cells under the control of different BSCs but belonging to the same Mobile Switching Center (MSC) (Inter-BSC, Intra- MSC handover) .
4. Cells under the control of different MSCs (Inter-MSC handover).

14 Define term HSCSD?

Ans. **HSCSD** (High-Speed Circuit-Switched Data) is essentially a new high speed implementation of GSM (Global System for Mobile Communication) data transfer.

15 List out four possible handover scenarios in GSM.

Ans.

Intra cell

Inter cell, Intra cell BSC

Inter BSC, Intra MSC

Inter MSC

16 Which security services offered by GSM.

Ans. Link

<https://www.rfwireless-world.com/Tutorials/gsm-security.html>

LONG QUESTIONS

1 Explain in detail the Mobile services.

Ans. There are several types of mobile services that are accessible via a cellphone, namely: the mobile internet, mobile instant messaging, mobile chat rooms, mobile content services, and dating services.

The Mobile Internet

Mobile phones today are equipped with Internet browsers and large colour screens. This allows someone to easily access the World Wide Web and download online content or access online services. People can use their phones to search on Google, send emails, or access a website.

There is a move to develop websites that are cellphone friendly, that is; they arrange text and images in a way that is easy to read on the small screen of a cellphone. You may hear people talk about WAP (wireless application protocols) which supported mobile services that provide data from an online server to a cellphone. Yet, the trend is now to talk about having a dot mobi service, where the web address (or URL) will include .mobi at the end, for example: [www.bethehero.mobi](http://www.bethehero.mobi/).

The billing for accessing the Internet from a mobile phone is based on the amount of data downloaded (regardless of the time spent online). The price of data is determined by a mobile network provider.

Mobile Instant Messaging Services

Mobile instant messaging (MIM) services are the same as online instant messaging such as ICQ, Skype, and Windows Live Messenger except that it used on a cellphone. It allows users to communicate with one or more selected friends or contacts using text messages. Users will need to have downloaded or accessed an MIM service to their cellphone. To use the service users have to be logged on to the MIM service. This provides a common platform from which instant messages can be sent and read in real-time. The most well-known MIM in South Africa is Mxit.

These messages are sent via the mobile Internet and are billed as part of mobile Internet data charges. Since text messages use very little data, these messages are much cheaper than SMS messages – a reason for MIM’s wide appeal among teens.

Mobile Chat Rooms

Many MIM services include anonymous chat rooms. These chat rooms involve the exchange of information with a group of other users, usually in the form of text messages. Some chat rooms allow users to display an identifying photo or allow users to send pictures to each other. However, most chat rooms are anonymous where the real identity of a participant is not known to others. Some chat rooms are moderated but most are not. Anonymous chat rooms often have adult discussion topics and many contain X-rated statements.

Premium Rate Mobile Content Services

Most mobile content services – such as ringtones, logos, video clips, games and adult content – are sold using premium rate SMS. This involves sending a keyword via SMS to a shortcode, for example, sending BABY to 35050 at a once-off cost of R5.00 to get the baby ringtone on your cellphone. Ringtones are the most popular mobile content service among those under 25 years of age.

However, premium rate SMS services also allow a service provider to charge a subscription for mobile services – such as content, belonging to a club or joining a dating service. A subscription service involves an ongoing daily, weekly or monthly charge after a user has sent a keyword to a shortcode.

Examples of mobile phone subscription services

* **SMS a star sign to 31314 to receive a daily horoscope.** This services costs R5.00 charged every five days (that is, around R30.00 per month).
* **SMS the word FLIRT to 31500 to join a mobile dating service.** While the first week is free, the service thereafter costs R7.50 per week (at around R30.00 to R37.50 per month).
* **SMS the word GAME to 39912 to download games and mobile content** at a cost of R15.00 per week (at around R60.00 to R75.00 per month).

There are certain industry rules that all subscription services have to comply with, namely: the advertising rules are defined for all media types, there has to be a clear agreement during the initial purchase when a user opts-in to receive the subscription, no mobile service can charge over R300.00 per month for a single service without getting permission from a cellphone user, a mobile service provider needs to remind a user that they are subscribed to a service on a monthly basis, and to unsubscribe a user just needs to SMS “STOP” to the shortcake.

Mobile Dating Services

Mobile dating services allow individuals to meet, flirt, chat, and possibly become romantically involved by using SMS messaging, mobile chat rooms or the mobile Internet.

On registration to a dating service, a user creates a short profile with personal details – possibly including a photograph – which is stored against their cellphone number. When using the dating service, a user searches for other registered users with the criteria that may include: age, gender, sexual preference or location. Mobile dating services are also billed using premium rate SMS. Some are billed for each SMS sent but others are subscription based services providing access to a WAP or mobile Internet dating service.

2 Write short note on Bearer services.

Ans. In [telecommunications](https://en.wikipedia.org/wiki/Telecommunications), **Bearer Service** or **data service** is a service that allows [transmission](https://en.wikipedia.org/wiki/Transmission_(telecommunications)) of [information](https://en.wikipedia.org/wiki/Information) signals between network interfaces. These services give the subscriber the capacity required to transmit appropriate signals between certain access points, i.e. user network interfaces.

The bearer services include the following:

1. Rate adapted sub-rate information like circuit switched asynchronous and synchronous duplex data, 300-9600 bits.
2. Speech and data swapping during a call, i.e. alternate speech and data.
3. Modem selection, i.e. selection of 3.1 kHz audio service when inter-working with [ISDN](https://en.wikipedia.org/wiki/ISDN).

[Bearer services](https://en.wikipedia.org/w/index.php?title=Bearer_services&action=edit&redlink=1) GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services. Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission. Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. The only mechanism to increase transmission quality is the use of forward error correction (FEC), which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors. Depending on the FEC, data rates of 2.4, 4.8, or 9.6 kbit/s are possible. Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover. Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a radio link protocol (RLP). This protocol comprises mechanisms of high-level data link control (HDLC), (Halsall, 1996) and special selective-reject mechanisms to trigger retransmission of erroneous data.

3 Explain radio sub system (RSS)

Ans. As suggested by the name, the radio subsystem is comprised of all the radio specific elements, i.e. the mobile stations (MS) and the base station subsystem (BSS). The connection between the RSS and the NSS (shown in figure x.ii) via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines). The A interface is generally based on a circuit-switched PCM-30 system (2.048 Mbit/s), carrying up to 30 X 64 kbit/s connections, whereas the O interface uses the Signalling System No. 7 (SS7) based on X.25 carrying system management data to/from the RSS.

Base Station Subsystem (BSS): A GSM network is made up of many BSSs, each one being controlled by a base station controller (BSC). The main function of the BSS is to maintain the radio connections to an MS, however, it does have several other functions such as the coding/decoding of voice, and rate adaptation to/from the wireless network part. As well as a BSC, the BSS contains several BTSs.

Base Transceiver Station (BTS): A BTS contains all the radio equipment (antennas, signal processing, amplifiers) necessary for radio transmission. A BTS can be used to form a radio cell, or if sectored antennas are used, several cells. The BTS is connected to the MS by the Um interface, and the BSC by the Abis interface. The Um interface comprises of all the mechanisms necessary for wireless transmission (TDMA, FDMA). Abis interface consists of 16 or 64 kbit/s connections. The area coverage from a GSM cell can vary from 100m and 35km depending on the expected traffic and the location environment.

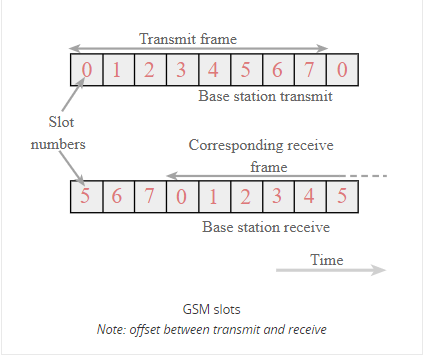
Base Station Controller (BSC): Basically, the BSC controls the BTS The functions of the BSC include reserving radio frequencies, handling handovers from one BTS to another and performing the paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.

Mobile Station (MS) : The MS is the user equipment which contains the software required for communication with the GSM network. The MS consists of user independent hard/software and the subscriber identity module (SIM), which stores the user specific data. While an MS can be identified via the international mobile equipment identity (IMEI)

Link <http://blueadmiral.com/Communications/comms/rss.shtml>

4 Explain GSM structuring of time using a frame hierarchy.

Ans. The basic element in the GSM frame structure is the frame itself. This comprises the eight slots, each used for different users within the TDMA system. As mentioned in another page of the tutorial, the slots for transmission and reception for a given mobile are offset in time so that the mobile does not transmit and receive at the same time.



The basic GSM frame defines the structure upon which all the timing and structure of the GSM messaging and signalling is based. The fundamental unit of time is called a burst period and it lasts for approximately 0.577 ms (15/26 ms). Eight of these burst periods are grouped into what is known as a TDMA frame. This lasts for approximately 4.615 ms (i.e.120/26 ms) and it forms the basic unit for the definition of logical channels. One physical channel is one burst period allocated in each TDMA frame.

In simplified terms the base station transmits two types of channel, namely traffic and control. Accordingly the channel structure is organised into two different types of frame, one for the traffic on the main traffic carrier frequency, and the other for the control on the beacon frequency.

5 Explain network and switching subsystem (NSS)

Ans.

* Central component of the Network Subsystem is the Mobile Switching Center (MSC).
* Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7).
* MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the callrouting and roaming capabilities of GSM
* MSC does the following functions:
  + it acts like a normal switching node for mobile subscribers of the same network (connection between mobile phone to mobile phone within the same network)
  + It acts like a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone).
  + It acts like a normal switching node for ISDN.
  + It provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers and call routing.
  + It includes databases needed in order to store information to manage the mobility of a roaming subscriber.
* GMSC is the interface between the mobile cellular network and the PSTN and also is in charge of routing calls from the fixed network towards a GSM user and vice versa
* GMSC is often implemented in the same node as the MSC
* GIWU (GSM Inter Working Unit) corresponds to an interface to various networks for data communications.

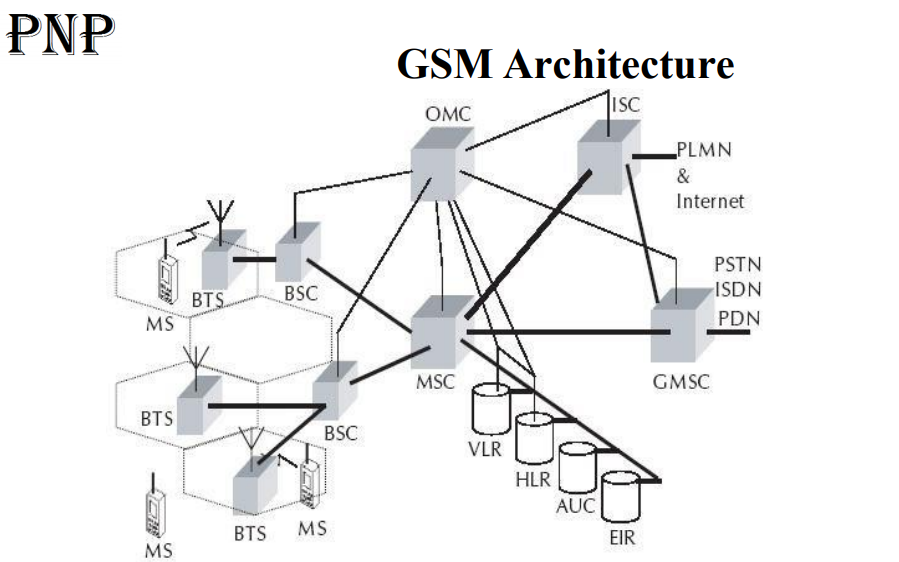
6 Explain operation subsystem (OSS).

Ans.

* Operations and Support Subsystem (OSS) controls and monitors the GSM system.
* OSS is connected to the different components of the NSS and to the BSC and also in charge of controlling the traffic load of the BSS.
* Equipment Identity Register (EIR) rests with OSS.
* EIR is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI)
* EIR contains a list of IMEIs of all valid terminals
* An IMEI is marked as invalid if it has been reported stolen or is not type approved
* The EIR allows the MSC to forbid calls from this stolen or unauthorized terminals
* Authentication Center (AUC) is responsible for the authentication of a subscriber
* AUC is a protected database and stores a copy of the secret key stored in each subscriber’s SIM card

7 Draw figure of functional architecture of a GSM system and explain.

Ans.



Cells are formed by the radio areas covered by a BTS (Base Transceiver Station)

Several BTSs are controlled by one BSC

Traffic from the MS (Mobile Station) is routed through MSC

Calls originating from or terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway MSC)

Explain this or

Link: <https://www.tutorialspoint.com/gsm/gsm_architecture.htm>

8 . Explain Control channels (CCH) of GSM.

Ans. The Common Control Channel (CCCH) is responsible for transferring control information between all mobiles and the BTS. This is necessary for the implementation of “call origination” and “call paging” functions. It consists of the following:

a. Random Access Channel ([RACH](https://en.wikipedia.org/wiki/Random-access_channel)) Used by the mobile when it requires gaining access to the system. This occurs when the mobile initiates a call or responds to a page.

b. Paging Channel (PCH) Used by the BTS to page MS, (paging can be performed by an IMSI, TMSI or IMEI).

c. Access Grant Control Channel (AGCH) Used by the BTS to assign a dedicated control channel to a MS in response to an access message received on the Random Access Channel. The MS will move to the dedicated channel in order to proceed with either a call setup, response to a paging message, Location Area Update or Short Message Service.

d. Cell Broadcast Channel (CBCH) This channel is used to transmit messages to be broadcast to all MS’s within a cell. The CBCH uses a dedicated control channel to send its messages, however it is considered a common channel because all mobiles in the cell can receive the messages.

Active MS’s must frequently monitor both BCCH and CCCH. The CCCH will be transmitted on the RF carrier with the BCCH.

OR

Reference link : <https://www.sciencedirect.com/topics/engineering/control-channel>

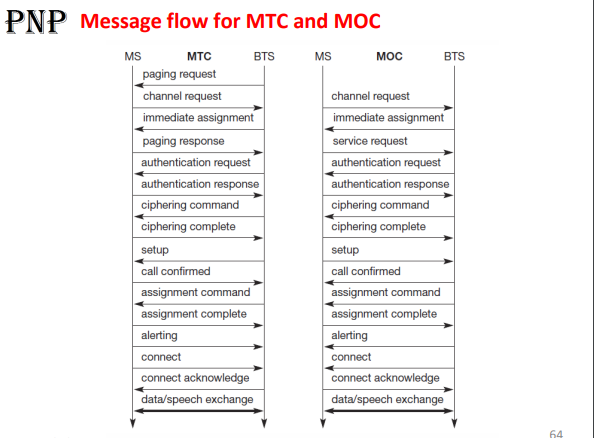
9 Explain the need to locate an MS and to address the MS.

Ans.

GSM (Global System for mobile communication) provides many useful services in which, one of the most important is the automatic, worldwide localization of users. The service provider system always knows where a user currently is, and the same phone number is valid worldwide.  
  
For localization of users, GSM performs periodic location updates even if a user does not use the mobile phones or some other devices but user should not be out of GSM network and is not completely switched off their devices.  
  
GSM uses two types of databases:  
  
Home Location Register (HLR)  
Visitor Location Register (VLR)  
  
The Home Location Register is a database from a mobile network in which information from all mobile subscribers is stored.  
  
The VLR contains the exact location of all mobile subscribers currently present in the service area.  
  
VLR is responsible for the MS (Mobile Station) to inform the HLR about location changes.  
  
As soon as user moves from one location to another location, the HLR sends all user data needed to the new VLR (New Location). Changing of one VLR to another VLR and their uninterrupted services is called as Roaming.  
  
Roaming can be taken place as follows:  
  
- Within the network of one provider  
- Between two providers in one country (National Roaming)  
- Different providers in different countries (International Roaming)  
  
To locate an MS and to address the MS, several numbers are needed:  
  
- Mobile station international ISDN number (MSISDN)  
- International mobile subscriber identity (IMSI)  
- Temporary mobile subscriber identity (TMSI)  
- Mobile station roaming number (MSRN)

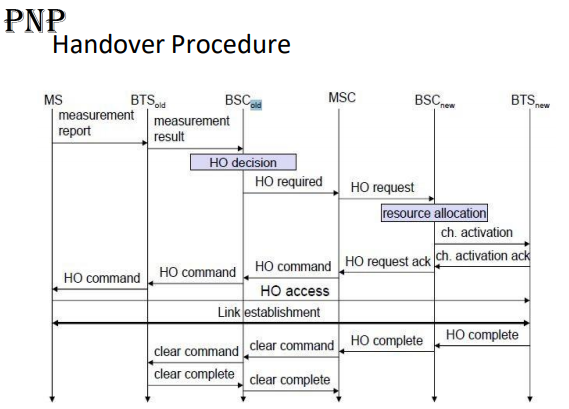
10 Explain Message flow for MTC and MOC.

Ans.



11 Explain handover procedures, for Cellular systems.

Ans,



Explanation:

Link : <https://www.sciencedirect.com/topics/computer-science/handover-procedure>

12 Explain Authentication process in GSM.

Ans.

In GSM, security is implemented in three entities: SIM card, GSM handset and Network. Subscriber identity module (SIM) contains: - IMSI - TMSI -PIN, -MSISDN -Authentication key Ki (64-bit) -Ciphering key (Kc) generating algorithm A8, and -Authentication algorithm A3. SIM is a single chip computer containing the operating system (OS), the file system, and applications. SIM is protected by a PIN and owned by an operator. SIM applications can be written with a SIM tool kit.

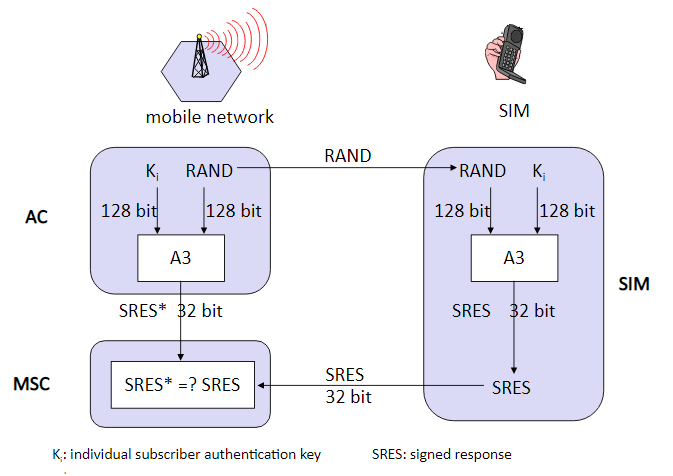
**GSM handset** contains ciphering algorithm A5.

**Network** uses algorithms

* A3 for Authentication,
* A5 for encryption: A5 is a stream cipher. It can be implemented very efficiently on hardware. Its design was never made public. A5 has several versions: A5/1 (most widely used today), A5/2 (weaker than A5/1; used in some countries), and A5/3 (newest version based on the Kasumi block cipher).
* A8 for ciphering the data; Ki and IMEI and IMSI of each subcriber are stored in the authentication center. Both A3 and A8 algorithms are implemented on the SIM. The operator can decide which algorithm is to be used. Implementation of an algorithm is independent of hardware manufacturers and network operators.

**1. Authentication of GSM mobiles:**

Authentication in the GSM system is achieved by the Base Station sending out a challenge to the mobile station. The MS uses a key stored on its SIM to send back a response that is then verified. This only authenticates the MS, not the user.



**Figure 15: process of authentication in GSM**

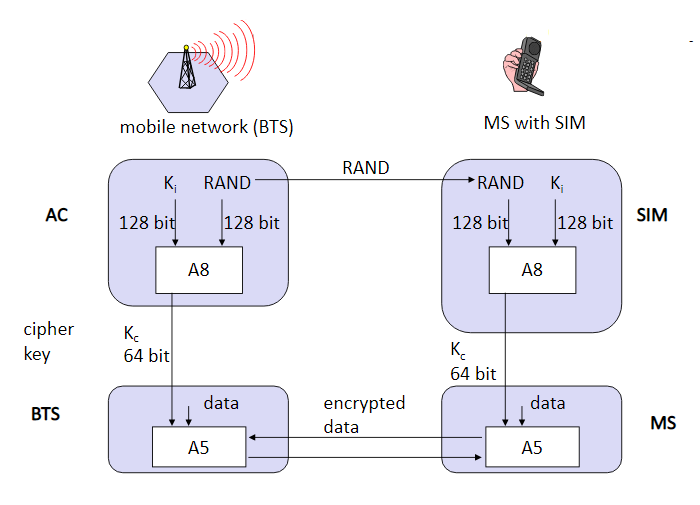
To request for a call or to receive a call, the MS has to get authenticated. The process is as follows:

* A unique subscriber authentication key is programmed on every SIM card. The authentication center (AuC) has a list which maps Ki number with the SIM card.It is a secure database.
* When a SIM card requests for a call, a 128 bit random number is instantaneously generated by the AuC and transmitted to the SIM card.
* The A3 algorithm which is programmed inside the SIM card processes the RAND number and Ki number and generates a 32 bit output called the Signed RESponse number (SRES).
* The same process is done on the AuC side.
* The SIM card transmits this SRES number to the AuC.
* The AuC compares the received SRES with the SRES that’s generated on the network side.
* The SIM is authenticated if and only if the two SRES are same.

The authentication centre contains a database of identification and authentication information for subscribers including IMSI, TMSI, location area identity (LAI), and authentication key (Ki). It is responsible for generating (RAND),response (RES), and ciphering key (Kc) which are stored in HLR / VLR for authentication and encryption processes. The distribution of security credentials and encryption algorithms provides additional security.

**2. Encryption in GSM:**

GSM uses information stored on the SIM card within the phone to provide encrypted communications and authentication. GSM encryption is only applied to communications between a mobile phone and the BS. The rest of the transmission over the normal fixed network or radio relay is unprotected, where it could easily be eavesdropped or modified. In some countries, the base station encryption facility is not activated at all, leaving the user completely unaware of the fact that the transmission is not secure. GSM encryption is achieved by the use of a shared secret key. If this key is compromised it will be possible for the transmission to be eavesdropped and for the phone to be cloned (i.e., the identity of the phone can be copied). A 64-bit key is divided to provide data confidentiality. It is not possible to encrypt all the data; for example, some of the routing information has to be sent in clear text. The detailed process of Encrypting the data is as shown in Figure 16.

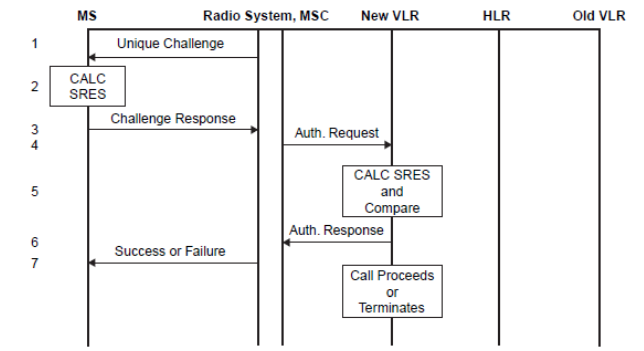


**Figure 16: process of authentication in GSM**

* The AuC generates a random number (RAND ) of 128 bits and sends it to the MS.
* The RAND and the Ki number is processed by the A8 algorithm on both the sides.
* The A8 algorithm produces a 64 bit ciphering key (Kc). Ciphering means scrambling or randomizing the data.
* The A5 algorithm takes Kc key and data to be transmitted as input and and accordingly encrypts the data.
* A5 algorithm is different for each service provider and is highly secretive.

**3. GSM Token-based challenge**

The security-related information consisting of triplets of RAND, signature response (SRES), and Kc are stored in the VLR. When a VLR has used a token to authenticate an MS, it either discards the token or marks it used. When a VLR needs to use a token, it uses a set of tokens that is not marked as used in preference to a set that is marked used. When a VLR successfully requests a token from the HLR or an old VLR, it discards any tokens that are marked as used. When an HLR receives a request for tokens, it sends any sets that are not marked as used. Those sets shall then be deleted or marked as used. The system operator defines how many times a set may be reused before being discarded. When HLR has no tokens, it will query the authentication centre for additional tokens. The token-based challenge can be integrated into various call flows (e.g., registration, handoff). It is described separately here for clarity. Figure 17 shows the call flows of token-based challenges.



**Figure 17: GSM token-based challenge**

* The serving system sends a RAND to the MS.
* The MS computes the SRES using RAND and the authentication key (Ki) in the encryption algorithm.
* The MS transmits the SRES to the serving system.
* The MSC sends a message to the VLR requesting authentication.
* The VLR checks the SRES for validity.
* The VLR returns the status to the MSC.
* The MSC sends a message to the MS with a success or failure indication.

Both GSM and North American systems use the international mobile equipment identity (IMEI) stored in the equipment identity register (EIR) to check malfunctions and fraudulent equipment. The EIR contains a valid list (list of valid mobiles), a suspect list (list of mobiles under observation), and a fraudulent list (list of mobiles for which service is barred).

13 Explain Encryption process in GSM.

Ans.

GSM is the abbreviated term for General System for Mobile communications and this is known as a standard for the mobile phone telephony system. And, the process in which phone conversations is messed up via a network while making use of GSM is called GSM encryption. Once GSM encryption has been executed it is no longer possible to descramble phone conversations and private communications may also be interrupted by vicious crooks.

There is a big chance that terrorists and aggressive countries will make use of GSM encryption in their activities. Hence, the Western intelligence agencies are alarmed regarding the threats that may be brought about when such codes are executed and used in evil deeds.

It is acknowledged by many experts that one of the best qualities of GSM is its unique security feature. With its protective functions, GSM is considered to be the safest cellular telecommunications protocol globally. Having complicated encryption algorithms is the greatest factor that made GSM the most secured standard of all.

The complex process of GSM’s security involves encryption

Of conversation with the use of an impermanent and randomly-produced ciphering key. Security is amplified as short-term identity is used to name a subscriber and this may also be modified as time passes by.

However, experts are still alarmed with the level of security of the GSM codes even if it has already been proven that GSM’s security is created intricately. And, the apprehensions of the authorities were substantiated upon initiation of the experimental trials in which the access into the GSM codes was forced.

Security-related agencies from different countries like USA, UK, and France requested that the export of encryption tool should be confined so as to prevent invaders and terrorists from using it in carrying out their wicked plans. As a sample scenario, terrorists may hold back the authorities from finding them if they have in their possession the encryption codes designated for cellular telecommunications.

TRUE/FALSE

1 T

2 F

3 T (may be)

4 T

5 T

6 T

7 T

8 T

9 T

10 T