MODEL ANSWER

SUMMER - 2017 EXAMINATION

Subject: Mobile Computing **Subject Code:** **17632**

Important Instructions to examiners:

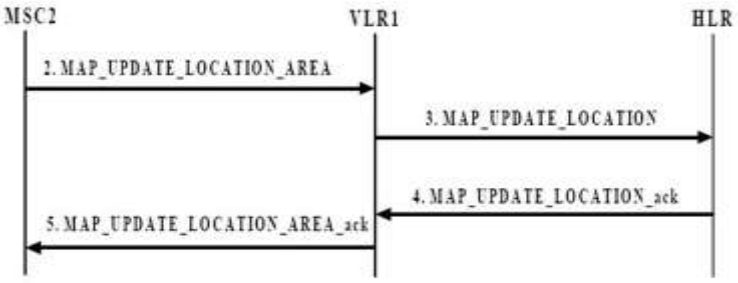
1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given moreImportance (Not applicable for subject English and Communication Skills).
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q.No.	Sub Q.N.	Answer	Marking Scheme
1.	**(A)**	**Answer any THREE of the following:**	**12**
	(a)	**Enlist the mobile computing devices.**	**4M**
	Ans.	**Mobile computing devices are:** 1. Laptop (notebook computer or notepad) 2. Mobile phone 3. Personal Digital Assistant 4. Pager/Beeper 5. Sensor and Embedded Controller 6. GPS Navigation device	***Any 4 devices 1M each***
	(b)	**State any four services of GSM.**	**4M**
	Ans.	**Four services of GSM:** 1. Emergency calling 2. Facsimile 3. SMS 4. Bearer /data Services 5. Call forwarding 6. Call hold 7. Call waiting 8. Caller line ID	***Any 4 services 1M each***

MODEL ANSWER

SUMMER - 2017 EXAMINATION

Subject: Mobile Computing **Subject Code:** **17632**

	(c) Ans.	**Write the steps of Inter-MSC movement of location update procedure.** In this case, two LAs belong to different MSCs of the same VLR. The location update procedure is as follows: **Steps 1 and 2:** • The location update request is sent from the MS to the VLR **Step 3:** • VLR updates the LAI and the MSC fields of VLR record, and derives the HLR address of the MS from the MS's IMSI • VLR sends the MAP_UPDATE_LOCATION message to the HLR. It gives the following details ➢ IMSI of the MS ➢ Address of the target MSC (i.e., MSC2) ➢ Address of the target VLR (i.e., VLR1)   **Step 4:** • HLR identifies the MS's record by using the received IMSI • MSC number field is updated • An acknowledgment is sent to the VLR	**4M** ***Relevant procedure 4M***

MODEL ANSWER

SUMMER - 2017 EXAMINATION

Subject: Mobile Computing **Subject Code:** **17632**

(d) **Differentiate between symmetric key cryptography & public key cryptography.** **4M**

Ans.

Sr No.	symmetric key cryptography	public key cryptography.
1	Also called as private key	Also called as asymmetric key
2	Only one key is used:Private key	Two keys are used: Public and private
3	The key is kept secret	Public key is freely available to all, while private key is a secret key
4	Same key is used for encryption and decryption.	One key is used for encryption while other is decryption.
5	Faster than public key cryptography	Slower than symmetric key cryptography
6	It is used for encrypting small or large messages.	It is used for encrypting small messages.

Relevant four points 4M

1. **(B)** **Answer any ONE of the following:** **6**

(a) **Write the steps for HLR failure restoration procedure.** **6M**

Ans. **HLR failure restoration:**

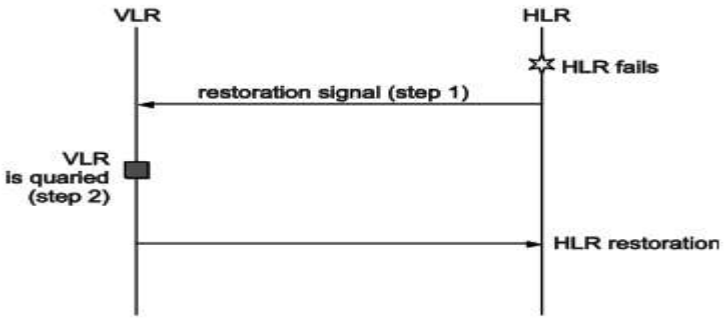
In GSM HLR, it is compulsory to save the updae into non-volatile storage. Changes of service information are backup immediately after every update and the location information is periodically transferred from HLR into backup. The service information is update infrequently because not all the subscriber chages their service profile after subscription.

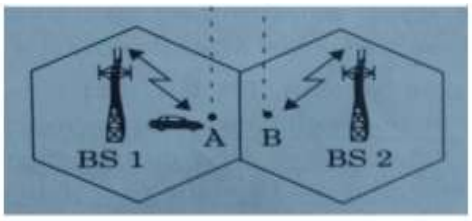
After HLR failure, the data in the backup are reloaded into the HLR. We also have 'uncovered period' as a time interval after last backup operation and before the restart of the HLR data that changes in the uncover period cannot be recoverd. The following HLR restoration procedure is executed.

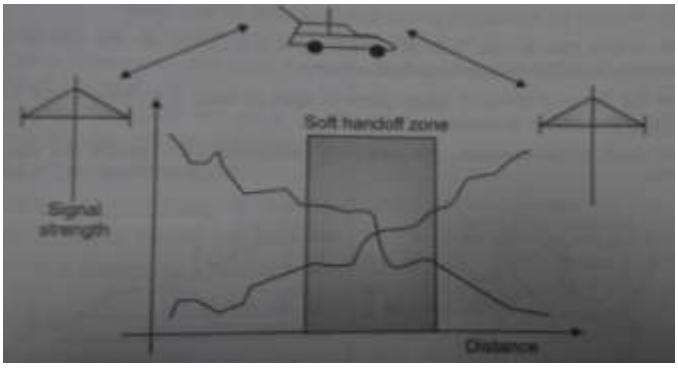
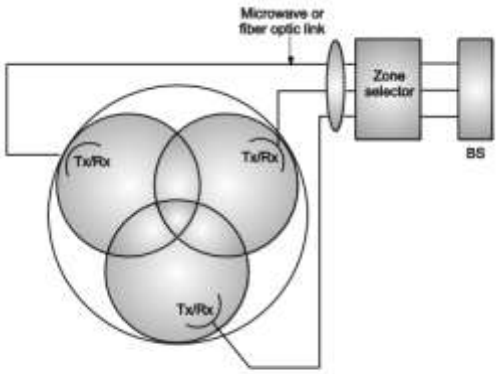
Proper steps with diagram 6M

Step 1: The HLR sends an signalling system 7 (SS7) TCAP (Transaction Capability Application Part) message. MAP_RESET to the all VLRs where its MSs are located (that is restoration signal).

Step 2: Each VLR that receives the restoration signal from HLR is queried to search the lost location information of user.

		Step 3: All the VLRs derived all MSs of the HLR, and for each MS, they send an SS7 TCAP message, MAP_UPDATE LOCATION, to the HLR.  	
	(b) Ans.	**Write steps to develop a User Interface for login (Assume two textboxes labelled as Username & Password and two buttons labelled as Submit & cancel)** **Open eclipse:** 1. Click the menu File → New Android Application Project 1. Name the project: In this stage, there exist three names described as: Specify Application Name, Project Name, Package name. 2. Click Next 3. Configure Launcher Icon 4. Choose "Blank Activity" Click next 5. It will display Activity Name and Layout Name Click finish 6. In Activity_main.xml file under text field folder we can see the different types of text fields for providing text, password, numbers, email-id etc. 7. Drag the desired text field on the graphical layout of the GUI and enter the desired input in respect to the type of text filed 8. Select another text field and provide the input 9. From the form widgets menu select the buttons you want and rename it as required **Output:** To run User **Interface** application launch **AVD (Android virtual Device)**	**6M** ***Proper steps 6M***

		Open project's activity files from eclipse and click Run icon from the toolbar. Eclipse installs the app on your AVD and starts it and if everything is fine with your setup and application, it will display following Emulator window. You can also run this application directly on your android device instead of AVD, First you need to enable USB debugging on your phone, then connect it to your computer via USB. Then eclipse will automatically start debugging on your phone instead of the AVD.	
2.	**(a)** Ans.	**Answer any FOUR of the following:** **Explain Handoff strategies with neat sketch.** When a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station. This process of transferring call to a new base station is called as Hand off.  **Types:** 1. Soft Handoff 2. Hard handoff 3. Delayed handoff 4. Queued handoff 5. C/I handoff 6. Mobile assissted handoff **Soft Hand off (Operational Procedure):** The handoff from CDMA cell to CDMA cell at the same CDMA frequency is called soft hand off. There is no need to change from one frequency to another frequency but change from one code to another code. The ability to select between the instantaneous received signals from a variety of base stations in a CDMA system is called soft hand off. **Diagram:**	**16** **4M** ***Handoff 1M*** ***Any 2 types 1M*** ***Explanation any one 1M***

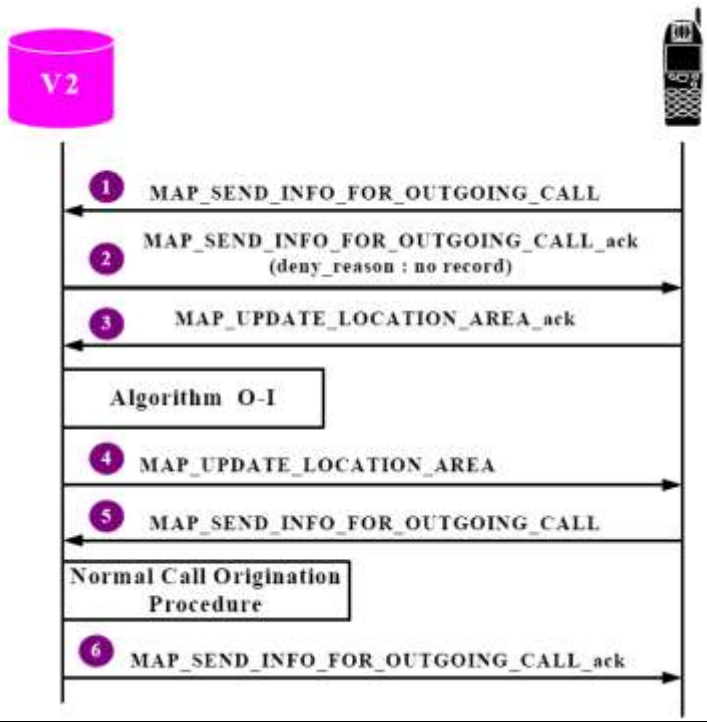
			***Diagram 1M***
	(b) Ans.	**Explain microcell zone concept briefly**.  **The Microcell concept, BS - Base station** • When sectoring is employed, lot of handoffs is required due to this load on switching and control link element of the mobile system increases. • To solve this problem, a microcell concept for seven cell reuse is used. • In this scheme, each of three (possibly more) zone sites are connected to single base station. The zone are connected by a co-axial, fibre optic cable or microwave link to a base stations. • Multiple zones and single station make a cell. As mobile travels within a cell, it served by zone with strong signal. • As mobile moves from one zone to another zone in same cell, it uses same channel, thus like a sectoring, handoff is not required at mobile switching centre (MSC) when mobile travels within the	**4M** ***Diagram 2M*** ***Explanation 2M***

		cell in different zone. • The base station simply changes the channel from one zone to another zone, and channel is active in particular zone in which mobile is travelling, hence interference is reduced. • The advantage of zone cell technique is that, cell maintains particular area of coverage, the co-channel interference in cellular system is reduced, as larger control base station is replaced by zone transmitter on edge of cell.	
	(c) Ans.	**Define the following identifiers:** **(i) MSISDN (ii) IMSI (iii) IMEI (iv) TMSI** **(i) MSISDN (Mobile Station ISDN number**) - A MSISDN uniquely classifies a subscription in the Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS) networks. It is the telephone number of the Subscriber Identity Module (SIM) card displayed on mobile or cellular phones. **(ii) IMSI (International Mobile Subscriber Identity**) - Which uniquely identifies the MS. It is used as the key to search any data the databases in VLR, HLR and GSN. An international mobile subscriber identity (IMSI) is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber. **(iii) IMEI (International Mobile Equipment Identity)** - IMEI is a 15- or 17-digit code that uniquely identifies mobile phone sets. The IMEI code can enable a GSM (Global System for Mobile communication) or UMTS (Universal Mobile Telecommunications Service) network to prevent a misplaced or stolen phone from initiating calls. **(iv) TMSI (Temporary mobile subscriber identity)** - Which is the GPRS equivalent of TMSI in GSM. Temporary Mobile Subscriber Identity for most commonly sent between the mobile and the network.. The TMSI number is local for a specific local area, and need to be updated every time when the mobile moves to a new geographical area. Paging a mobile is the key use of the TMSI.	**4M** ***Each definitio n 1M***

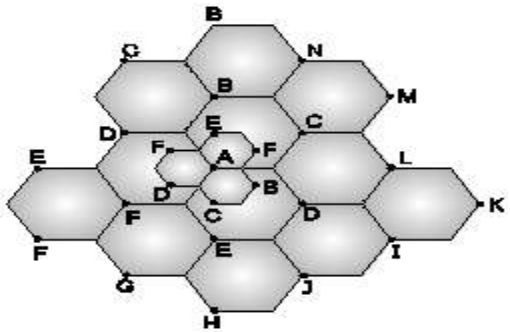
MODEL ANSWER

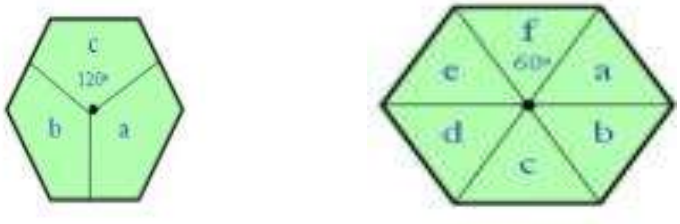
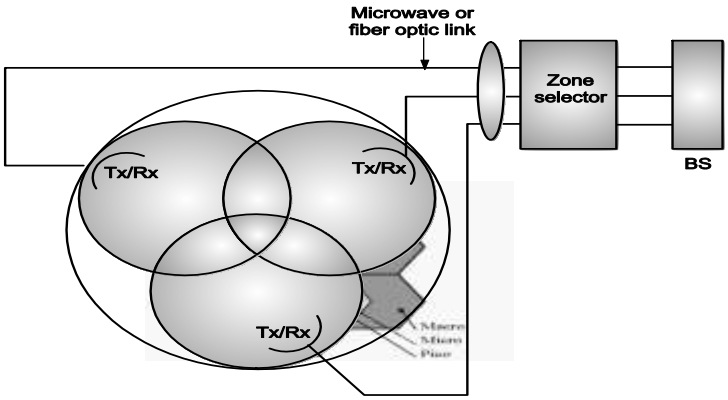
SUMMER - 2017 EXAMINATION

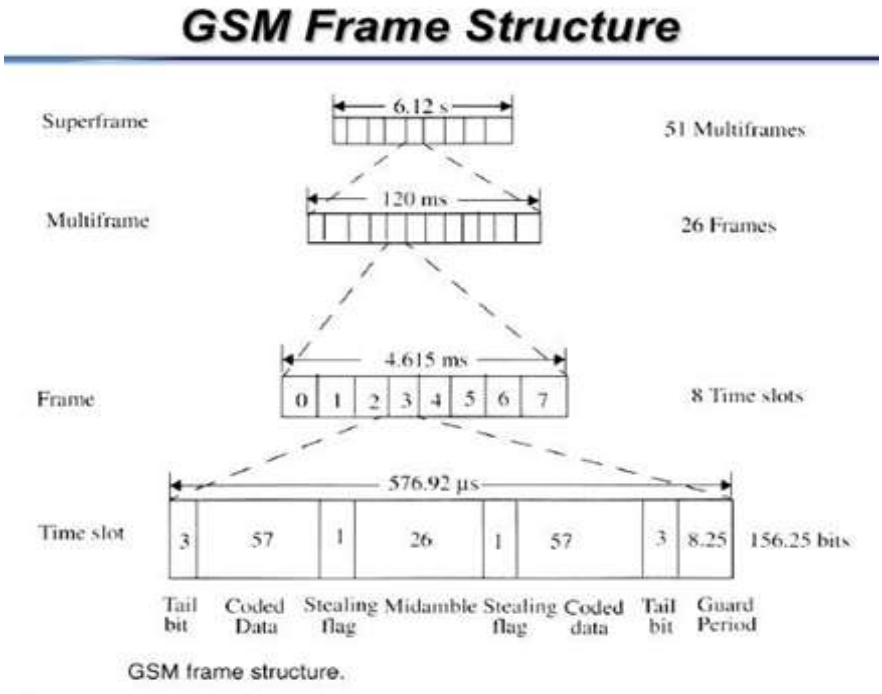
Subject: Mobile Computing **Subject Code:** **17632**

	(d) Ans.	**Write algorithm for call origination of VLR overflow with neat sketch.** **Call origination:** • Step 1. The MS sends the call origination request to V2 • Step 2. V2 cannot find u1*'s record, and* denies the call request • Steps 3 and 4. The MS initiates the registration procedure; Algorithm O-I is executed • Steps 5 and 6. The MS reissues the call origination request, and the normal call origination procedure is executed  	**4M** ***Proper steps, diagram 4M***

	(e) Ans.	**State applications and limitations of GPRS.** **Applications:** **1. Mobility** - The ability to maintain constant voice and data communications while on the move. **2. Immediacy** - Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session. **3. Localization** - Allows subscribers to obtain information relevant to their current location. **4.** Still images such as photographs, pictures, postcards, greeting cards and presentations, static web pages can be sent and received over the mobile network. **Limitations:** **1.** Limited Cell Capacity for All Users: GPRS does impact a network's existing cell capacity. There are only limited radio resources that can be deployed for different uses **2.** Speeds Much Lower in Reality **3.** Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight timeslots without any error protection. Transit Delays GPRS packets are sent in all different directions to reach the same destination. This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link.	**4M** ***Any 2 applications 2M*** ***Any 2 limitations 2M***
	(f) Ans.	**Explain RSA algorithm.** RSA is named after it's inventors: Ron Rivest, Adi Shamir, and Len Adleman at MITRSA is public key algorithm. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024. Before stating RSA let us see main ingredients used in algorithm: p,q, two prime numbers : (private, chosen) n = pq : (public, calculated) e, with gcd (f(n),e) = 1; 1< e < f(n): (public, chosen) d k e-1 (mod f(n)) : (private, calculated) RSA algorithm works as follow:	**4M** ***Explanation RSA algorithm 4M***

		1. Choose two prime numbers p and Q. 2. Multiply p and q to generate n. n will be used as the modulus. 3. Calculate ϕ (n) = (p-1) * (q-1). ϕ (n) is the Euler's totient function. ϕ (p) is the number of positive integers less than p and relatively prime to p. 4. Choose a number e such that it is relatively prime to ϕ (n). 5. Find d such that it is multiplicative inverse of e, $d = e^{-1} \bmod \phi$ (n). 6. (e,n) is the public key and (d,n) is the private key. 7. To encrypt, we use the formula (Ciphertext block) = (Plaintext block)^e mod n. 8. To decrypt, we use the formula (Plaintext block) = (Ciphertext blcok)^d mod n.	
3.	**(a)** Ans.	**Answer any FOUR of the following:** **Explain the techniques for improving coverage and capacity in celluar systems.** Techniques for improving coverage and capacity of celluar system are: - Cell Splitting: It is the process of subdividing a congested cell into smaller cells, - It increase the capacity of cellular system line it increases the number of times channels are reused. - By defining new cells which have smaller radius than original cells and by installing by these smaller cells (microcells) between existing cells.  **Fig: Cell Splitting** Sectoring uses directional antenna to control interference and frequency reuse.	**16** **4M** ***Explanation 4M***

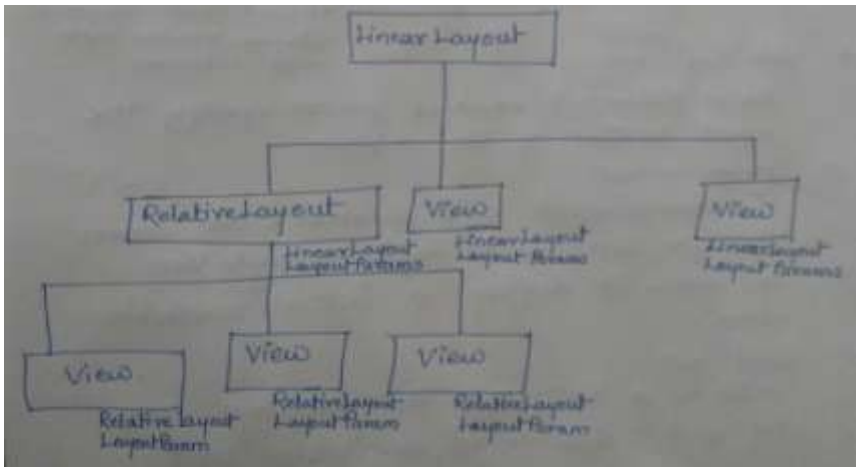
		A cell is normally partitioned into 3 sectors 120^0, each sectors or 6 sectors 60^0 each.  **Coverage zone (Microcell concept):** - When sectoring is employed, lot if handoff is required due to this load on switching and control link element of the mobile system increases. To solve this, a microcell concept for seven cell reuse is used. - Each of three zones sites are connected to single base station. - Zones are connected by co-axial fibre optic cable or microwave link to a base station.  	
	(b) Ans.	**Explain the GSM frame structure.** **Frame structure in GSM:** • The length of GSM frame in a frequency channel is 4.615 ms. • The frame is divided into 8 bursts of length of 0.577ms • The timeslots in the uplink are derived from downlink by a time delay of 3 time slots • This arrangement prevents an MS from transmitting and receiving at	**4M** ***Explanation 2M***

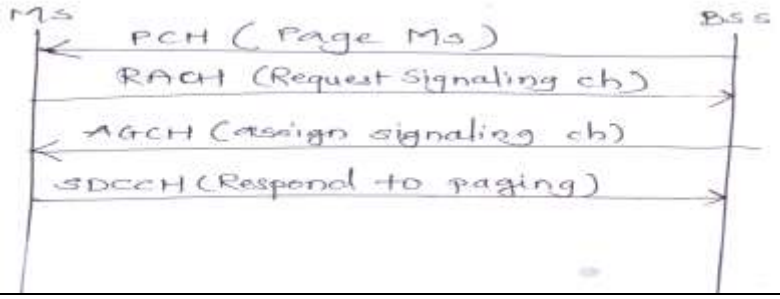
		the same time • However, due to propagation delay (when MS is far away from BTS) the 3 TS delay cannot be maintained accurately  GSM frame structure. **GSM Burst structure:** • Each burst contains 148 bits (0.546ms) followed by 0.031ms guard time (8.25bits) • The burst begins with 3 head bits and 3 tail bits (logical Zeroes) • Two groups are data bits are separated by an equalizer Training sequence of 26 bits • Each data group consists of 57 bit information bits and 1 flag that indicate whether the information bits are for user speech/ data or signaling.	***Diagram 2M***
	(c) Ans.	**Explain VLR Failure Restoration procedure.** **VLR Failure Restoration:** Ater a VLR failure, the service information of a VLR record is recovered by the first contact between the VLR and the HLE of the	**4M**

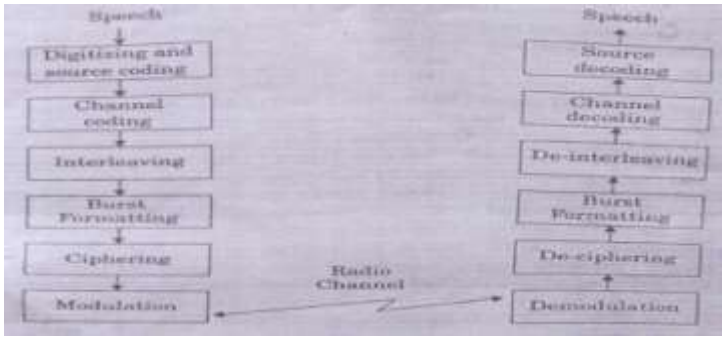
		corresponding MS. The location information is recovered by the first radio contact between the VLR and the MS. The mobile station information is recovered either by contact with the HLR or MS. VLR record restoration is intitiated by one of the three events. 1) MS registration 2) MS call originaton 3) MS call termination **1) MS Registraion:** Since the VLR record was erased by the failure, the VLR considers the registration as a case of inter-VLR movement. Following the normal registration procedure defined in inter-VLR movement, the VLR record is recovered. In this case, TMSI sent from the MS to the VLR cannot be recognized, and the MS is asked to send IMSI over the air. **2) MS call originaton:** When the VLR receives the call origination request MAP_SEND_INFO_FOR_OUTGOING_CALL from the MSC, the VLR record for the MS is not found. The VLR considers the situation as system error, with the cause "unidentified subscriber". The request is rejected, and the MS is asked to initate the location registration procedure. After the registration procedure, the VLR record is recovered. **3) MS call termination:** **Step 1 and 3**: The IMSI and the MSC no. are provided in the MAP_PROVIDE_ROAMING_NUMBER message sent from the HLR to the VLR. The VLR searches the MS record by using the received IMSI. Since the record has been erased after the failure, the search fails. The VLR creates a VLR record for the MS. Neither the service nor the location information is available in this record. **Step 4 and 7:** Since the VLR does not have the routing information, it uses the MSC no. provided by the MAP_PROVIDE_ROAMING_NUMBER message to create the MSRN. The no. is sent back to the gateway MSC to set up the call. **Step 5 and 6:** The VLR recovers the receive information of the VLR record by sending a MAP_RESTORE_DATA message to the HLR.	***Explanation 4M***

		Step 8: After the gateway MSC receives the MSRN. The SST ISUP message IAM is sent to the target MSC. **Step 9 and 11:** The target MSC does not have the LA information of the MS. In order to procedd to set up the call, the MSC sends the message MAP_SEND_INFO_FOR_INCOMING_CALL to the VLR. The VLR does not have the LAI information either. Hence, the VLR asks the MSC to determine the LA of the MS by sending a MAP_SEARCH_FOR_MOBILE_SUBSCRIBER message. **Step 12 and 13:** The MSC initiaties paging of the MS in all Las. IF the paging is successful, the current LA address of the MS is sent back to the VLR. At this point the location information of the VLR record is recovered.	
	(d) Ans.	**Explain the functions of GPRS support nodes.** **Serving GPRS Support Node: (SGSN):** A seving GPRS support node (SGSN) is at the same hierarchical level as the MSC. Whatever MSC does for voice, SGSN does the same functions for packet data. SGSN's tasks include packet switching, routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles of all GPRS users registered with this SGSN. SGSN sends queries to Home Location Register (HLR) to obtain profile data of GPRS subscribes. The SGSN is connected to the base station system with Frame Relay. **Gateway GPRS Support Node (GGSN):** A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks. GGSN's function is similar to that of a router in a LAN. GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like Internet or X.25. PDP sends these packets out on the corresponding packet data network. In the other direction, PDP receives incoming data packets from data networks and converts them	**4M** ***Functions of GPRS support nodes 4M***

		to the GSM address of the destination user. The readdressed packets ar sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN also performs authentication and charging functions related to data transfers.	
	(e) Ans.	**Write features of Android OS.** **Features of Android OS:** **1. Near Field Communication (NFC)**: Most Android devices support NFC, which allows electronic devices to easily interact across short distances. **2. Custom ROMs**: Android operating system is open source, developers can tweak the current OS and build their own versions, which users can download and install in place of the stock OS. Some are filled with features, while others change the look and feel of a device. Chances are if there's a feature you want, someone has already built a custom ROM for it. **3. Widgets**: Apps are versatile, but sometimes you want information at a glance instead of having to open an app and wait for it to load. Android widgets let you display just about any feature you choose, right on the home screen—including weather apps, music widgets, or productivity tools that helpfully remind you of upcoming meetings or approaching deadlines. **4. Custom Home Screens**: While it's possible to hack certain phones to customize the home screen, Android comes with this capability from the get-go. Download a third-party launcher like Nova, Apex or Slide and you can add gestures, new shortcuts, or even performance enhancements for older-model devices.	**4M** ***Features of android OS 4M***
	(f) Ans.	**Explain UI layouts available in Android environment.** **UI Layouts:** • UI Layouts are subclasses of ViewGroup class. • Typical layout defines the visual structure for and Android user interface and can be created either at run time using view/ViewGroup objects or you can declare your layout using XML file main_layout.xml which is located in res/layout folder of your project.	**4M**

		 There are number of layouts provided by Android which you will use in almost all the Android applications to provide different view, look and feel. 1. Linear Layout- aligns children in single direction, vetically or horizontally 2. Relative Layout- Displays child views in relative position 3. Table Layout- Table Layout enables you views into rows and columns 4. Absolute Layout- Absolute layout enables you to specify the exact location of its children. 5. Frame Layout- The Frame layout is a placeholder on screen that you can use to display a single view. 6. List view- It displays a list of scrollable items. 7. Grid view- It is a Viewgroup that displays items in a two dimensional, scrollable grid. Layouts has a set of attributes which defines the visual properties of that layout. For Example: android : id, android : layout_width android : layout_height, android : layout_marginTop, android : layout_marginleft, android : layout_marginright etc	***Correct mentioned 7 layout and description of attributes contains 4M***
4.	**(A)** **(a)**	**Answer any THREE of the following:** **Explain Co-channel Interference.**	**12** **4M**

	Ans.	**Co-channel Interference:** Frequency reuse implies that in a given coverage area there are several calls that use the same set of frequencies. These cells are called co-channel cells and the interference between signals from these cells is called Co-channel interference. Co-channel Interference can't be combated by simply increasing the carrier power of transmitter. This is because an increase in carrier transmit power increases the interference to neighbouring Co-channel cells must be physically reparted by a minimum distance to provide sufficient isolation due to propagation. When the size if each cell is approximalily same and the base station transmit the same power, the co-channel interference ratio is independent of the transmitted power and becomes a function of the radius of the cell (R) and distance between centres of the nearest Co-channel Cells (D). By increasing the ratio of D/R. the spatial separation between Co-channel. Cells relative to the coverage distance of a cell is increased. Thus, interference is reduced from improved isolation of RF energy from the co-channel cell. The parameter Q called the Co-channel reuse ratio, is related to the cluster size . For hexagonal geometry $Q = {}^{D}/_{R} = \sqrt{3N}$ Small Q provides large capacity since cluster size N is small. Whereas large value of Q improves the transmission quality, due to smaller level of Co-channel interference.	***Listing of correct channel 2M*** ***Description 2M***
	(b) Ans.	**Explain the sequence of events that takes place during PSTN to GSM call.** 	**4M** ***Correct sequence of events contains 4M***

		When a PSTN subscriber calls a mobile station the following sequence of events takes place: 1) The Gateway MSC recevies the call and queries the HLR for the information needed to route the call to the serving MSC/ VLR. 2) The GMSC routes the call to the MSC/VLR 3) The MSC checks the VLR for the location area of the MS. 4) The MSC contacts the MS via the BSC throug a broadcast message i.e. paging request. 5) The MS responds to the page request. 6) The BSC allocates a traffic channel and sends a message to the MS to tune to the channel. The MS generates a ringing singal and the subsriber answers, the Speech connection is established. 7) Handover,if required takes place.	
	(c) Ans.	**Discuss signal processing in GSM.** **Signal Processing in GSM**  **Speech Coding:** The coder provides 260 bits for each 20ms blocks of speech, which yield a bit rate of 13kbps. **Channel Coding:** The output bits of the speech coder are ordered into groups for error protection, based on their significance in contributing to, speech quality. Out of the total 260 bits in a frame, the most important 50 bits called (Ia bits) have 3 parity check (CRC) bits added to them. This facilitate the non correctable errors at the receiver. The next 132 bits (Type Ib) along with 53 bits are reordered and appended by providing a data block of 189 bits. This block is then encoded for	**4M** ***Diagram 2M*** ***Explanation 2M***

		error using rate ½ Convolution encoder. The least important 78 bits (Type 2) are not error protected and are just joined to form 456 bits in a 20 ms frame. **Interleaving:** The 456 bit in 20ms speech frame is broken into Eight 57 bit sub blocks. They form the consecutive TCH time slots. **Ciphering:** It modifies the contents of the eight interleaved blocks through the use of encryption techniques known only to a particular mobile station and bas transceiver. **Burst Formatting:** Adds binary data to the ciphered blocks to help synchronization and equalization of the received signal. **Modulation:** It is 0.3 GMSK. It is a type of digital FM. 1's and 0's are represented by shifting the RF carrier by +- 67.708 KHz. **Demodulation:** The appropriate TS is demodulated with the aid of synchronization data provided by the burst formatting. After demodulation, the binary info is deciphered, de-interleaved, channel decoded and speech decoded.	
	(d) Ans.	**Explain the Information Security Attacks.** **Attacks:** A security system is a system to defend our assets from attacks. In the physical world, these attacks are carried out at the weak points in the defense system. When the vulnerability is exploited by some interest or selfish motive, it is an attack on the system. **Attacks on dynamic asset can be of the following types:** 1. **Interception**: An unauthorized party gaining access to an asset will be part of this attack. This is an attack on Confidentiality like unauthorized copying of files or tapping a conversation between parties. 2. **Modification**: An unauthorized party gaining control of an asset	**4M** ***Relevant explanation (any four attacks) 4M***

		and tampering with it is part of this attack. This is an attack on integrity like changing the content of a message being transmitted through the network. 3. **Fabrication**: An unauthorized party inserts counterfeited objects into the system. 4. **Interruption**: An asset is destroyed or made unusable. This is an attack on availability Attacks on static assets can be of the following types. Virus and worms: There are a type of program that replicates and propagates from one system to another. **5. Denial of Service**: These are attacks on the system to prevent legitimate users from using the using. **6. Intrusion**: these are people or software, which enter into computer systems and perform function without the knowledge of the owner of the asset. **7. Replay Attack**: In a replay attack the opponent passively captures the data without trying to analyze the content. At a later time, the same is used in the same sequence to impersonate an event and gain unauthorized access to resource. 8.**Buffer Overflow attack**: In buffer overflow attack, the vulnerability of an executable program is exploitable. 9.**Trapdoor attacks**: These are exploitations of some undocumented features of a system.	
4.	**(B)** **(a)** Ans.	**Answer any ONE of the following:** **Draw and explain GSM channels.** There are mainly two types of GSM logical channels. (i) Traffic channels (TCHs). (ii) Control channels (CCHs). Traffic channels carry digitally encoded user voice or user data and have identical formats of both forward link and reverse link. Control channels carry signal and synchronization commands between the base station and mobile station. Other control channels are used only for forward and reverse link. GSM traffic channel carry digital voice and user data either at half rate or at full rate.	**6** **6M** ***List 1M***

		Full Rate Traffic Channels (TCH): **(i) Full-rate speech channel (TCH/FS):** This channel carries user speech in digitized form at a raw data rate of 13 kbps. GSM channel coding is added to digitized speech then the full rate speech channel carries 22.8 kbps. **(ii) Full-rate data channel for 9600 bps (TCH/F9.6):** This channel carries raw user data which is transfers at 9600 bps with additional forward error correction applied by GSM, the 9600 bps data sent at 22.8 kbps. **(iii) Full-rate data channels for 4800 bps (TCH/F4.8):** This channel carries raw user data which is transferred at 4800 bps with additional forward error correction applied by GSM, the 4800 bps is sent at 22.8 kbps. **(iv) Full rate data channel for 2400 bps (TCH/F2.4):** This channel carries raw user data which is transferred at 2400 bps with additional forward error correction coding by GSM, the 2400 bps is sent at 22.8 bps. **Half-rate Traffic Channels:** **(i) Half-rate speech channel (TCH/HS):** This channel carries digitized speech which is sampled at a half rate then the full rate GSM channel coding added to digitized speech and half rate speech channel carry 11.4 kbps. **(ii) Half-rate data channels for 4800 bps (TCH/H4.8):** This channel carries raw user data which is to be transferred at 4800 bps. With additional forward error correction applied by GSM, the 4800 bps data sent at 11.4 kbps. **(iii) Half-rate data channels for 2400 bps (TCH/H2.4):** This channel carries raw user data which is to be transferred at 2400 bps with additional forward error correction by the GSM, the 2400 bps data sent at 11.4 kbps.	***Relevant explanation 3M***

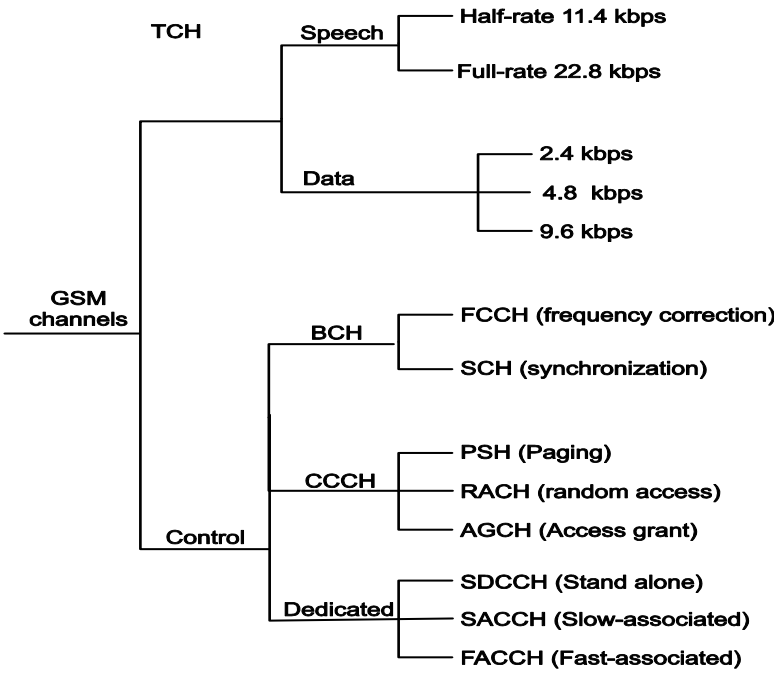


Fig. GSM Channels

Diagram 3M

GSM Control Channels (CCH):

There are three control channels in GSM:

1. Broadcast control channels.
2. Common control channels.
3. Dedicated control channels.

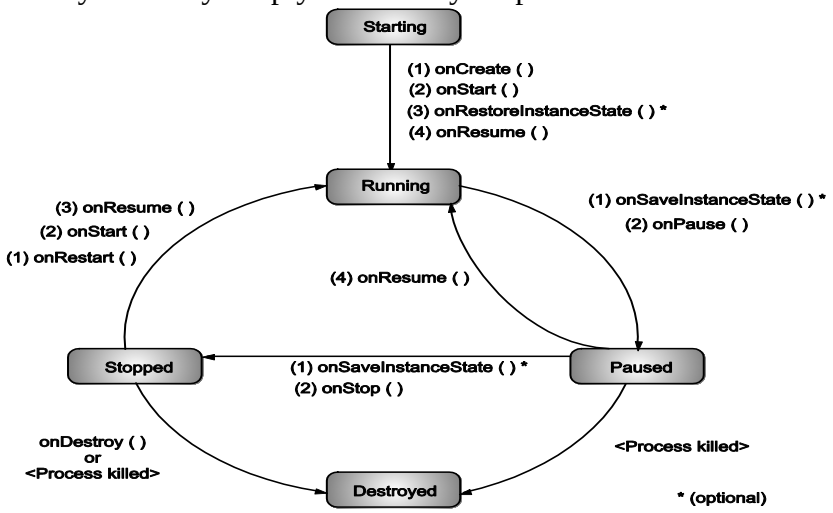
1. Broadcast control channels (BCH) :

The BTS uses this channel to give information to all MSs within a cell. Information uses by this channel is cell and network identity, current control channel structure, channel availability and congestion. The broadcast control channel also sends the list of channels that are currently used within cell.

2. Common Control Channels (CCCH):

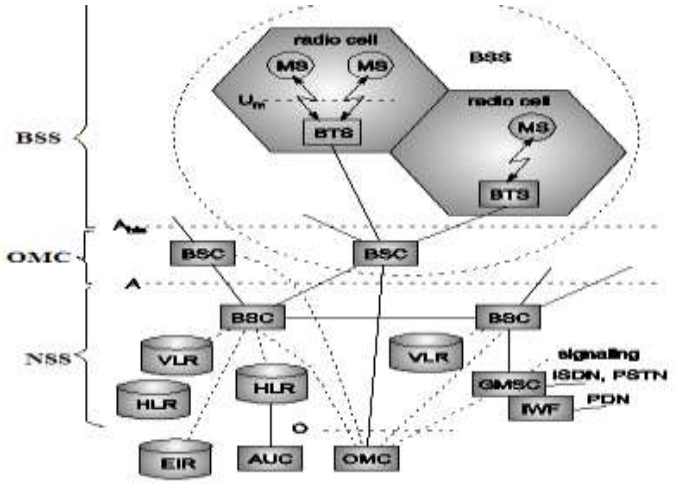
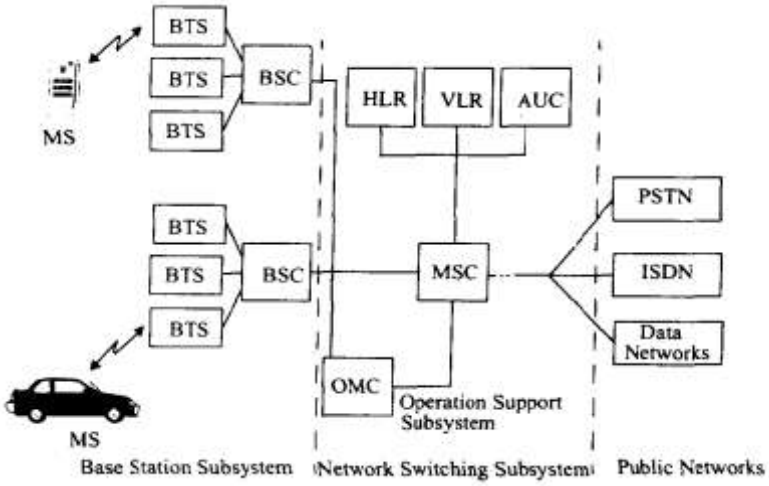
All the information regarding setting up a connection between MS and BS is exchanged via the CCCH. The common control channel occupies TSO (frame) of GSM frame and that is not used by BCH

		and ideal channels. **3. Dedicated Control Channels (DCCH):** They have same format and function on both forward and reverse links.	
	(b) Ans.	**Explain the life cycle of Android Activity.** In Android, there is one foreground application, which typically takes over the whole display except for the status line. • When the user runs an application, Android starts it and brings it to the foreground. From that application, the user might invoke another application, or another screen in the same application, and then another and another. • All these programs and screens are recorded on the *application stack* by the system's Activity Manager. At any time, the user can press the Back button to return to the previous screen on the stack. From the user's point of view, it works a lot like the history in a web browser. Pressing Back returns them to the previous page. • Internally, each user interface screen is represented by an Activity class. Each activity has its own life cycle. An application is one or more activities plus a Linux process to contain them. • In Android, an application can be "alive" even if its process has been killed. • Put another way, the activity life cycle is not tied to the process life cycle. • During its lifetime, each activity of an Android program can be in one of several states, as shown in Let us see commands used in this life cycle taking activity in different states: • **onCreate(Bundle):** This is called when the activity first starts up. You can use it to perform one-time initialization such as creating the user interface. • **onStart():** This indicates the activity is about to be displayed to the user. • **onResume():** This is called when your activity can start interacting with the user. This is a good place to start animations and music.	**6M** ***Explanation 4M***

		• **onPause():** This runs when the activity is about to go into the background, usually because another activity has been launched in front of it. • **onStop():** This is called when your activity is no longer visible to the user and it won't be needed for a while. If memory is tight, onStop() may never be called the system may simply terminate your process. • **onRestart():** If this method is called, it indicates your activity is being redisplayed to the user from a stopped state. • **onDestroy():** This is called right before your activity is destroyed. If memory is tight, onDestroy() may never be called, the system may simply terminate your process.  **Fig.: Life cycle of an Android activity** • **onSaveInstanceState(Bundle):** Android will call this method to allow the activity to save per-instance state, such as a cursor position within a text field. • **onRestoreInstanceState(Bundle):** This is called when the activity is being reinitialized from a state previously saved by the onSaveInstanceState() method.	***Diagram 2M***
5.	**(a)** Ans.	**Answer any TWO of the following:** **Explain the GSM architecture in detail with neat sketch.** **GSM system consists of three major components:** (i) Base Station System (BSS).	**16** **8M**

		(ii) Operation and Maintenance Center (OMC). (iii) Network and Switching Subsystem (NSS). **(i) Base Station System (BSS):** This system consists of Mobile Station (MS), Base Station Controller (BSC), Base Transreceiver Station (BTS). As shown in Fig. the BSS and NSS connected to each other via A interface (solid lines) and the connection to OMC via O interface (dashed lines). • Base Station Subsystem (BSS): GSM system consists of many BSS, each one is controlled by Base Station Controller (BSC). BSS performs all the functions which are required to maintain connection to MS, coding/decoding of voice etc. BSS also contains Base Trans receiver Stations (BTS). • Base Station Controller (BSC): BSC provides all the control functions and physical link between MSC and BTS. BSC is connected to BTS and MSC (Mobile Switching Center). Base Trans receiver Station (BTS): BTS is responsible for handling radio interface to the mobile station. It is connected to MS via Um interface and it is also connected to BSC via the Abis interface. The Um interface contains all mechanism for wireless interface (TDMA, FDMA etc.). The BTS is a radio equipment (trans receiver or antenna) needed to service each cell in the network. **(ii) Operation and Maintenance Center (OMC):** OMC is connected to all equipments in switching system and to the BSC. It maintains operation of the GSM network by observing the handovers, system load, blocking rates etc. OMC provides network overview and allow network engineers to monitor, diagnose and troubleshoot every aspect of GSM network. **(iii) Network and Switching Subsystem (NSS):** NSS is responsible for performing call processing and subscriber related functions. It also includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AUC), Equipment Identity Register (EIR) etc.	***Explanation 4M***

		• Mobile Switching Center (MSC): It is used to handle communication between different MS connected to different BSCs. The function of MSC is to locate different MS and associated BTS, call switching and authentication etc. • Home Location Register (HLR): It is a database for managing the mobile subscriber. HLR stores permanent data of subscriber which include subscribers service profile, location information and its activity. A home subscriber charges are less than the roaming subscriber. • Visitor Location Register (VLR): 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. • Authentication Center (AUC): This authentication center is used to provide authentication and encryption method that is used to verify the user identity and ensure the confidentiality and secrecy of each call. • Equipment Identity Register (EIR): It contains a list of all valid MS equipment within the network, where each MS is known by it's IMEI. • This IMEI is divided into three groups. 1. White IMEI: All known IMEI. 2. Black IMEI: All stolen mobile handset. 3. Gray IMEI: Handset that is uncertain.	

		 **OR** 	***4M diagram***
	(b) Ans.	**Explain the GPRS Data Services and Bearer Services.** **GPRS Data Services:** Wide range of corporate and consumer applications are enable by GPRS services. GPRS Service include all normal GSM services but in more efficient way. It also support services like • Email	**8M**

		• Web browsing • Enhanced short message • Wireless imaging with instant picture • Video service • Document and information sharing A user is likely to use either of the two modes of the GPRS network. These are 1. Application mode 2. Tunneling mode **1. Application Mode:** • In this mode the user will be using the GPRS mobile phone to access the application running on the phone itself. • The phone here acts as the end user devices. • All GPRS phone have web browser as embedded application. • This browser allows browsing of web sites. • Some GPRS device support mobile execution environment. **2. Tunneling Mode:** • This mode is for mobile computing where the user will use the GPRS interface as an access to the network. • The end user device will be a large footprint device like laptop computer or small footprint device like PDA's. • The MS will be connected to the device and used as a modem to access the wireless data network. **GPRS Bearer Services:** GPRS is a wireless extension of data networks. It can access to data networks, such as IP-based networks (public internet, private intranet, IPv4 and IPv6 protocols) and X.25 based networks. GPRS upgrades GSM data services and provides the following services: 1. Point-to-point (PTP) service: internetworking with the Internet (IP protocols) and X.25 networks. 2. Point-to-multipoint (PTM) service: point-to-multipoint	***Data Services 4M*** ***Bearer Services 4M***

		multicast and point-to- multipoint group calls. 3. SMS service: bearer for SMS 4. Anonymous service: anonymous access to predefined services 5. Future enhancements: flexible to add new functions, such as more capacity, more users, new accesses, new protocols, new radio networks.	
	(c) Ans.	**Explain 3GPP Security and Smart Card security.** It is 3rd Generation Partnership Project. **3rd Generation** Partnership Project (3GPP) is a collaborative project aimed at developing globally acceptable specifications for third generation (3G) mobile systems. It is a collaboration between groups of telecommunications associations, to make a globally applicable third generation (3G) mobile phone system. 3GPP Specifications are also referred to as UTRAN, UMTS (in Europe) and FOMA (in Japan). The telecommunications standards bodies that make up the 3GPP are known as Organizational Partners (OP) and those are: • Japan‟s Association of Radio Industries and Businesses (ARIB) • Japan‟s Telecommunications Technology Committee (TTC), • China Communications Standards Association (CCSA), • South Korea‟s Telecommunications Technology Association (TTA), • European Telecommunications Standards Institute (ETSI), and • Alliance for Telecommunications Industry Solutions (ATIS). The Four Technical Specification Groups (TSG) in 3GPP are: • Radio Access Networks (RAN), • Service and Systems Aspects (SA), • Core Network and Terminals (CT) and • GSM EDGE Radio Access Networks (GERAN). 3GPP caters to the following technologies: • GSM: Global System for Mobile • GSM includes GPRS (General Packet Radio Service) and EDGE (Enhanced Data rates for Global Evolution) • WCDMA - Wideband Code Division Multiple Access • HSPA - High Speed Packet Access	**8M** ***3GPP security Explanation 4M***

- LTE - Long Term Evolution

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system. A security feature is a service capability (e.g. user data confidentiality) that meets one or several security requirements.

Overview of the security architecture:
Fig gives an overview of the complete 3G security architecture.

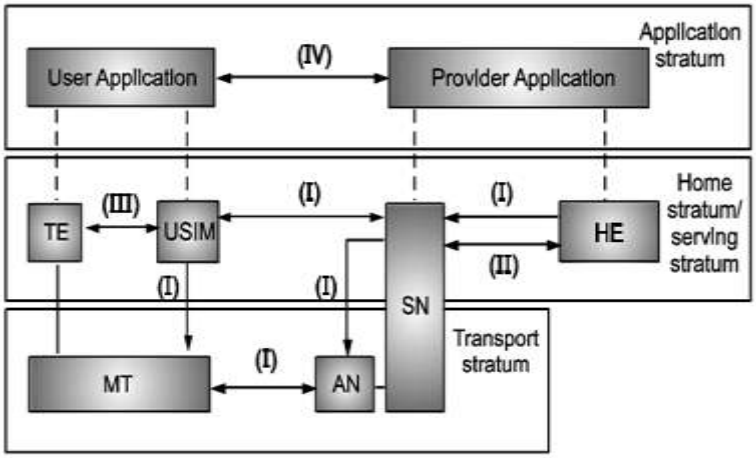


Fig Overview of the 3G security architecture

From Fig, four security feature groups are defined. Each of these feature groups meets certain threats, accomplishes certain security objectives:

1. Network access security (I): The set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link.
2. Network domain security (II): The set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wireline network.
3. User domain security (III): The set of security features that secure access to mobile stations.
4. Application domain security (IV): The set of security features that enable applications in the user and in the provider domain to securely

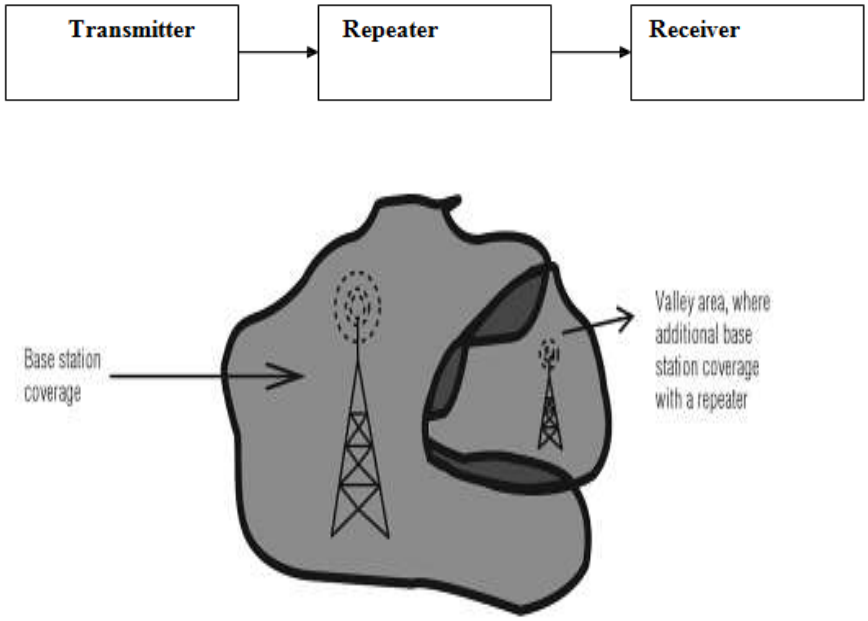
		exchange messages. **Smart Card Security:** Smart card is called „smart" because it contains a computer chip. Indeed, smart card is often referred to as „chip card 'or' integrated circuit card". It provides not only memory capacity, but computational capability as well. The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications, which require strong security protection and authentication. Where are smart cards used? There are different types of smart cards used in various application scenarios like: Smart card can act as an identification card, which is used to prove the identity of the card holder. It can also be a medical card, which stores the medical history of a person. Furthermore, the smart card can be used as a credit/debit bank card which allows off-line transactions. All of these applications require sensitive data to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication, etc. In same way, one more example of smart card is SIM in mobile phone. SIM card (also known as a subscriber identity module) is a smart card with a microprocessor and it consists of the following modules: • CPU • Program memory (ROM) Working memory (RAM) • Data memory (EPROM or E2PROM) Serial communication module • SIM stores subscriber data that includes user identity, network authorization data, personal security • keys, contact lists and stored text messages. Smart Card Security: **Factors which make SIM secure are:** 1.Cryptographic algorithm The presence of cryptographic algorithm and secret key in SIM card makes the SIM card secure.	***smart card security Explanation 4M***

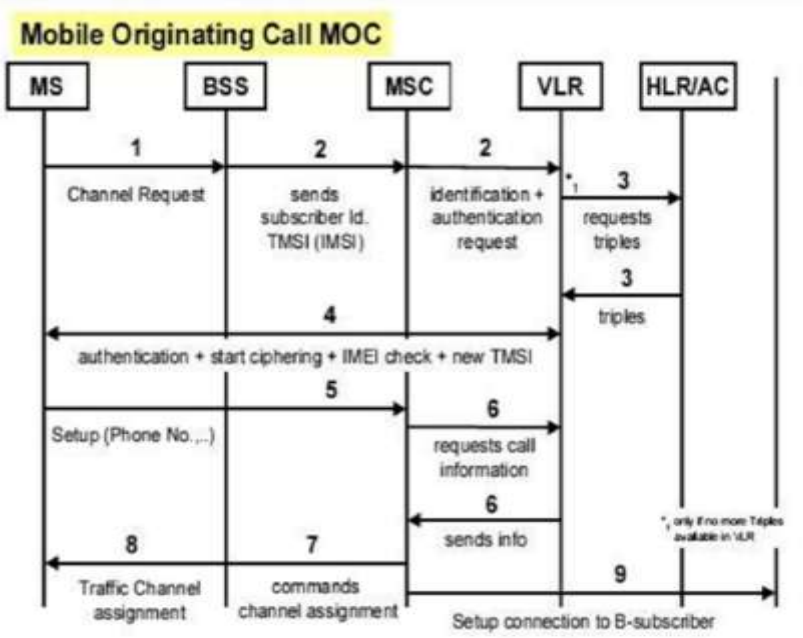
		The most sensitive information of SIM card is the cryptographic algorithm A3, A8, secret Ki, PIN, PUK and Kc. A3, A8 algorithm were written into the SIM card in the producing process, and most people could not read A3, A8 algorithm. HN code could be settled by the phone owners. PUK code is held by the operator. Kc was derived in the process of encryption from Ki. Many of SIMS have RSA, DES, 3DES cryptographic algorithms implemented. 2.Secret key: PIN and PUK • PIN – Personal Identification Number.2 PINs exist (PIN1 and PIN2). Limited attempts on PIN access. • PUK-PIN Unblocking Code.resetting PUK, resets PIN and the attempt counter.Too many attempts on PUK blocks use permanently. 3. SIM files system: SIM is organized in a hierarchical tree structure; it consists of the following three types of elements: • Master File (MF). • Dedicated File (DF). • Elementary File (EF). These file systems have stringent security controls. These files are even protected through password known to user or operator.	
6.	**(a)** Ans.	**Answer any FOUR of the following:** **Explain the role of Repeaters.** • The use of repeater in cellular mobile communication system is for extending the range of the reception of the receiver. • Especially, the repeater is used when it is hard for the transmitted signal to reach up to the receiver set. • Repeaters are bidirectional in nature and simultaneously send signals to and receive signals from a serving BS. Upon receiving signals from BSs in forward link, the repeater amplifies and reradiates the BS signals to the specific coverage region. • Repeaters are being widely used to provide coverage into and around buildings, where coverage has been traditionally weak. • Repeaters do not add any capacity to the system, they just increase the reach of a BS or MS into "shadowed" areas.	**16** **4M** ***1M for each role***

MODEL ANSWER

SUMMER - 2017 EXAMINATION

Subject: Mobile Computing **Subject Code: 17632**

			
	(b) Ans.	**Describe basic call originating procedure.** **Call Setup in GSM:** Mobile Originating Call (MOC): Call setup, which are initiated by an MS 1. Channel Request: The MS requests for the allocation of a dedicated signalling channel to perform the call setup. 2. After allocation of a signalling channel the request for MOC call setup, included the TMSI (IMSI) and the last LAI, is forwarded to the VLR 3. The VLR requests the AC via HLR for Triples [(random number (RAND), Signed Response (SRES) and a Cipher Key (Kc)] (if necessary). 4. The VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI Re-allocation (optional). 5. If all this procedures have been successful, MS sends the Setup information (number of requested subscriber and detailed service description) to the MSC. 6. The MSC requests the VLR to check from the subscriber data whether the requested service an number can be handled (or if there are restrictions which do not allow further proceeding of the call setup)	**4M** ***Explanation 2M***

		7. If the VLR indicates that the call should be proceeded, the MSC commands the BSC to assign a Traffic Channel (i.e. resources for speech data transmission) to the MS 8. The BSC assigns a Traffic Channel TCH to the MS 9. The MSC sets up the connection to requested number (called party)  	***Diagram 2M***
	(c) Ans.	**Explain the function of HLR and VLR.** **Home Location Register (HLR):** • It is a database for managing the mobile subscriber. • HLR stores permanent data of subscriber which include subscribers service profile, location information and its activity. • A home subscriber charges are less then the roaming subscriber. **Visitor Location Register (VLR):** • 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.	**4M** ***Any 2 function of HLR 2M*** ***Any 2 function of VLR 2M***

	(d) Ans.	**Explain the events when GSM location update takes place.** **Updating on entering a new location Area:** The Location Area Identity (LAI) is broadcast in system information message and stored in mobile station memory. When a new received location area identity does not match with the previously stored location area identity, then MS does a location update. **Periodic update:** Whenever MS performs location update if reset timer T. A time has timeout value. As and when the timer expires, the MS does the location update. **Updating on deactivation and activation:** Mobile equipment do this update and send IMSI DETACH message when it is deactivated. The network marks that MS as a deactivated and does not send paging message to for MS until it is activated again. A MS send IMSI DETACH message does a location update when it is activated again.	**4M** ***Explanation 4M***
	(e) Ans.	**Explain advantages and disadvantages of 4G.** **Advantages of 4G:** • The most obvious advantage of the 4G mobile network is its amazing speed. Increased bandwidth leads to much faster data transfer speed, which is especially advantageous for mobile devices. • Users of the 4G network get the advantage of superior, uninterrupted connectivity, especially for advanced tasks such as video chats and conferences. • Mobile device users, they can stream music, videos and movies at a much faster rate than ever before and can also easily share information online. • 4G networks offer much more coverage than other systems such as WiFi, which forces users to depend upon hotspots in each area you visit. • 4G offers a coverage of 30 miles and more, as also overlapping network ranges, users would be assured of complete connectivity at all times. • 4G networks offer complete privacy, security and safety. This is	**4M** ***Any 2 advantages 2M***

		especially beneficial for corporate establishment sand business persons, who hold sensitive information on their respective mobile devices. • 4G networks are quite affordable these days, what with pricing schemes being considerably slashed to fit users' budgets. Of course, this type of connectivity is more expensive than traditional WiFi networks, but it also has a lot more advantages to offer to users. • This network also offers users several options to choose from, as regards plans and equipment to connect to the 4G network. Many mobile carriers also offer special introductory offers for new customers, which works out to be very reasonable for them. **Disadvantages of 4G :** • Though the hardware compatible with 4G networks is available at much cheaper rates today than earlier, the fact remains that this new equipment would necessarily have to be installed in order to supply these services. • Since 4G mobile technology is still fairly new, it will most likely have its initial glitches and bugs, which could be quite annoying for the user. • 4G mobile networks use multiple antennae and transmitters and hence, users would experience much poorer battery life on their mobile devices, while on this network. • Users would be forced to make do with 3G or WiFi connectivity in the areas that do not yet have 4G mobile network coverage. While this is a problem in itself, the worse issue is that they would still have to pay the same amount as specified by the 4G network plan.	***Any 2 disadvantages 2M***
	(f) Ans.	**Explain UMTS briefly.** UMTS (Universal Mobile Telecommunications Service) is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates upto 2 megabits per second (Mbps). • Universal Mobile Telecommunications System (UMTS) is a air interface standard and has evolved since late 1996 under the European Telecommunications Standards Institute (ETSI). European carriers, manufacturers, and government regulators collectively developed the early versions of UMTS as a competitive open air-interface standard for 3G wireless telecommunications.	**4M** ***Correct Explanation 4M***

		• UMTS offers a consistent set of services to mobile computer and phone users, which is not depend on the location. UMTS is based on the Global System for Mobile (GSM) communication standard. Once UMTS is available, computer and phone users can be continuously connected to the Internet wherever they travel, will have the same set of capabilities. Users will get access to internet via combination of terrestrial wireless and satellite transmissions. • Earlier cellular telephone systems were using circuit-switched connection, where the connections were always dependent on circuit availability. A packet-switched connection uses the Internet Protocol (IP), meaning that a virtual connection is always available. • The 3G W-CDMA air interface standard had been designed for "always-on" packet based wireless service, so that computers, entertainment devices, and communication device all share the same wireless network and be connected to the Internet, anytime, anywhere. W-CDMA is used to transfer packet up to 2.048 Mbps per user (if the user is stationary), thereby allowing high quality data, multimedia, streaming audio, streaming video and broadcast-type services to consumers. Future versions of W-CDMA will support stationary user data rates in excess of 8 Mbps. W-CDMA provides public and private network features, as well as video conferencing and virtual home entertainment (VHE). W-CDMA designers contemplate that broadcasting, mobile commerce (m- commerce), games, interactive video, and virtual private networking will be possible throughout the world, all from a small portable wireless device. • UMTS also makes it possible to provide new services like alternative billing methods or calling plans. For instance, users can choose to pay-per-bit, pay-per-session, flat rate, or asymmetric bandwidth options. • The higher bandwidth of UMTS also enables other new services like video conferencing. UMTS may allow the Virtual Home Environment (VHE) to fully develop, where a roaming user can have the same services to either at home, in the office or in the field through a combination of transparent terrestrial and satellite connections.	