MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer **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 more Importance (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**
	(i)	**State different handoff strategies used in analog generation and second generation.**	***4M***
	Ans.	**Handoff:** A handoff refers to the process of transferring an active call or data session from one cell in a cellular network to another or from one channel in a cell to another. A well implemented handoff is important for delivering uninterrupted service to a caller or data session user. ***Handoffs may be classified into two types:*** **1. Hard Handoff:** Characterized by an actual break in the connection while switching from one cell or base station to another. The switch takes place so quickly that it can hardly be noticed by the user. Because only one channel is needed to serve a system designed for hard handoffs, it is the more affordable option. It is also sufficient for services that can allow slight delays, such as mobile broadband Internet. **2. Soft Handoff:** Entails two connections to the cell phone from two different base stations. This ensures that no break ensues during the handoff. Naturally, it is more costly than a hard handoff.	***Hard Handoff : 2M*** ***Soft Handoff : 2M***

	(ii) Ans.	**List broadcast channels of GSM and describe two of them.** A Broadcast Channel (BCH) is a downlink channel in a GSM system that is used by the base stations to provide signalling information to the mobile stations. The mobile station needs this information to find a network, synchronize with it and to connect to it. There are three types of broadcasting channels: 1. Frequency correction channel (FCCH) 2. Synchronization channel (SCH) 3. Broadcast control channel (BCCH) **1. FCCH - Frequency Correction Channel:** The Frequency Correction Channel is a broadcast channel used by GSM base stations. It provides a unique tone of 67.7 kHz for the Mobile Stations. This tone is used to synchronize the local clock of the mobile receiver with the base station. This is needed to correctly extract the data. **2. Synchronization channel (SCH):** The Synchronization Channel (SCH) is a downlink broadcast channel of the base stations of a GSM network. The SCH provides information to the Mobile Stations needed to search for base stations, identify them and synchronize with them **3. Broadcast control channel (BCCH):** The Broadcast Control Channel (BCCH) is a logical broadcast channel used by the base station in a GSM network to send information about the identity of the network. This information is used by a mobile station to get access to the network. This information includes the Mobile Network Code (MNC), the Location Area Code (LAC) and a list of frequencies used by the neighboring cells (BA: BCCH Allocation List).	***4M*** ***List: 2M*** ***Explanation: 2M***
	(iii) Ans.	**Write a stepwise procedure of basic call origination and termination in GSM.** **Mobile Originating Call (MOC):** 1. Channel Request: The MS requests for the allocation of a dedicated signaling channel to perform the call setup. 2. After allocation of a signaling 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. 4. The VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI Re-allocation (optional).	***4M*** ***Stepwise Procedure: 4M***

		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) 7. If the VLR indicates that the call should be preceded, 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)	
	(iv) Ans.	**Describe data services used in GPRS.** GPRS is a wireless extension of data networks. It can access to data networks, such as IP-based networks (public internet, private intranet, and 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 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	***4M*** ***Any 4 Services : 1M Each***
1.	**b)** **(i)** Ans.	**Answer any <u>ONE</u> of the following:** **With neat labelled diagram describe GSM architecture. List subsystems involved in it.** A GSM network comprises of many functional units. These functions and interfaces are explained in this chapter. **The GSM network can be broadly divided into:** • The Mobile Station (MS) • The Base Station Subsystem (BSS) • The Network Switching Subsystem (NSS) • The Operation Support Subsystem (OSS)	**6** ***6M*** ***List of Subsystems: 2M***

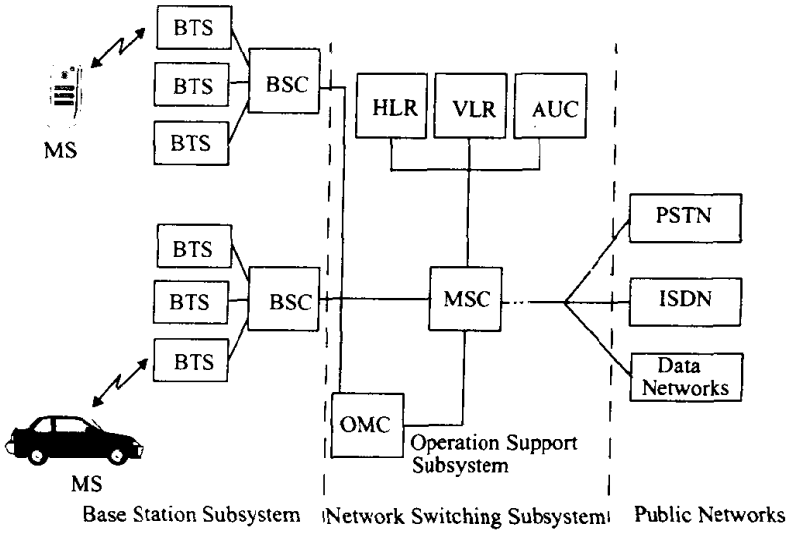


Fig: GSM Architecture

Diagram : 2M

Base Station System (BSS): It consists of Mobile Station (MS), Base Station Controller (BSC), and Base Trans-receiver Station (BTS), the BSS and NSS connected to each other via 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 Transreceiver Stations (BTS).

Explanation: 2M

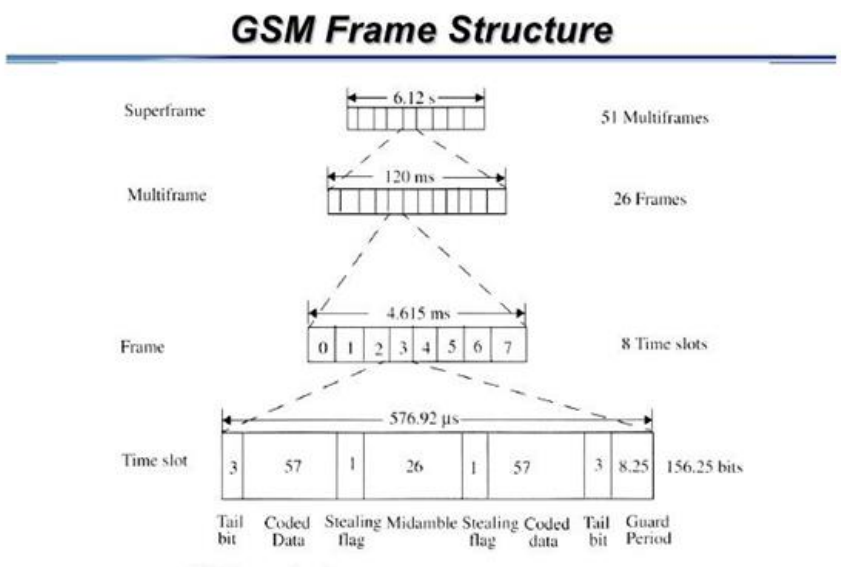
Base Transreceiver Station (BTS): BTS is responsible for handling radio interface to the mobile station. It is connected to MS via Um interface and it is also connected to BSC via the Abis interface. The Um interface contains all mechanism for wireless interface (TDMA, FDMA etc.). The BTS is a radio equipment (Transreceiver or antenna) needed to service each cell in the network.

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 Centre). The BSC manages the radio resources for one or more BTS. It handles radio channel setup, frequency hopping and handovers. The BSC is the connection between the mobile and the MSC. It assigns and releases

		frequencies and time-slots for the MS. The BSC also handles inter-cell handover. It controls the power transmission of the BSS and MS in its area. **Operation and Maintenance Center (OMC):** OMC is connected to all equipment's in switching system and to the BSC. Administration and commercial operation (subscription, end terminals, charging and statistics) Security management, Network Configuration, Operation and Performance Management, Maintenance tasks. **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. Mobile Switching Centre (MSC): It is used to handle communication between different MS connected to different BSCs. MSC performs the switching of calls between the mobile and other fixed or mobile network users as well as the management of mobile services such as registration, authentication, location updating, handovers and call routing to a roaming subscriber.	
	(ii) Ans.	**Describe security framework for mobile environment in detail.** Mobile application spans over several networks. One of these networks will be a wireless radio network. Others will be wired network. At the boundary of any of these networks, there is need for protocol conversion gateways. These gateways run either at the transport layer or at the application layers. Multiple gateways and multiple networks make security challenges in mobile environment complex. In security system, authentication and non-repudiation are meaningful only when these are implemented end to end between parties that need to authenticate each other. Authorization is a direct function of authentication. Therefore it is also an end to end function. Authentication, authorization and non-repudiation must therefore be implemented at the application layer. Confidentiality and Integrity can be implemented at any layer or through multiple layers. Therefore to offer secured environment in a mobile environment, security procedures will be a combination of many procedures and function.	***6M*** ***Explanation: 2M***

		1. 3GPP security architecture In 3GPP's security architecture, the emphasis is on the network access security mechanism, including mutual authentication, universal terrestrial radio access network (UTRAN) ciphering, and integrity protection of signaling data. Network access security mechanisms mainly fall into three categories: • Identification by temporary identities such as Temporary Mobile Subscriber Identity (TMSI) • Identification by a permanent identity such as International Mobile Subscriber Identity (IMSI) • Authentication and key agreement (AKA). 3GPP looked into these concerns and proposed a new architecture through following important changes: • Changes were made to defeat the false base station attack. It is now capable of identifying the network. • Key lengths are increased to allow stronger algorithms for encryption and integrity. • Mechanisms are included to support security within and between networks. • Security is based within the switch rather than the base station to ensure that links are protected between station and switch. • The authentication algorithm has not been defined but guidance on choice will be given. **2. Mobile Virtual Private Network** 1. Mobile VPN is a private network over a public network (usually the Internet) to connect two endpoints. 2. Instead of using a dedicated physical connection such as leased line, a VPN uses virtual connections routed through the Internet from the enterprise's private network to the remote mobile device. 3. VPN implements this through an encrypted private connection between nodes. 4. It generally uses IPSec and other PKI frameworks to offer confidentiality, authentication, non-repudiation and Integrity. **3. SMART CARD Security** 1. Smart card is called smart because it contains a computer chip. 2. Indeed, smart card is often referred to as chip card or integrated circuit card. It provides not only memory capacity, but	***Any 2 Security framework: 2M each***

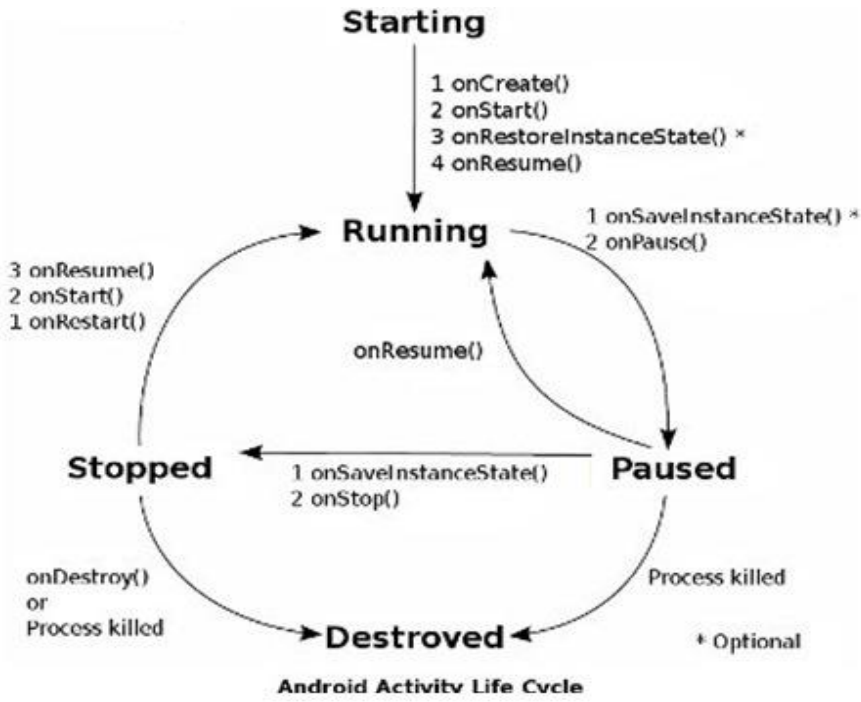
		computational capability as well. 3. The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. 4. Because of this characteristic, smart cards are often used in different applications, which require strong security protection andauthentication. **4. Multifactor Security**: Multifactor security implies to a system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multifactor Security can be a combination of any of the following factors: **a. What You Know:** The idea here is that you know a secret often called a password that nobody else does. Thus, knowledge of a secret distinguishes you from all other individuals. And the authentication system simply needs to check to see if the person claiming to be you knows the secret. (e.g. Password, Pass Phrase , PIN, Answer to some personal question) **b. What You Have:** Instead of basing authentication on something a principal knows and can forget, maybe we should base it on something the principal has. (E.g. Magnetic Stripe Card, Smart Card, Hardware token, Physical Key, Private Key protected by password) **c. Who You Are:** Authentication based on "something you are" will employ behavioral and physiological characteristics of the principal. (E.g. Retinal scan, Fingerprint reader, Handprint reader, Voice print)	
2.	**a)** Ans.	**Answer any FOUR of the following:** **With neat labeled diagram describe GSM frame architecture.**	**16** ***4M***

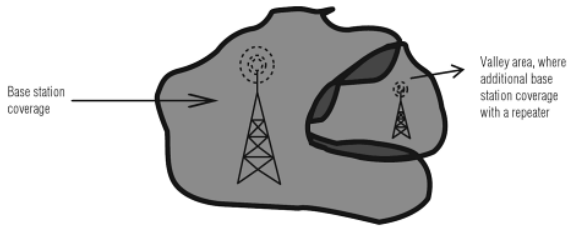
		 **Frame structure in GSM:** 1. The length of GSM frame in a frequency channel is 4.615 ms. 2. The frame is divided into 8 bursts of length of 0.577ms 3. The timeslots in the uplink are derived from downlink by a time delay of 3 time slots 4. This arrangement prevents an MS from transmitting and receiving at the same time 5. However, due to propagation delay (when MS is far away from BTS) the 3 TS delay cannot be maintained accurately.	***Diagram 2M*** ***Explanation 2M***
	b) Ans.	**Describe user services provided in GSM.** **GSM Services and Features:** 1. SMS - Short Message Service - Allows you to send text messages to and from phones 2. Multi Party Calling - Talk to five other parties as well as yourself at the same time. 3. Call Holding - Place a call on Hold 4. Call Waiting - Notifies you of another call whilst on a call 5. Mobile Data Services - Allows handsets to communicate with computers. 6. Mobile Fax Service - Allows handsets to send, retrieve and receive faxes 7. Calling Line Identity Service - This facility allows you to see the telephone number of the incoming caller on our handset before	***4M*** ***Any 4 Service & Features : 1M Each***

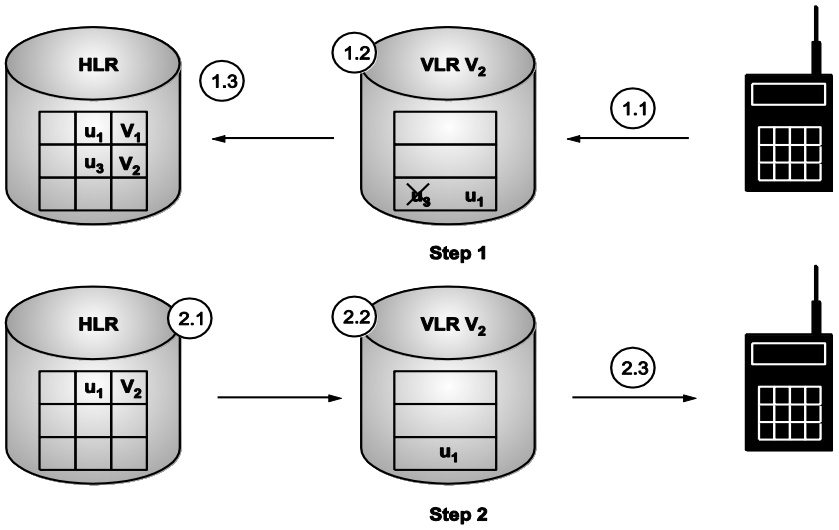
		answering 8. Advice of Charge - Allows you to keep track of call costs 9. Cell Broadcast - Allows you to subscribe to local news channels 10. Mobile Terminating Fax - Another number you are issued with that receives faxes that you can then download to the nearest fax machine.	
	c) Ans.	**State four features of linux operating system.** **Features of Linux Operating System:** 1. **Portable** – Portability means softwares can works on different types of hardwares in same way. Linux kernel and application programs support their installation on any kind of hardware platform. 2. **Open Source** – Linux source code is freely available and it is community based development project. Multiple teams works in collaboration to enhance the capability of Linux operating system and it is continuously evolving. 3. **Multi-User** – Linux is a multiuser system means multiple users can access system resources like Memory/RAM/Application programs at same time. 4. **Multiprogramming** – Linux is a multiprogramming system means multiple applications can run at same time. 5. **Hierarchical File System** – Linux provides a standard file structure in which system files/ user files are arranged. 6. **Shell** – Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to do various types of operations, call application programs etc. 7. **Security** – Linux provides user security using authentication features like password protection/ controlled access to specific files/ encryption of data.	***4M*** ***Any 4 Features : 1M Each***
	d) Ans.	**Define public key cryptography and describe components of it.** Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication. A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used. Public key cryptography is based on a secure secret key pair. Each key (one half of the pair) can only decrypt information encrypted by its corresponding key (the other half of the pair). A key pair includes: • The private key, known only to its owner • The public key, distributed widely, but still associated with its	***4M*** ***Definition: 1M***

		owner **Components of Public Key cryptography:** **1. Plaintext:** The original data or text is called plaintext. **2. Cipher text:** The original message changed to another unreadable format using some algorithm is called Cipher text. **3. Digital certificates:** Digital "identities" issued by trusted third parties that identify users and machines. They may be securely stored in wallets or in directories. **4. Public and private keys:** Form the basis of a PKI for secure communications, based on a secret private key and a mathematically related public key **5. Secure sockets layer (SSL):** An Internet-standard secure protocol **6. Certificate Authority (CA):** Acts as a trusted, independent provider of digital certificates.	***Description of Components: 3M***
	e) Ans.	**List 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. **4.** Transit Delays GPRS packets are sent in all different directions to reach the same destination. This opens up the potential for one or	***4M*** ***Any 2 Applications: 1M each*** ***Any 2 Limitations: 1M each***

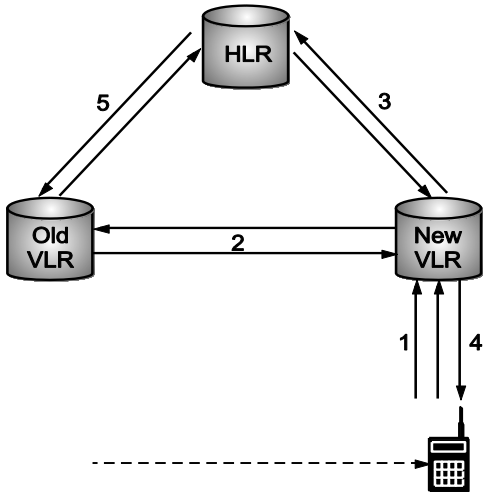
		some of those packets to be lost or corrupted during the data transmission over the radio link.	
	f) Ans.	**With the neat diagram describe methods of life cycle of android activity.** As an activity transitions from state to state, it is notified of the change by calls to the f***ollowing*** **protected methods**: 1. onCreate(): This is the first callback and called when the activity is first created. 2. onStart(): This callback is called when the activity becomes visible to the user. 3. onResume(): This is called when the user starts interacting with the application. 4. onPause(): The paused activity does not receive user input and cannot execute any code and called when the current activity is being paused and the previous activity is being resumed. 5. onStop(): This callback is called when the activity is no longer visible. 6. onDestroy(): This callback is called before the activity is destroyed by the system. 7. onRestart(): This callback is called when the activity restarts after stopping it. Taken together, these seven methods define the entire lifecycle of an activity.	***4M*** ***Explanation: 2M***

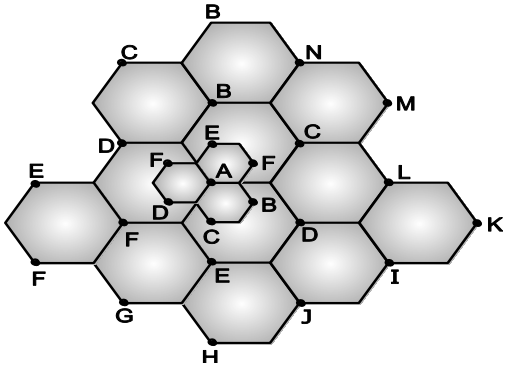
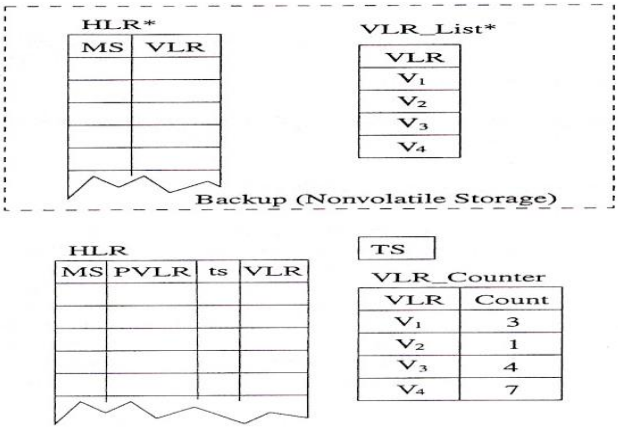
		 **Android Activity Life Cycle**	***Diagram : 2M***
3.	**a)** Ans.	**Answer any FOUR of the following:** **Describe how repeaters can be used for range extension in cellular systems.** • The use of repeater in cellular mobile communication system is for extending the range of the reception of the receiver. • 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. • However, repeaters do not add any capacity to the system, they just increase the reachof a BS or MS into "shadowed" areas. 	**16** ***4M*** ***2M for Description***

			***2M for Diagram***
	b) Ans.	**List bearer services provided in GPRS and describe each of them.** • GPRS 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 IPv6protocols) 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 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.	***4M*** ***List 2M*** ***Description 2M***
	c) Ans.	**Write an algorithm for call registration in VLR overflow.** If the VLR is full and a new mobile user arrives, then the user is failed to register in the database, so it can't receive cellular services. This situation is called as VLR overflow. When VLR is full, a new user can't register using the registration procedure. To resolve this problem, overflow control algorithm 0-I, 0-II, 0-III and 0-IV are presented which allow a new user to receive services when the VLR is full. In the overflow control system an extra flag (1-bit) is required in HLR record. No changes are required in MS. Algorithm 0-1: Registration When MS moves into particular VLR called V. If V is not full, then the normal registration procedure is carried out but if V is full, then the following steps are executed. **Step 1: Registration Request** Step 1.1: This is same as normal registration procedure. Step 1.2: When the database is full V follows a replacement policy to	***4M*** ***Explanation 2M***

		select a record to be deleted as shown in Fig. (u3), is selected for deletion. The storage space of deleted record is used to store new information. The selected user (u3) is called as overflow user. The replacement can be done on the various factor. For example, V may select a record randomly, select old record or select an inactive record (i.e. the user has not had call for a long time). We may select (u1) as a new overflow user (i.e. u3 = u1) and does not create any new VLR record for u1. Step 1.3: We forward the registration request to HLR by indicating that u3's record is deleted due to database overflow. **Step 2: Registration Response** Step 2.1: The HLR updates the location of u1 and set overflow flag in front of u3. Note that u3 may be identical to u1 as described in 1.2. Step 2.2: The HLR acknowledges the registration operation and send u1's profile to V. If the u1 is overflow user then the message does not include profile information. Step 2.3: We send acknowledgement to the MS.  **Figure: Overflow registration operation**	***Diagram 2M***
	d) Ans.	**State the need of smart card security.** **Need of smart card Security:** 1.Smart cards are often used in different applications, which require strong security protection and authentication. 2.Smart card can act as an identification card, which is used to prove the identity of the card holder. 3.The smart card can be used as a credit/debit bank card which allows off-line transactions. All of these applications require sensitive data	***4M*** ***Each Point- 1M***

		to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication, etc. 4.Smart card is SIM in mobile phone. SIM card (also known as a subscriber identity module) is a smart card which stores subscriber data that includes user identity, network authorization data, personal security keys, contact lists and stored text messages.	
	e) Ans.	**State the key features of Symbian operating system.** **Features of Symbian operating system:** • **Real-time:** It has a real-time, multithreaded kernel. • **Multimedia support:** It supports audio, video recording, playback and streaming, and image conversion. • **Platform Security:** Symbian provides a security mechanism against malware. It allows sensitive operations and can be accessed by applications which have been certified by a signing authority. In addition, it supports full encryption and certificate management. • **Internationalization support:** It supports Unicode standard. • **Client-server architecture:** It provides simple and high-efficient inter-process communication. This feature also eases porting of code written for other platforms to Symbian OS. • Fully object-oriented and component-based. • Optimized memory management. • Flexible user interface design. • Multi-tasking. • A Hardware Abstraction Layer (HAL): This layer provides a consistent interface to hardware and supports device in dependency.	***4M*** ***Each Point-1M***
4.	**a)** **(i)** Ans.	**Answer any <u>THREE</u> of the following:** **Write the stepwise procedure for call delivery to a roaming user in GSM.** The location of mobile station is maintained by HLR and the VLR. When an MS visit a new location, it must register in the VRL of the visited location. Then the HLR must also be informed about this registration. To access MS, the HLR has to find the current VLR of the MS. The registration process of MS when it is moving from one VLR to another VLR is as follows. **Step 1:**The MS periodically listens to the BCCH broadcast from the BSS. If MS detect that it has entered into a new area, then it sends registration message to VLR by using SDCCH channel.	**12** ***4M*** ***2M for Explanation***

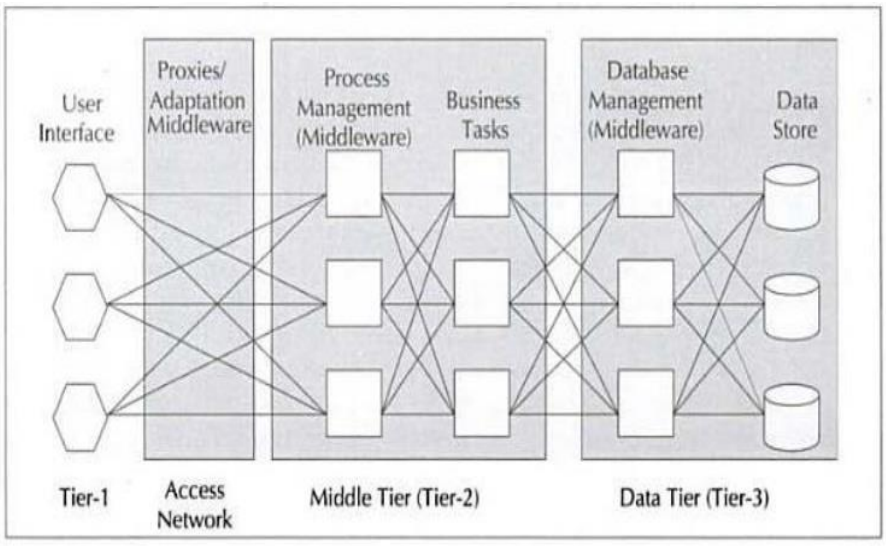
		Step 2: Then new VLR communicates with old VLR to find the HLR of the MS. Then new VLR performed authentication process. **Step 3:** After MS authentication, the new VLR sends registration message to the HLR. If registration request is accepted, then HLR provides the new VLR with all the subscriber information for call handling. **Step 4:**The new VLR informs the MS about successful registration. **Step 5:**After step 3, the HLR sends cancellation message to old VLR. The old VLR cancels the record for MS and sends on acknowledgement to HLR about the cancellation. When MS is inactive due to switching off or SIM removal, it transmits a detach to deregister from network. MS has to periodically send registration message to network. The range of period may be from 6 minutes to slightly more than 24 hours.  **Diagram: The MS registration process**	***2M for Diagram***
	(ii) Ans.	**Describe cell splitting of cellular system in detail.** Cell splitting is the process of dividing a congested cell into smaller cells, each smaller cell have its base station and the height of antenna and transmission power is less than original (bigger) cell. Cell splitting increases the capacity of cellular system by reusing the number of channels. New cell has smaller radius than original cell and by installing smaller cell which is called as micro cell between existence cell, capacity of cellular network increases. An example of cell splitting is shown in Figure. The base stations are placed at corner of each cell. It is assumed that the area which is covered by station A to be flooded with traffic. New base station	***4M*** ***2M for Explanation***

		therefore needed to increase the number of channel and also to reduce the area served by single base station. In Figure, the original base station is surrounded by six new microcell. In Figure, it is shown that the smaller cells were added in such a way that as to preserve frequency reuse plan. B is placed in such a way that B was placed half way between two larger stations.  **Figure: Cell splitting**	***2M for Diagram***
	(iii) Ans.	**Write the stepwise procedure of registration in VLR identification algorithm.** **HLR Architecture:**  **Registration:** **Step 1. Update HLR:** V_{old} ← HLR[p].VLR; Send message, MAP_CANCEL_LOCATION, to cancel the VLR entry of p at V_{old}: HLR[p].VLR ← V_{new}; t_{old}← HLR[p].ts	***4M*** ***Diagram 1M*** ***Algorithm 3M***

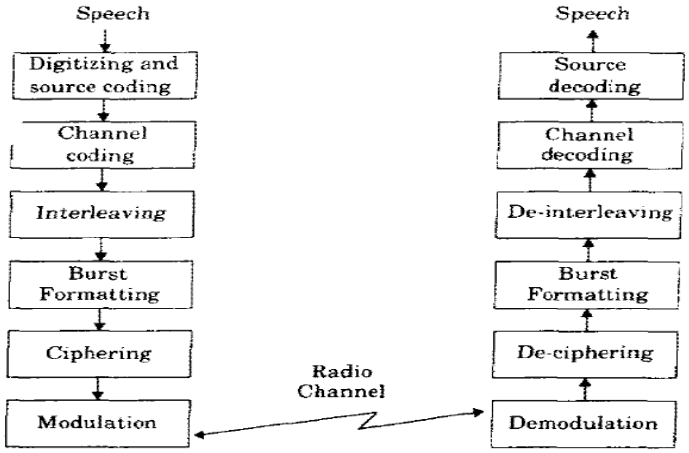
		HLR[p].ts ← t **Step 2. Update the V_{new} Count field in** VLR_Counter: **If HLR[p].VLR != HLR[p].PVLR then:** Step 2.1 **If VLR_Counter[V_{new}] exists, then:** VLR_Counter[V_{new}] ← VLR_Counter[V_{new}] +1; Step 2.2 **Else create VLR_Counter[V_{new}] and** VLR_List*[V_{new}] ; VLR_Counter[V_{new}] ← 1 **Step 3. Update the V_{old} counter entry: If t_{old}** >TS and V_{old}!=HLP[p].PVLR **then:** Step 3.1 VLR_Counter[V_{old}] ← VLR_Counter[V_{old}] −1; Step 3.2 **If VLR_Counter[V_{old}] .Count = 0 then:** Step 3.2.1 Delete VLR_Counter[V_{old}] and VLR_List*[V_{old}] At Step1 of procedure 2, the location information of the MS is updated and its location record at the old VLR, V_{old}, is cancelled by the deregistration message. MAP_CANCEL_LOCATION. The last update time, V_{old} is saved to be used in step3. At Steps 2 & 3 of procedure 2, VLR counter[] is used to count the "effective" number of MS_S that enter the VLR_S during the period [TS,t]. Note that if the MS was in V_{new} before TS [i.e. HLR [p]. VLR = LR* [p]. VLR = HLR[p].PVLR), then the HLR may consider that the MS never moves out of the VLR, and there is no need to increments the VLR counter, and step2 is skipped. If MS moved into V_{old} during the uncovered period that is TS_{old} > TS- it implies that the movement into V_{old} is not effective because the MS has moved out of V_{old} at t. Thus, the V_{old} counter, should be decremented by 1. When VLR counter [v]. count>1, then any update to VLR counter [v] will not invoke modification to VLR_List*[ ]. In other words, access to the HLR backup is avoided. The purpose of procedure 2 is to avoid updating the backup for every registration operation.	
	(iv) Ans.	**List static asset attacks and describe each of them.** **Virus and Worms**: These are a type of program that replicates and propagates from one system to another. Most of the virus do malicious destructive functions in the system. **Denial of Service:** These are attacks on the system to prevent	***4M*** ***Any 4 Attack 1M each***

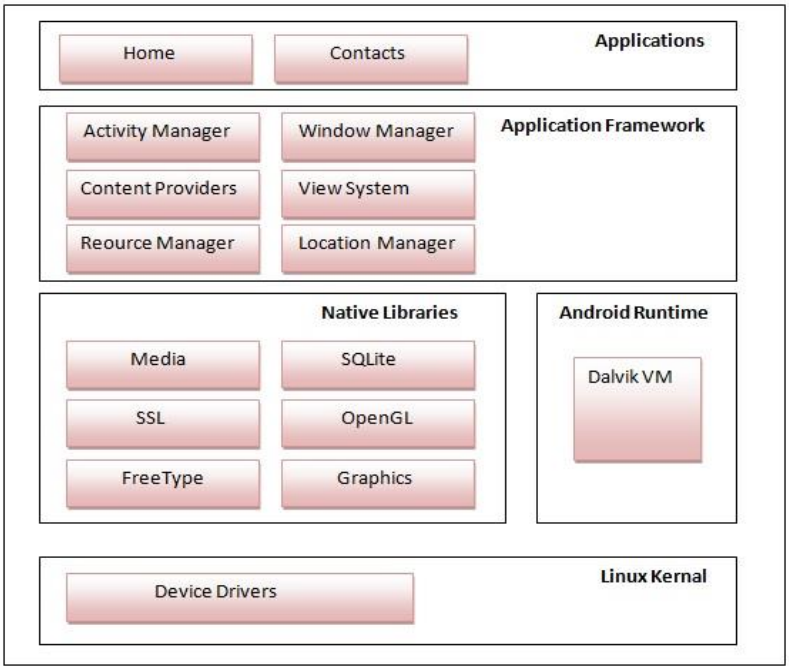
		legitimate users from using the service. **Intrusion**: These are people or software, which enter into computer systems and perform function without the knowledge of the owner of the asset. These are also called hackers. **Replay Attack**: In a replay attack the opponent passively captures the data with-out 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. **Buffer overflow attacks**: In a buffer overflow attack, the vulnerability of an exe-cutable program is exploited to force a stack overflow condition, inducing the program counter of the process to change. The program counter is then manipulated to do the work for the attacker. **Trapdoor attacks:** These are exploitations of some undocumented features of system. Undocumented functionality are designed to debug, service, supporter take control of the system.	
4.	**b)**	**Answer any ONE of the following:**	**6**
	(i)	**Describe UMTS in 3G and 4G technology with its goals.**	***6M***
	Ans.	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. • 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,	***Any Relevant points explanation-4M, goal 2M***

		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. • HSPA+, or Evolved High-Speed Packet Access, is a technical standard for wireless, broadband telecommunication. HSPA+ enhances the widely used WCDMA based 3G networks with higher speeds for the end user that are comparable to the newer LTE networks. HSPA+ was first defined in the technical standard 3GPP release 7 and expanded further in later releases. • HSPA+ provides an evolution of High Speed Packet Access High Speed Packet Access provides data rates up to 168 Megabits per second (Mbit/s) to the mobile device and 22 Mbit/s from the mobile device.	
	(ii) Ans.	**List components of information security and describe each of them.** The Standard X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures security of the systems for data transfer. These security services are treated as basic principles of information security system. These services are also considered as main components of	***6M***

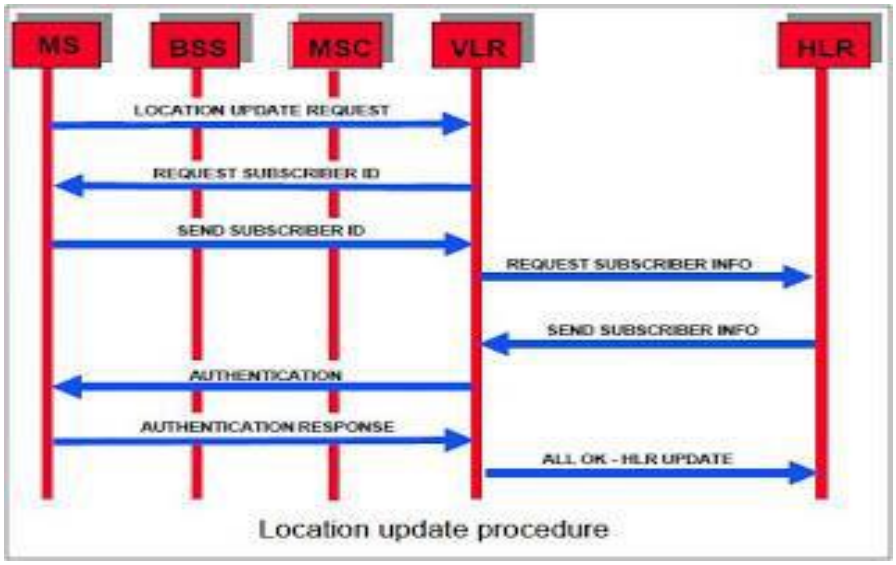
		information security system. **1. Confidentiality** **2. Authentication** **3. Authorization** **4. Integrity** **5. Non-repudiation** **6. Availability** **7. Trust** **8. Accounting** **1. Confidentiality** is the property where the information is kept secret so that unauthorized persons cannot get at the information. **2. Integrity** is the property of keeping the information intact. **3. Availability** is the property of a system by which the system will be available to its legitimate users. **4. Non-repudiation** is the property by which the identify of both sender and receiver of message can be identified and verified, **5. Authorization** is the property by which the users properties can be associated to the information access. **6. Trust** is the property of expectation, confidence and belief over time. **7. Accounting** is the property of calculating the fee for a service rendered	***List 2M*** ***Explanation 4M***
5.	**a)** Ans.	**Answer any TWO of the following:** **With neat labeled diagram describe three-tier mobile computing architecture.**  	**16** ***8M*** ***Diagram : 4M***

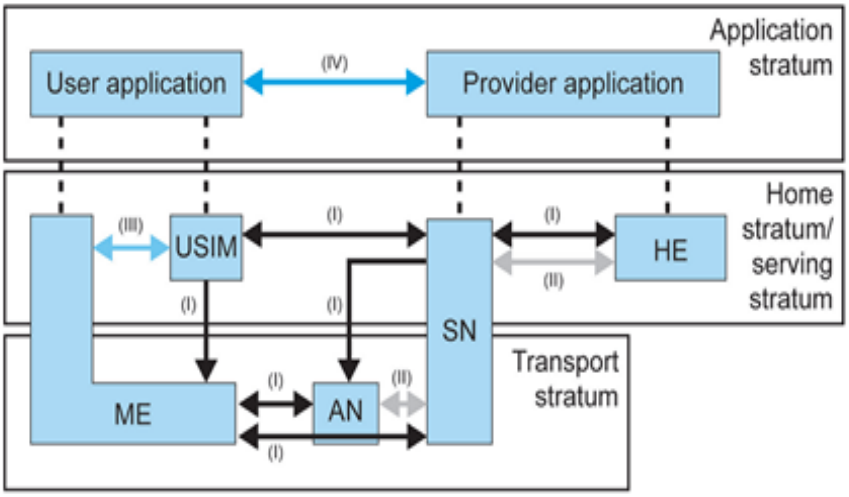
		• First tier is user interface of presentation tier. This layer deals with facing device handling and rendering. • This tier includes a user system interface where user services text input, session, display management. • Second tier is the process management or application tier. This layer is for application programs or process management where business logic and rules are executed. • This layer controls hundreds of users. Middle process management tier controls transactions. The third and final tier is the database management or data tier. This layer is for database access and management. • It provides 1. Performance 2. Flexibility 3. Maintainability 4. Reusability 5. Scalability	***Explanation: 4M***
	b) Ans.	**Describe signal processing in GSM in detail.** **Speech Coding** - The GSM speech coder is based on the Residually Excited Linear Predictive Coder **(RELP).** The coder provides 260 bits for each 20 ms blocks of speech, which yields a bit rate of 13 kbps. This speech coder was selected after extensive subjective evaluation of various candidate coders available in the late 1980s. Provisions for incorporating half-rate coders are included in the specifications. **TCHIFS, SACCH, and FACCH Channel Coding** - The output bits of the speech coder are ordered into groups for error protection, based upon their significance in contributing to speech quality. Out of the total 260 bits **in** a frame, the most important 50 bits, called type Ia bits, have *3* parity check (CRC) bits added to them. **Channel Coding for Data Channels**- The coding provided for GSM full rate data channels (TCHIF9.6) is based on handling 60 bits of user data at 5ms intervals, in accordance with the modified CCIIT V.llO modem standard. **Channel Coding for Control Channels** - GSM control channel messages are defined to be 184 bits long, and are encoded using a shortened binary cyclic fire code, followed by a half-rate convolutional coder. **Interleaving** - In order to minimize the effect of sudden fades on the received data, the total of 456 encoded bits within each 20 ms speech frame or control message frame are broken into eight 57 bit sub-	***8M*** ***Explanation: 4M***

		blocks. These eight subblocks which make up a single speech frame are spread over eight consecutive TCH time slots. **Ciphering** - Ciphering modifies the contents of the eight interleaved blocks through the use of encryption techniques known only to the particular mobile station and base transceiver station. **Burst Formatting** - Burst formatting adds binary data to the ciphered blocks, in order to help synchronization and equalization of the received signal. **Modulation** - The modulation scheme used by GSM is 0.3 GMSK where 0.3 describes the 3 dB bandwidth of the Gaussian pulse shaping filter with relation to the bit rate (e.g., *BT* = 0.3). GMSK is a special type of digital FM modulation. **Frequency Hopping-** Under normal conditions, each data burst belonging to a particular physical channel is transmitted using the same carrier frequency. However, if users in a particular cell have severe multipath problems, the cell may be defined as a *hopping cell* by the network operator, in which case *slow frequency hopping* may be implemented to combat the rnultipath or interference effects in that cell. **Equalization** - Equalization is performed at the receiver with the help of the training sequences transmitted in the midamble of every time slot. The type of equalizer for GSM is not specified and is left up to the manufacturer. **Demodulation** - The portion of the transmitted forward channel signal which is of interest to a particular user is determined by the assigned TS and ARFCN.  	***Diagram : 4M***

	c) Ans.	**With the neat diagram describe android architecture.**  **Android architecture** or **Android software stack** is categorized into five parts: 1. linux kernel 2. native libraries (middleware), 3. Android Runtime 4. Application Framework 5. Applications **1) Linux kernel** It is the heart of android architecture that exists at the root of android architecture. **Linux kernel** is responsible for device drivers, power management, memory management, device management and resource access. **2) Native Libraries** On the top of linux kernel, there are **Native libraries** such as WebKit, OpenGL, FreeType, SQLite, Media, C runtime library (libc) etc. The WebKit library is responsible for browser support, SQLite is for database, FreeType for font support, Media for playing and recording audio and video formats. **3) Android Runtime**	***8M*** ***Diagram : 4M*** ***Explanation: 4M***

		In android runtime, there are core libraries and DVM (Dalvik Virtual Machine) which is responsible to run android application. DVM is like JVM but it is optimized for mobile devices. It consumes less memory and provides fast performance. **4) Android Framework** On the top of Native libraries and android runtime, there is android framework. Android framework includes **Android API's**such as UI (User Interface), telephony, resources, locations, Content Providers (data) and package managers. It provides a lot of classes and interfaces for android application development. **5) Applications** On the top of android framework, there are applications. All applications such as home, contact, settings, games, browsers are using android framework that uses android runtime and libraries. Android runtime and native libraries are using linuxkernal.	
6.		**Answer any FOUR of the following:**	**16**
	a)	**Write a stepwise procedure of GSM updation for inter MSC movement.**	***4M***
	Ans.	The **Location Update process** consists of the following phases Request for service; the MS detects that it has entered a new Location Area and requests to update its location. The new MSC/VLR identifies the MS. • Authentication - The new MSC/VLR requests to the AUC for authentication parameters (SRES). Using these parameters the MS is authenticated. • Ciphering - Using the parameters which were made available earlier during the authentication the uplink and the downlink are ciphered. • Update HLR/VLR - The new MSC/VLR requests to update the MS location in the HLR. The MS is de-registered in the old VLR. • TMSI re-allocation - The MS is assigned a new TMSI.	***GSM updation Procedure 3M***

			***Diagram : 1M***
	b) Ans.	**Describe mobility database of GSM in detail.** Home location register (HLR) is a database used for mobile user information management. All permanent subscriber data are stored in this database An HLR record consists of 3 types of information: **Mobile station information** 1. IMSI used by MS to access network 2. MSISDN **Location information** 1. ISDN number (address) of VLR and MSC where MS resides **Service information** 1. Service subscription 2. Service restrictions 3. Supplementary services Visitor location register (VLR) is a database of the service area visited by MS. All subscriber data of an MS required for call handling and other purpose are stored in VLR. VLR information consists of 3 parts: **Mobile station information** 1. IMSI 2. MSISDN 3. TMSI **Location information** 1. MSC number	***4M*** ***4M Explanation***

		2. Location area ID (LAI) **Service information** 1. Subset of the service information stored in the HLR	
	c) Ans.	**With neat labeled diagram describe 3GPP security architecture.**  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.	***4M*** ***Diagram : 2M*** ***Explanation 2M***
	d) Ans.	**Describe routing of packets in GPRS in detail.** • The example assumes two intra PLMN backbone networks of different PLMN. • Intra PLMN backbone network connect GSN of the same PLMN or the same network operator. • These are private packet based networks of the GPRS network provider; for example Airtel GSN in Mumbai connecting to Airtel GSN in Delhi through a private data network.	***4M*** ***4M Explanation***

		• GPRS mobile station located in PLMN1 send IP packets to a host connected to the IP network e.g to a web server connected to the internet.	
	e) Ans.	**Describe the attachment and detachment procedure of GPRS in detail.** **Attachment and Detachment Procedure:** • In order to access the GPRS services, an MS needs to make its presence known to the network. It must register itself with an SGSN of the network. • This is done through a GPRS attach. This operation establishes a logical link between the MS and the SGSN. • The network checks if the MS is authorized to use the services; if so it copies the user profile from the HLR to the SGSN, and assigns a packets with external PDN after successful GPRS attach, a mobile station must apply for an address. • This address called as PDN (packet data protocol) address. Allocation of the PDP address can be static or dynamic. In case static address the network operation permanently assigns a PDP address to the user. In dynamic allocation address change every time. The disconnection from the GPRS Network is called GPRS Detach. All the resources are released following GPRS detach. Detach process can by initialized by the MS or by the network.	***4M*** ***4M Explanation***