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.1.

A. Attempt any THREE of the following: 12

a) What is mobile computing? Give its functions.
(Definition 1M , Function 3M)

Mobile computing can be defined as a computing environment over physical mobility. The user of the mobile computing environment will be able to access data, information or logical objects from any device in any network while on move.

A computing environment is defined as mobile if it supports one or more of these characteristics:

User mobility: User should be able to move from one physical location to another location and use same service

Network mobility: User should be able to move from one network to another network and use same service

Device mobility: User should be able to move from one device to another and use same service

Session mobility: A user session should be able to move from one user-agent environment to another.

Service mobility: User should be able to move from one service to another

Host mobility: The user should be either a client or server

b) State any four features of GSM.
(Each feature 1M, Any four)

Subscriber Identity Module: It is a memory device that stores info such as subscriber identification no., the networks & countries where the subscriber is entitled for service, privacy keys and other user specific information. The SIM gives the GSM subscriber unit their identity

On –the- air privacy: The privacy is made possible by encrypting the digital bit stream sent by GSM transmitter, according to a secret cryptographic key that is known only to cellular carrier. This key changes with time for each user

The features of GSM are

- Call Waiting - Notification of an incoming call while on the handset
- Call Hold- Put a caller on hold to take another call
- Call Barring - All calls, outgoing calls, or incoming calls
- Call Forwarding- Calls can be sent to various numbers defined by the user
- Multi Party Call Conferencing- Link multiple calls together
- **Calling Line ID** - incoming telephone number displayed
- **Alternate Line Service**
  - One for personal calls
  - One for business calls
- **Closed User Group** - call by dialing last for numbers
- **Advice of Charge**
  - Tally of actual costs of phone calls
- **Fax & Data**
  - Virtual Office / Professional Office
- **Roaming :** services and features can follow customer from market to market

c) **Write an algorithm for call termination of VLR overflow.**
(Algorithm 2M, diagram 2M)

Step 1. Location query:

Step 1.1. The calling party dials the phone number of u1. The request is sent to the origination switch in the PSTN

Step 1.2. The origination switch sends a location query message to the HLR

Step 1.3. The HLR determines that u1 is an overflow user and sends a query message to obtain the routing information. The user profile information is attached in the message

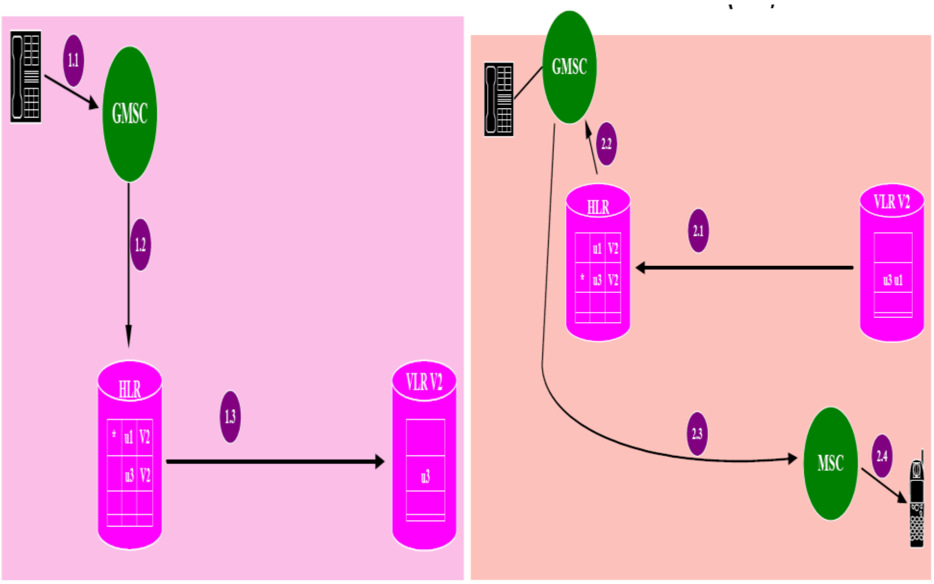
Step 2. Location response:

Step 2.1. If V2 is not full, a record for u1 is created. If V2 is full, a user record is deleted and is used to store u1 and sends it back to HLR. V2 creates the routable address of u1 and sends it back to the HLR. If a record is replaced, the replacement information is included in the message

Step 2.2. HLR returns the routable address to the originating switch. If a record is replaced, the overflow flags are updated at the HLR

Step 2.3. The origination switch sets up the trunk to the MSC based on the routable address

Step 2.4. The MSC pages the mobile phone and the call path is established



d) Explain components of information security.
(Naming components 1M, Description 3M)

- Information security is an art of keeping the message secret ie to encrypt and hide it from others getting to know it. The components are: (CIANATA)

➢ Confidentiality
➢ Integrity
➢ Availability
➢ Non- repudiation
➢ Authorization
➢ Trust
➢ Accounting

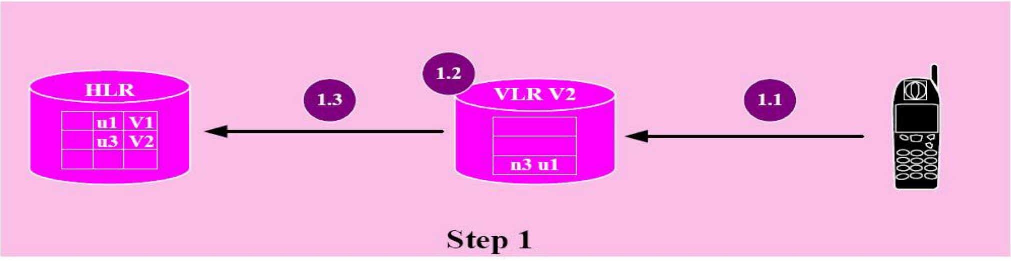
- Confidentiality: It is the property where the information is kept secret so that unauthorized persons cannot get at the information. It is ensured through *Encryption* of data.
- Integrity: Integrity is achieved by adding additional information into a message. It is done through checksums, message digests or digital signature. The receiver of the message checks this extra information to verify whether the message has been tampered.
- .Authentication is a process by which we validate the identity of the parties involved in a transaction.
- In Non – repudiation, we identify the identity of these parties beyond any point of doubt. *Non-repudiation does not allow the sender of the message to refute the claim of not sending that message*
- Availability: Media management is part of the larger security framework. It is essential to ensure availability of service.
- Trust: Trust involves developing a security policy, assigning credentials to entities, verifying that credentials fulfill the policies
- Accounting: It is the process by which usage of service is metered. Based on the usage, the service provider collects the fees either directly from the customer or through home network. This will be true even if the user is roaming in a foreign network and using the services in a foreign network

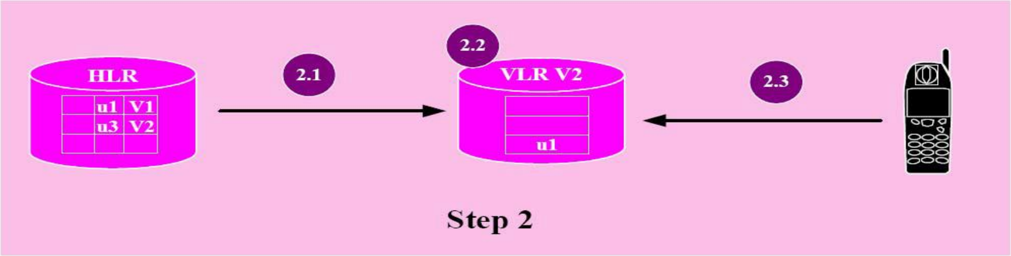
B. Answer any ONE of the following: 6

a) Write an algorithm for Registration of VLR overflow.
(Algorithm for registration-4M, diagram 2M)

When a VLR is full, the incoming mobile users cannot receive cellular services

- To solve VLR overflow problem, overflow control algorithms O-I, O-II, O-III, and O-IV are presented
- An extra flag (1 bit) is required in the HLR records
- Registration:





Step 1. Registration Request:

Step 1.1 Same as step 1 of the normal registration procedure

Step 1.2 V2 is full. V2 follows a replacement policy to select a record to be deleted (u3 in Fig.). The storage for the delete record is used to store u1's information. The selected user (i.e., u3) is called overflow user. The replacement policy may be based on various heuristics

Step 1.3 V2 forwards the registration request to the HLR with indication that u3's record is delete due to database overflow

Step 2. Registration Response:

Step 2.1 HLR update the location of u1, and sets the overflow flag in u3's record

Step 2.2 HLR acknowledges the registration operation and sends u1's profile to V2.

Step 2.3 V2 sends an acknowledgment to MS

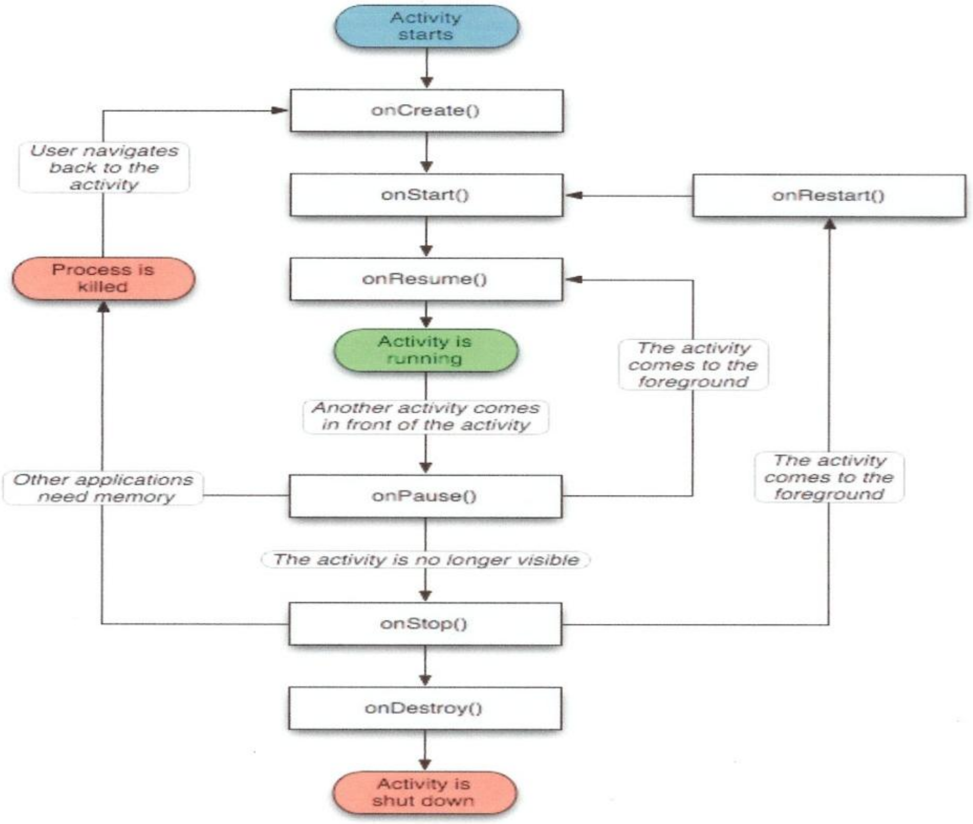
b) Explain life cycle of android activity with neat sketch.
(Diagram 3M; lifecycle explanation 3M)

The steps that an application goes through from starting to finishing Slightly different than normal Java life cycle due to:

- the difference in the way Android application are defined
- the limited resources of the Android hardware platform

Lifecycle:

- Each application runs in its own process.
- Each activity of an app is run in the apps process
- Processes are started and stopped as needed to run apps components.
- Processes may be killed to reclaim needed resources.
- Killed apps may be restored to their last state when requested by the user


Activity starts
onCreate()
User navigates back to the activity
onStart()
onRestart()
Process is killed
onResume()
Activity is running
The activity comes to the foreground
Another activity comes in front of the activity
Other applications need memory
onPause()
The activity comes to the foreground
The activity is no longer visible
onStop()
onDestroy()
Activity is shut down

Q.2. Answer any FOUR of the following: 16

a) Explain channel Assignment Strategies.
(Naming types of strategy 1M; explanation of each strategy 1 ½ M each)
Channel Assignment strategies:

- Channel assignment strategy – Types

– fixed channel assignment
– dynamic channel assignment

- **Fixed channel assignment**

– each cell is allocated a predetermined set of voice channel
– Any new call attempt can only be served by the unused channels in the cell.
– the call will be *blocked* if all channels in that cell are occupied

- Borrowing strategy is a type of fixed channel assignment strategy.
- In this the cell is allowed to borrow channels from neighboring cell if all of its own channel are already occupied.
- The MSC (Mobile switching centre) supervises such borrowing procedures and ensures that borrowing of a channel does not disrupt or interfere with any of the calls in progress in the donor cell

–

- **Dynamic channel assignment**

– Channels are not allocated to cells permanently.
– Mobile Switching centre (MSC) allocate channels based on request.
– Reduce the likelihood of blocking, increase capacity.

This requires the MSC to collect real time data on channel occupancy, traffic distribution & Radio Signal strength Indications (RSSI) of all channels on a continuous basis.

b) Explain cell splitting & sectoring.

- Methods for improving capacity in cellular systems

Cell Splitting: subdividing a congested cell into smaller cells.

Sectoring: directional antennas to control the interference and frequency reuse.

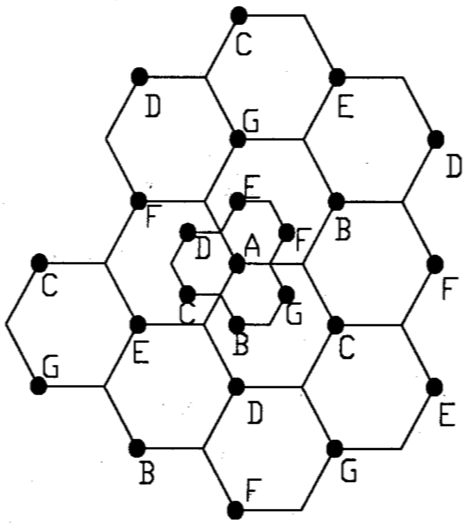
Cell Splitting: (Explanation 1 1/2M, diagram 1/2M)

It is the process of subdividing a congested cell into smaller cells, each with its own base station and a corresponding reduction in antenna height and transmitter power.

Cell splitting increase the capacity of the cellular system since it increases the number of times that channels are reused.

By defining new cells which have a smaller radius than the original cells and by installing these smaller cells (microcells) between the existing cell, capacity increases due to additional channels/ unit area.

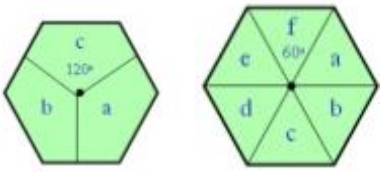
An example of cell splitting is shown below the base station are placed in corners of the cells, and area served by base station A is assumed to be saturated with traffic. New base stations are therefore needed in the region to increases the number of channels in the area and to reduce the area served by the single base station.



Sectoring: (Explanation 1 1/2M, diagram 1/2M)

Another method to increase capacity is to keep the cell radius unchanges and seek methods to decrease D/R ratio. Sectoring increases SIR, so that the cluster size may be reduced. First the SIR is improved using directional antennas, then capacity improvement is achieved by reducing the number of cell in the cluster; thus increasing the frequency reuse. To achieve this, it is necessary to reduce the relative interference without decreasing the transmit power.

A cell is normally partitioned into 3 120^0 sectors and 6 60^0 sectors.



c) **Draw and explain frame structure of GSM.**
(Explanation 2M, diagram 2M)

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 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

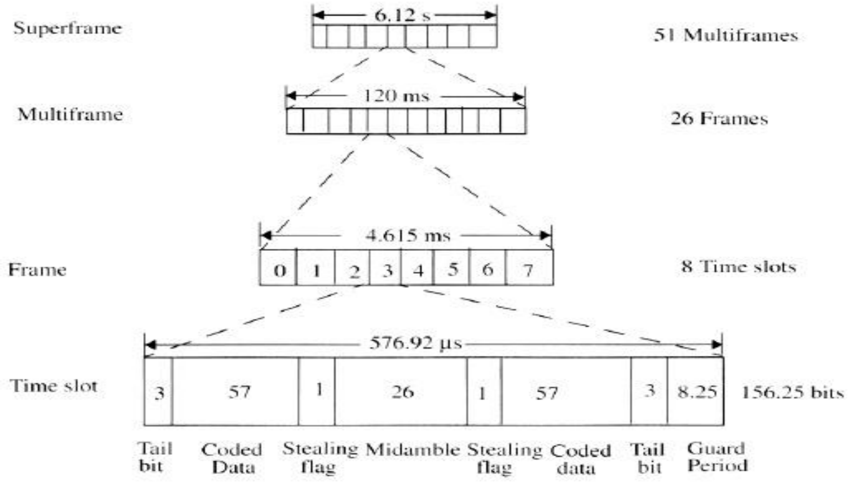


Figure 11.10 GSM frame structure.

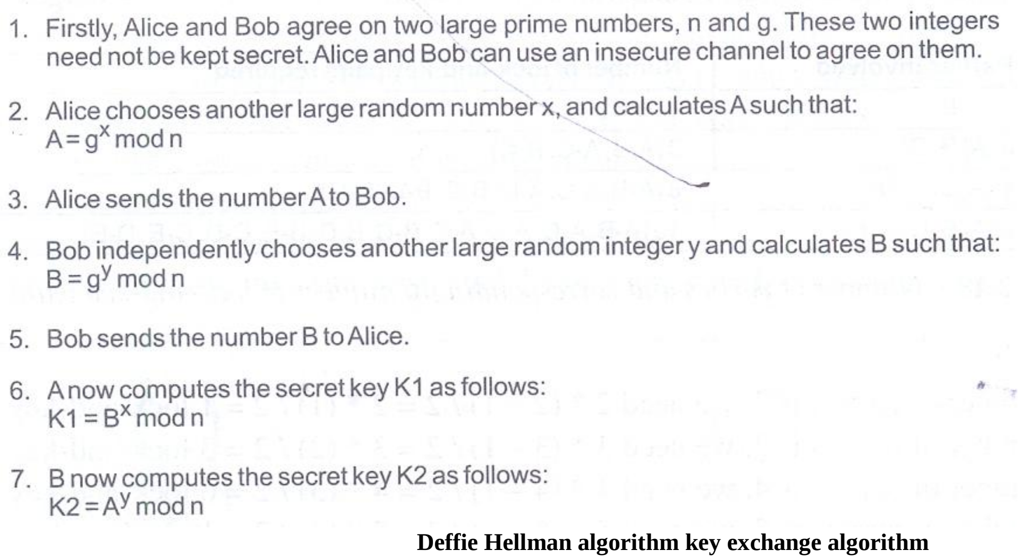
BOISE STATE UNIVERSITY EE 542/452 Spring 2008

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 indicates whether the information bits are for user speech/ data or signaling.

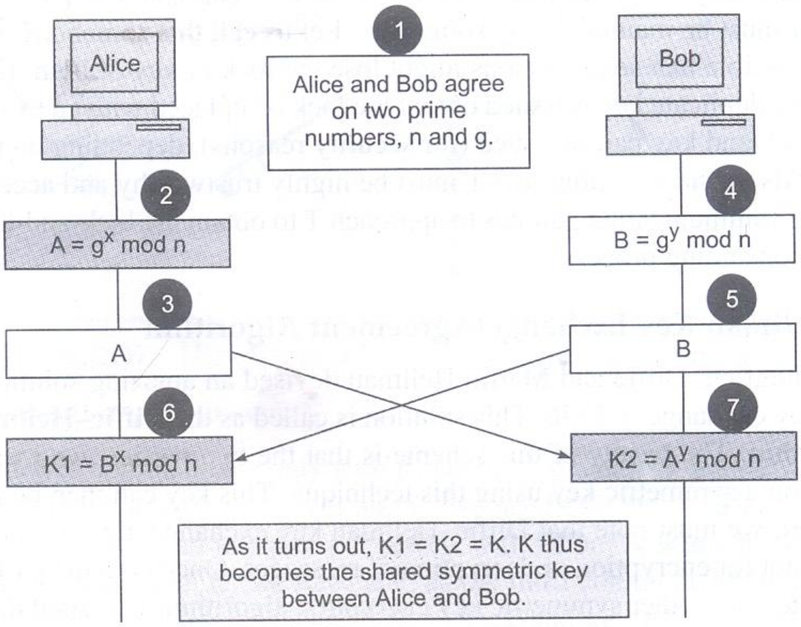
d) Explain any one Symmetric key Algorithm.
(Explanation of algorithm 4M)

Symmetric Key algorithm: Deffie Hellman algorithm is a symmetric Key algorithm

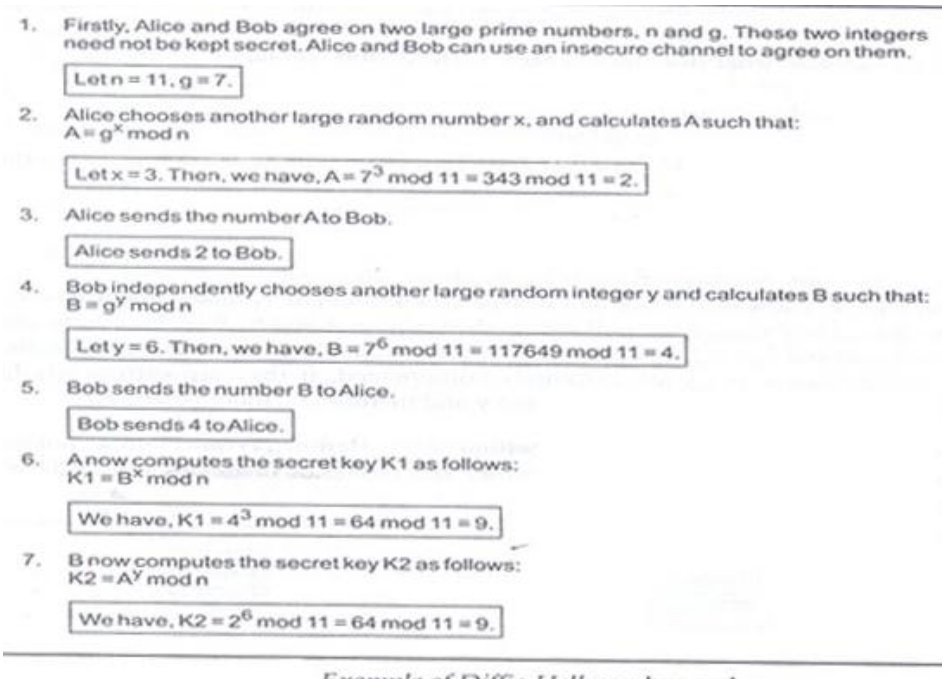


1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.
2. Alice chooses another large random number x, and calculates A such that: $A = g^x \bmod n$
3. Alice sends the number A to Bob.
4. Bob independently chooses another large random integer y and calculates B such that: $B = g^y \bmod n$
5. Bob sends the number B to Alice.
6. A now computes the secret key K1 as follows: $K1 = B^x \bmod n$
7. B now computes the secret key K2 as follows: $K2 = A^y \bmod n$

Deffie Hellman algorithm key exchange algorithm


Alice
Bob
1
Alice and Bob agree on two prime numbers, n and g.
2
A = g^x mod n
3
A
4
B = g^y mod n
5
B
6
K1 = B^x mod n
7
K2 = A^y mod n
As it turns out, K1 = K2 = K. K thus becomes the shared symmetric key between Alice and Bob.

Deffie Hellman key exchange illustrated



1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let n = 11, g = 7.

2. Alice chooses another large random number x, and calculates A such that: $A = g^x \bmod n$

   Let x = 3. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$.

3. Alice sends the number A to Bob.

   Alice sends 2 to Bob.

4. Bob independently chooses another large random integer y and calculates B such that: $B = g^y \bmod n$

   Let y = 6. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$.

5. Bob sends the number B to Alice.

   Bob sends 4 to Alice.

6. A now computes the secret key K1 as follows: $K1 = B^x \bmod n$

   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$.

7. B now computes the secret key K2 as follows: $K2 = A^y \bmod n$

   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$.

Example of Diffie-Hellman key exchange

e) **Explain Mobility Database. (HLR 2M, VLR 2M)**

Mobility Database:

- **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

  IMSI used by MS to access network

MSISDN

- Location information

ISDN number (address) of VLR and MSC where MS resides

- Service information

Service subscription

Service restrictions

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

□ IMSI

□ MSISDN

□ TMSI

Location information

□ MSC number

□ **Location area ID (LAI)**

Service information

□ Subset of the service information stored in the HLR

f) Give the features of Windows CE.
(Any four features 1M)

Features of Windows CE OS:

- Similar to windows 95.
- It is a Microsoft’s mobile os used in smart phones and mobile devices
- It is a 32 bit multitasking, multithreading os that has scalable, open architecture design , providing support for variety of devices . Windows CE is compact , providing high performance in limited memory configurations
- Standard communication support is built into this OS enabling access of internet.
- Integrated power management enabling long battery life
- GUI facilitating ease of use for end users
- Subset of *win 32 API :* widows CE supports more than 700 of the most frequently used win 32 APIs , enabling developers to take advantage of vast amounts of third party programming resources, tools , documentation for their windows CE based development
- Low cost, familiar development tools
- Scalable , full featured OS
- Extensive and extensible device support- supports keyboard, mouse devices, touch panels, serial ports , Ethernet modems, USB devices, audio devices, parallel port, printer devices, storage devices
- Wide microprocessor support

Q.3. Answer any FOUR of the following: 16

a) Explain Frequency reuse with neat sketch.
(Diagram 2M; Explanation 2M)

Frequency reuse is a technique of reusing frequencies and channels within a communication system to improve capacity and spectral efficiency. Frequency reuse is one of the fundamental concepts on which commercial wireless systems are based that involve the partitioning of an RF radiating area into cells. The increased capacity in a commercial wireless network, compared with a network with a single transmitter, comes from the fact that the same radio frequency can be reused in a different area for a completely different transmission.

Frequency reuse in mobile cellular systems means that frequencies allocated to the service are reused in a regular pattern of cells, each covered by one base station. The repeating regular pattern of cells is called cluster. Since each cell is designed to use radio frequencies only within its boundaries, the same frequencies can be reused in other cells not far away without interference, in another cluster. Such cells are called ‘co-channel’ cells. The reuse of frequencies enables a cellular system to handle a huge number of calls with a limited number of channels.

Figure shows a frequency planning with cluster size of 7, showing the co-channels cells in different clusters by the same letter. The closest distance between the co-channel cells (in different clusters) is determined by the choice of the cluster size and the layout of the cell cluster.

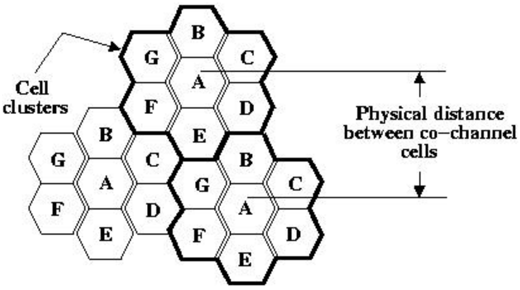


Figure: Frequency reuses technique of a cellular system.

b) Explain GSM channel types.

GSM uses number of channels to carry data over Air Interface, these channels are broadly divided in to following two categories:

1. **Physical Channels**
2. **Logical Channels**

PHYSICAL CHANNELS: (2M)

A physical channel is determined by the carrier frequency or a number of carrier frequencies with defined hopping sequence and the Time Slot number.

8 Time Slots (1 Time Slot = 1 Physical Channel) of 577 µs constitutes a 4.615 ms TDMA Frame. In GSM standard data on a time slot transmitted in bursts, so time slot is often expressed in BP (Burst Period). 1 BP represents 1 TS. TDMA frame (4.615 ms of 8 TS) further structured in to multiframes. There are two types of multiframes in the system:

- 26 TDMA Multiframe: Consists 26 TDMA frames with duration of 120 ms and used to carry the Logical Channels TCH, SACCH, FACCH etc.
- 51 TDMA Multiframe: Consists 51 TDMA frames with duration of 234.5 ms and used to carry the Logical Channels FCCH, SCH, BCCH, CCCH, SDCCH, SACCH etc.

LOGICAL CHANNELS: (2M)

Logical Channels are determined by the information carried within the physical channel. Logical channels used to carry data and signaling information. Different logical channels are mapped in either direction on physical channels.

Logical channels divided in to following two categories:

- Traffic Channels
- Signaling Channels

TRAFFIC CHANNELS

In GSM system two types of traffic channels used:

- **Full Rate Traffic Channels (TCHF):** This channel carries information at rate of 22.8 Kbps.
- **Half Rate Traffic Channels (TCHH):** This channel carries information at rate of 11.4 Kbps.

SIGNALLING CHANNELS

Signaling channel carries control information to enable the system to operate correctly. There are three main categories of signaling channels in GSM which are further divided in several categories:

1. BROADCAST CHANNELS (BCH)

- Broadcast Control Channel (BCCH)
- Frequency Correction Channel (FCCH)
- Synchronization Channel (SCH)
- Cell Broadcast Channel (CBCH)

2. COMMON CONTROL CHANNELS (CCCH)

- Paging Channel (PCH)
- Random Access Channel (RACH)
- Access Grant Channel (AGCH)

3. DEDICATED CONTROL CHANNELS (DCCH)

- Standalone Dedicated Control Channel (SDCCH)
- Fast Associated Control Channel (FACCH)
- Slow Associated Control Channel (SACCH)

BROADCAST CONTROL CHANNEL (BCCH) – DOWNLINK

- Broadcasts Network and Cell specific information required to identify the network and gain access.
- Broadcast parameters include Location Area Code (LAC), Mobile Network Code (MNC), Control Channel Structures, BCCH frequencies of neighboring Cells and other access parameters.

FREQUENCY CORRECTION CHANNEL (FCCH) – DOWNLINK

- This channel contains frequency correction bursts, used by the mobiles for frequency correction.
- Bears information for frequency Synchronization.

SYNCHRONIZATION CHANNEL (SCH) – DOWNLINK

- This channel is used by the MS to learn the Base Station Information Code (BSIC) as well as the TDMA frame number (FN).
- 6 bits of BSIC having two parts. 3 bits NCC and 3 bits BCC. NCC stands for Network Color Code and used to identify the BTS for which measurement is made. BCC stands for Base-Station Color Code and used for a better transmission in case of interference.
- BICS avoids ambiguity or interference which can arise when a Mobile Station can receive SCH from two cells using the same BCCH frequency.

CELL BROADCAST CONTROL CHANNEL (CBCH) – DOWNLINK

- This channel is used to broadcast specific information to network subscribers; such as weather, traffic, sports, stocks and other public services and announcement.
- This channel is assigned with SDCCH and usually occupies the second sub slot of the SDCCH.

PAGING CHANNEL (PCH) – DOWNLINK

- This channel is used for alerting to Mobile Subscribers for incoming calls, SMS and other mobility services.
- Every MS in a cell periodically listen to this channel.

RANDOM ACCESS CHANNEL (RACCH) – UPLINK

- This channel is used by a MS seeking attention of the BTS. When MS wants to initiate dialogue with network, this channel is used to send request to the network for a dedicated resource.
- The real dialogue between MS and Network will take place on the dedicated channel.
- If the request is not granted within a specific time period by the network, the MS repeats the request on the RACCH.

ACCESS GRANT CHANNEL (AGCH) – DOWNLINK

- This channel is used by a BTS to notify the MS of the assignment of an initial SDCCH for initial signaling.
- In response to request from MS on RACH, the network allocates a specific dedicated signaling channel (SDCCH) for further communication. This response is sent on AGCH.

STAND-ALONE DEDICATED CONTROL CHANNEL (SDCCH) – UPLINK/DOWNLINK

- In response of RACCH, network allocates SDCCH over AGCH for further communication between MS and BTS.

- This channel is used for the Location Update, Voice Call Set up and SMS.

FAST ASSOCIATED CONTROL CHANNEL (FACCH) – UPLINK/DOWNLINK

- This channel is used to convey Handover information.

- There is no TS and frame allocation dedicated to this channel. This channel can be associated with SDCCH or TCH and works on the principle of stealing. The burst of TCH is replaced by FACCH signaling when required.

SLOW ASSOCIATED CONTROL CHANNEL (SACCH) – UPLINK/DOWNLINK

- This channel is always associated with TCH or SDDCH used for control and supervision of signals associated with the traffic channels.

- Used to convey the periodic carrier-signal strength measurements to the network, transmit power control and timing advance.

c) Explain HLR failure Restoration.

(Message Flow diagram: 1 M, Steps: 3 M)

HLR Failure Restoration:

1. It is mandatory to save the updates into nonvolatile storage.
2. Changes of the service information are saved into the backup storage device immediately after any update.
3. The location information is periodically transferred from the HLR into the backup.
4. After an HLR failure, the data in the backup are reloaded into the HLR.

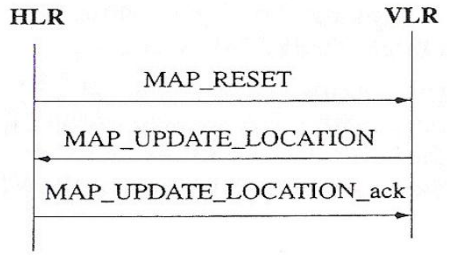


Fig: HLR Restoration Procedure Message Flow

After an HLR failure, the data in the backup are reloaded into the HLR.
• An Uncovered Period = the time interval after the last backup operation and before the restart of the HLR.
• Data that have been changed in the uncovered period cannot be recovered.
Step 1. The HLR sends an SS7 TCAP message MAP_RESET to the VLRs where its MSs are located. Step 2. All the VLRs derive all MSs of the HLR. For each MS, they send an SS7 TCAP message, MAP_UPDATE_LOCATION, to the HLR.
• The HLR restoration procedure is not robust.
– An MS may move into a VLR (which does not have any other MSs from the given HLR residing) during the uncovered period.
– The new location is not known to the HLR at the last check-pointing time.
– If so, the HLR will not be locate the VLR of the MS during Step 1 of HLR restoration.

d) Give application and limitation of GPRS

(Any four applications: 2 M, Any four Limitations: 2 M)
Application 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 -** Still images such as photographs, pictures, postcards, greeting cards and presentations, static web pages can be sent and received over the mobile network as they are across fixed telephone networks. It will be possible with GPRS to post images from a digital camera connected to a GPRS radio device directly to an Internet site, allowing near real-time desktop publishing.
5. **Moving Images -** Over time, the nature and form of mobile communication is getting less textual and more visual. The wireless industry is moving from text messages to icons and picture messages to photographs and blueprints to video messages and movie previews being downloaded and on to full blown movie watching via data streaming on a mobile device.

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** - 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.

3. **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.
4. **Support of GPRS Mobile Terminate by Terminals is Not Ensured -** At the time of writing, there has been no confirmation from any handset vendors that mobile terminated GPRS calls (i.e. receipt of GPRS calls on the mobile phone) will be supported by the initial GPRS terminals. Availability or not of GPRS MT is a central question with critical impact on the GPRS business case such as application migration from other non-voice bearers.

e) Give the features of Symbian OS.

(Any four Features, 1 M each)

1. **Processes and Threads:** Symbian OS is a multitasking and multithreaded operating system. Many processes can run concurrently, can communicate with each other, and can utilize multiple threads that run internal to each process
2. **Common File system Support:** Symbian OS organizes access to system storage using a file system model, just like larger operating systems. It has a default file system compatible with Windows ((by default, it uses a FAT-32 file system); it supports other file system implementations through a plug-in style interface. Symbian OS supports several different types of file systems, including FAT-16 and FAT-32, NTFS, and many storage card formats
3. **Networking:** Symbian OS supports TCP/IP networking as well as several other communication interfaces, such as serial, infrared, and Bluetooth.
4. **Memory management:** It organizes memory access in pages and allows for the replacement of pages, that is, bringing pages in, but not swapping them out

f) Explain Android architecture with diagram.

(Architecture diagram: 2 M, Explanation: 2 M)

Android operating system is a stack of software components which is roughly divided into five sections and four main layers as shown below in the architecture diagram.

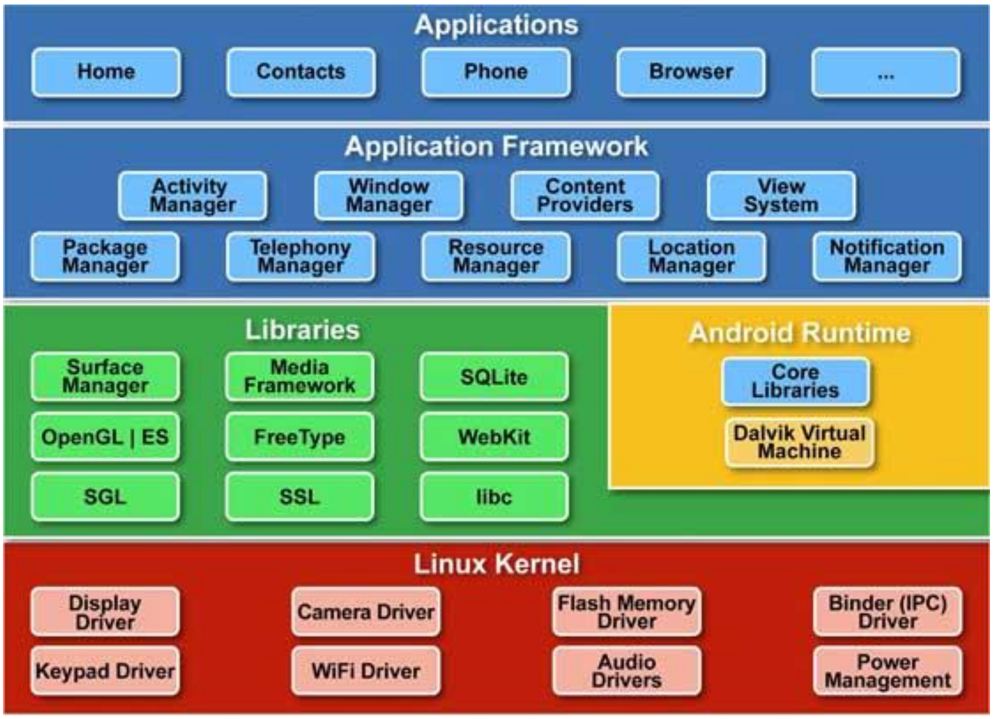


Fig: Android Architecture

Linux kernel

At the bottom of the layers is Linux - Linux 2.6 with approximately 115 patches. This provides basic system functionality like process management, memory management, device management like camera, keypad, display etc. Also, the kernel handles all the things that Linux is really good at such as networking and a vast array of device drivers, which take the pain out of interfacing to peripheral hardware.

Libraries

On top of Linux kernel there is a set of libraries including open-source Web browser engine WebKit, well known library libc, SQLite database which is a useful repository for storage and sharing of application data, libraries to play and record audio and video, SSL libraries responsible for Internet security etc.

Android Runtime

This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called **Dalvik Virtual Machine** which is a kind of Java Virtual Machine specially designed and optimized for Android.

The Dalvik VM makes use of Linux core features like memory management and multi-threading, which is intrinsic in the Java language. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine.

The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.

Application Framework

The Application Framework layer provides many higher-level services to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications.

Applications

You will find all the Android application at the top layer. You will write your application to be installed on this layer only. Examples of such applications are Contacts Books, Browser, and Games etc.

Q.4.

A. Answer any THREE of the following: 12

a) Explain Handoff strategies.

(Hand off: 1 M, Types: 3 M)

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.

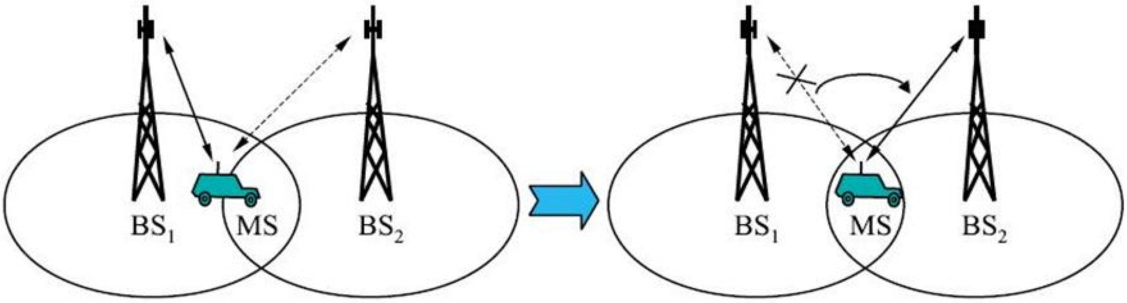


Fig: Handoff

Handoffs may be classified into two types:

- **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.
- **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.

b) Explain how GSM to PSTN call takes place in Mobile Environment.

(Steps: 4 M)

Mobile Phone (GSM) to Public Switched Telephone Network (PSTN) –

Procedure: When a mobile subscriber makes a call to a PSTN telephone subscriber, the following sequence of events takes place:

1. The MSC/VLR receives the message of a call request.
2. The MSC/VLR checks if the mobile station is authorized to access the network. If so, the mobile station is activated. If the mobile station is not authorized, then the service will be denied.
3. MSC/VLR analyzes the number and initiates a call setup with the PSTN.
4. MSC/VLR asks the corresponding BSC to allocate a traffic channel (a radio channel and a time slot).
5. The BSC allocates the traffic channel and passes the information to the mobile station.
6. The called party answers the call and the conversation takes place.
7. The mobile station keeps on taking measurements of the radio channels in the present cell and the neighboring cells and passes the information to the BSC. The BSC decides if a handover is required. If so, a new traffic channel is allocated to the mobile station and the handover takes place. If handover is not required, the mobile station continues to transmit in the same frequency.

c) **What is multifactor security? How it is achieved in mobile Environment?**
(Definition: 1 M, 3 Factors: 1 M each)

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:

1. **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.

- Password
- Pass Phrase
- PIN
- Answer to some personal question
- Sequence of a Number
- Predetermined events

2. **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. Various token/card technologies support authentication along these lines. For all, *2-factor authentication* becomes important an authentication process that involves 2 independent means of authenticating the principal. So, we might require that a principal not only possess a device but also know some secret password (often known as a PIN, or personal identification number). Without 2-factor authentication, stealing the device would allow an attacker to impersonate the owner of the device; with 2-factor authentication, the attacker would still have another authentication burden to overcome.

- *Magnetic strip card*. (e.g. Credit card) One serious problem with these cards is that they are fairly easy to duplicate. It only costs about $50 to buy a writer, and it's easy to get your hands on cards to copy them. To get around these problems, banks implement 2-factor authentication by requiring knowledge of a 4 to 7 character PIN whenever the card is used.
- *Proximity card or RFID*. These cards transmit stored information to a monitor via RF. There is currently a debate in this country as to the merits of using RF proximity cards (RFID tags) for identification of people and products.
- *Challenge/Response cards and Cryptographic Calculators*. These are also called *smart cards* and perform some sort of cryptographic calculation. Sometimes the card will have memory, and sometimes it will have an associated PIN. A smart card transforms the authentication problem for humans, because we are no longer constrained by stringent computational and storage limitations. Unfortunately, today's smart cards are vulnerable to power-analysis attacks.

3. **What You Are**

Since people forget things and lose things, one might contemplate basing an authentication scheme for humans on something that a person is. After all, we recognize people we interact with not because of some password protocol but because of how they look or how they sound --- "something they are". Authentication based on "something you are" will employ behavioral and physiological characteristics of the principal. These characteristics must be easily measured accurately and preferably are things that are difficult to spoof. For example, we might use

- Retinal scan
- Fingerprint reader
- Handprint reader
- Voice print
- Keystroke timing
- Signature
- Face (picture in passport)
- Biometrics

d) What do you mean by attacks? Give its categories.
(Attacks: 1 M, Types 1 M, Explanation of its types: 1 M each)

ATTACK: An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, botnet, phishing, spamming, inside and outside.
It is classified in two types
Active Attack: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data in route to the target.
Types of active attacks:

1. Masquerade Attack: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.
2. Session Replay Attack: In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.
3. Message Modification Attack: In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.
4. DoS Attack: In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

Passive Attack: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.
Passive attacks include active reconnaissance and passive reconnaissance. In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture. In active reconnaissance, the intruder engages with the target system through methods like port scans.
Types of passive attacks:

1. War driving: War driving detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna. The attack is typically carried out from a moving vehicle, sometimes with GPS systems that hackers use to plot out areas with vulnerabilities on a map. War driving can be done just to steal an Internet connection or as a preliminary activity for a future attack.
2. Dumpster diving: In dumpster diving, intruders look for information stored on discarded computers and other devices or even passwords in trash bins. The intruders can then use this information to facilitate covert entry to a network or system.
3. Intruder attack: An intruder might masquerade as an authorized network user and spy without interaction. With that access, an intruder might monitor network traffic by setting the network adapter to promiscuous mode.

B. Answer any ONE of the following: 6

a) Explain Location tracking and call setup in GSM.
(Location Tracking: 2 M, Call setup: 2 M, Diagram 2M)

Location Tracking: A GSM network is divided into cells. A group of cells is considered a location area. A mobile phone in motion keeps the network informed about changes in the location area. If the mobile moves from a cell in one location area to a cell in another location area, the mobile phone should perform a location area update to inform the network about the exact location of the mobile phone.

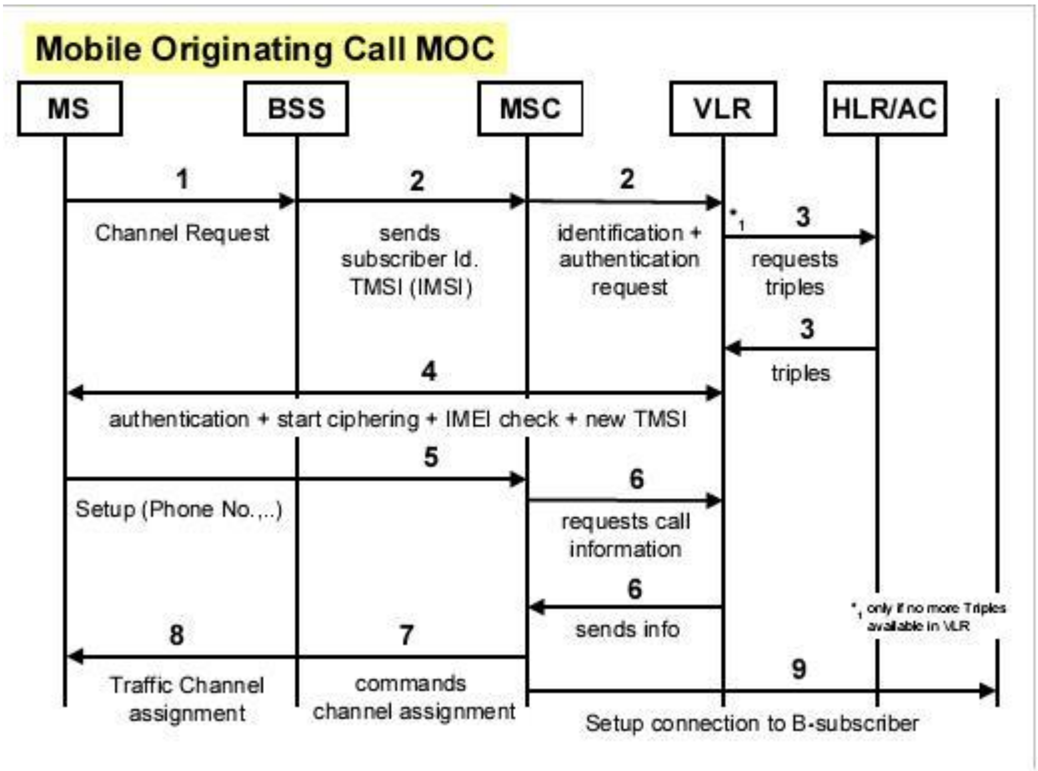
Home Location Register (HLR) The HLR maintains a database for the mobile subscribers. At any point of time, the HLR knows the address of the MSC VLR that controls the current location area of the mobile. The HLR is informed about a location area update only if the location area change has resulted in a change of the MSC VLR.

Mobile Switching Center - Visitor Location Register (MSC VLR) The MSC VLR is responsible to switching voice calls and it also keeps track of the exact location area where the mobile user is present

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 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 via HLR for Triples (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)
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)


Mobile Originating Call MOC
MS
BSS
MSC
VLR
HLR/AC
1
Channel Request
2
sends subscriber Id. TMSI (IMSI)
2
identification + authentication request
*1
3
requests triples
3
triples
4
authentication + start ciphering + IMEI check + new TMSI
5
Setup (Phone No.,..)
6
requests call information
6
sends info
*1 only if no more Triples available in VLR
8
Traffic Channel assignment
7
commands channel assignment
9
Setup connection to B-subscriber

Request Access

- The MS sends a *Channel Request* (CHAN_REQ) message on the RACH.
- The BSS responds with a radio resource assignment (IMM_ASS_CMD) on the AGCH.
- The MS sends a *Service Request* (CM_SERV_REQ) message to the BSS on the SDCCH.

Call Establishment

Once the MSC receives the ACM, it sends an ALERT message to the MS indicating that the call is going through. The BSS sends the ALERT message on the FACCH. Once the MS receives the ALERT, it will generate the ringing sound in the earpiece. The BSS sends an alerting message the subscriber will hear the line ringing.

Once the called party answers the phone, the PSTN will send an Answer message to the MSC. The MSC forwards this to the MS in a Connection (CON) message.

Once the MS receives the CON message, it switches over to voice and begins the call. All voice traffic occurs on the assigned TCH.

Call Termination

When either the caller or the called party hangs up, the call will be disconnected. Either party can initiate the disconnect. In this example, the MS initiates the disconnect. The MS sends a Disconnect (DISC) message to the BTS on the FACCH.

The BSS forwards the DISC to the MSC. Once the MSC receives the DISC message, it sends a Release (REL) message through the GMSC to the PSTN as well as down through the BSS to the MS.

The MS responds by sending a Release Complete (REL_COM) message to the BSS on the FACCH.

The BSS forwards the REL_COM message up to the MSC. Once the MSC receives the REL_COM message the call is considered ended from the call control perspective.

Although the call has ended, the BSS still has a TCH allocated to the MS. The MSC sends a Channel Release (CHAN_REL) message to the BSS. The BSS forwards the CHAN_REL message to the MS.

The MS responds with a DISC (LAPDm) message and returns to an idle mode. The BSS reallocates the channel for other call or releases the TRX.

b) Explain any one public key Cryptography algorithm.

(Public Key Cryptography: 2 M, Any one Algorithm: 4M)

Public-key cryptography is also known as asymmetric-key cryptography. Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the public key and the private key.

Two of the best-known uses of public-key cryptography are:

- *Public-key encryption*, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.
- *Digital signatures*, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as any manipulation of the message will result in changes to the encoded message digest, which otherwise remains unchanged between the sender and receiver.

RSA Algorithm:

Generating Public and Private Keys:

1. pick two prime numbers, we'll pick p = 3 and q = 11
2. calculate n = p * q = 3 * 11 = 33
3. calculate z = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20
4. Choose a prime number k, such that k is co-prime to z, i.e, z is not divisible by k. We have several choices for k: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5). Let's pick k=7 (smaller k, "less math").
5. So, the numbers n = 33 and k = 7 become the Server's public key.
6. Now, still done in advance of any transmission, the Server has to calculate it's secret key. Which is calculated as
7. k * j = 1 (mod z)
8. 7 * j = 1 (mod 20)
9. (7 * j) / 20 = X with the remainder of 1

   Note: the "X" here means: "something", we are only interested in the remainder). Since we selected (on purpose) to work with small numbers, we can easily conclude that 21 / 20 gives "something" with the remainder of 1. So, 7 * j = 21, and j = 3. This is our secret key. We MUST NOT give this key away.

Encrypting the message:

1. P ^ k = E (mod n) "^" means "to the power of" P is the Plain message we want to encrypt n and k are Server's public key E is our Encrypted message we want to generate
2. After plugging in the values, this equation is solved as follows:
   14 ^ 7 = E (mod 33)
   This equation says: raise 14 to the power of 7, divide this by 33, giving the remainder of E.
3. 105413504 / 33 = 3194348.606
4. 3194348 * 33 = 10541348
5. E = 105413504 - 10541348 = 20

So, Encrypted message is E=20.

Decrypting the Message:

1. E ^ j = P (mod n)
   E is the Encrypted message just received, j is the Server's secret key, P is the Plain message we are

trying to recover, n is Server's public key

After plugging in the values:

2. 20 ^ 3 = P (mod 33)
3. 8000 / 33 = X with the remainder of P.
   So to calculate this remainder.
4. 8000 / 33 = 242.424242...
5. 242 * 33 = 7986
6. P = 8000 - 7986 = 14.

So Decrypted message is D=14

RSA Algorithm Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of *m = 2* is $c = 2^7 \% 33 = 29$
- The decryption of *c = 29* is $m = 29^3 \% 33 = 2$

Q.5. Answer any TWO of the following: 16

a) Explain GSM architecture in detail with neat sketch.
(4M-diagram 4M Explanation)

GSM system consists of three major components:

(i) Base Station System (BSS).

(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 Trans receiver 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 U_m interface and it is also connected to BSC via the A_{bis} interface.

The U_m 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.

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 then the roaming subscriber.

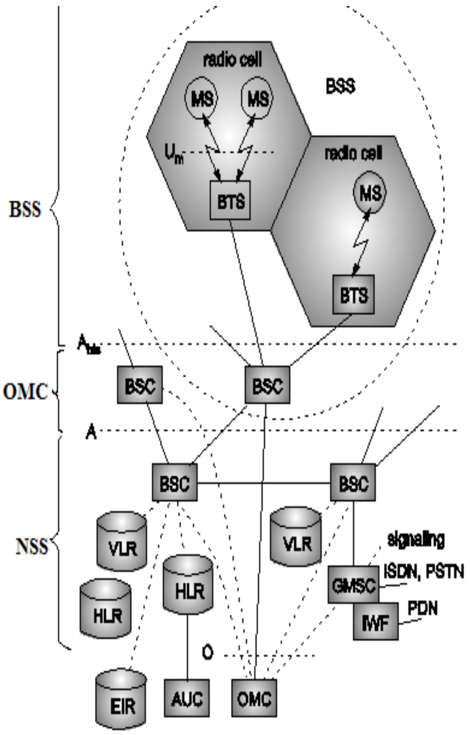
Visitor Location Register (VLR): It is a database which consists of temporary information about subscribers which is used by MSC in order to provide services to visiting subscriber. MSC updates the VLR by determining which users are in roaming. Once, the roaming mobile information is updated, then MSC sends necessary information to roaming mobile subscribers so that roaming mobile call can be properly routed.

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.



b) Explain 3GPP security and smart card security.

(4M-3GPP security Explanation 1M for each point 4M- smart card security Explanation 1M for each point)

- **3GPP:** 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
- 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.

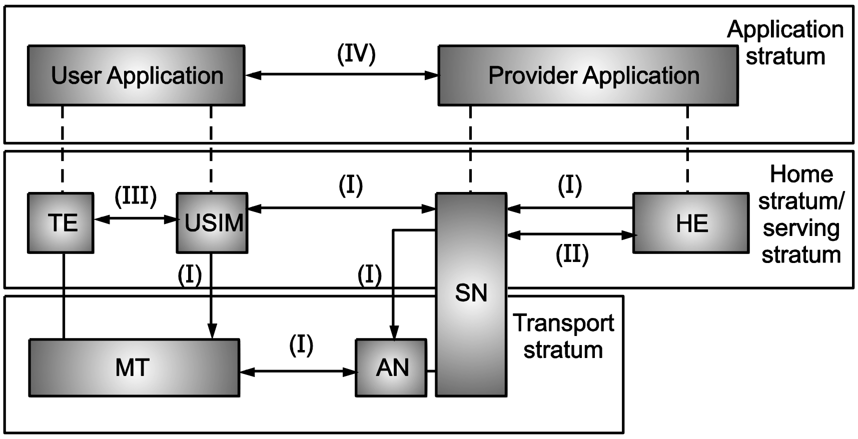


Fig Overview of the 3G security architecture

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:

What is smart card?

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. 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.

c) **Explain GPRS architecture in detail with neat sketch.**
(Diagram 4M; GPRS 4M)
GPRS Architecture

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.
- GPRS is usually attempts to reuse the existing GSM network elements as much as possible. There are new entities called GPRS that supports nodes (GSN) which are responsible for delivery and routing of data packets between mobile stations and external packets networks. There are two types of GSNs,
  - Serving GPRS Support Node (SGNS)

– Gateway GPRS Support Node (GGNS)

- There is also a new database called GPRS register which is located with HLR. It stores routing information's and maps the IMSI to a PDN address. Thus, GPRS Reference Architecture is shown as:

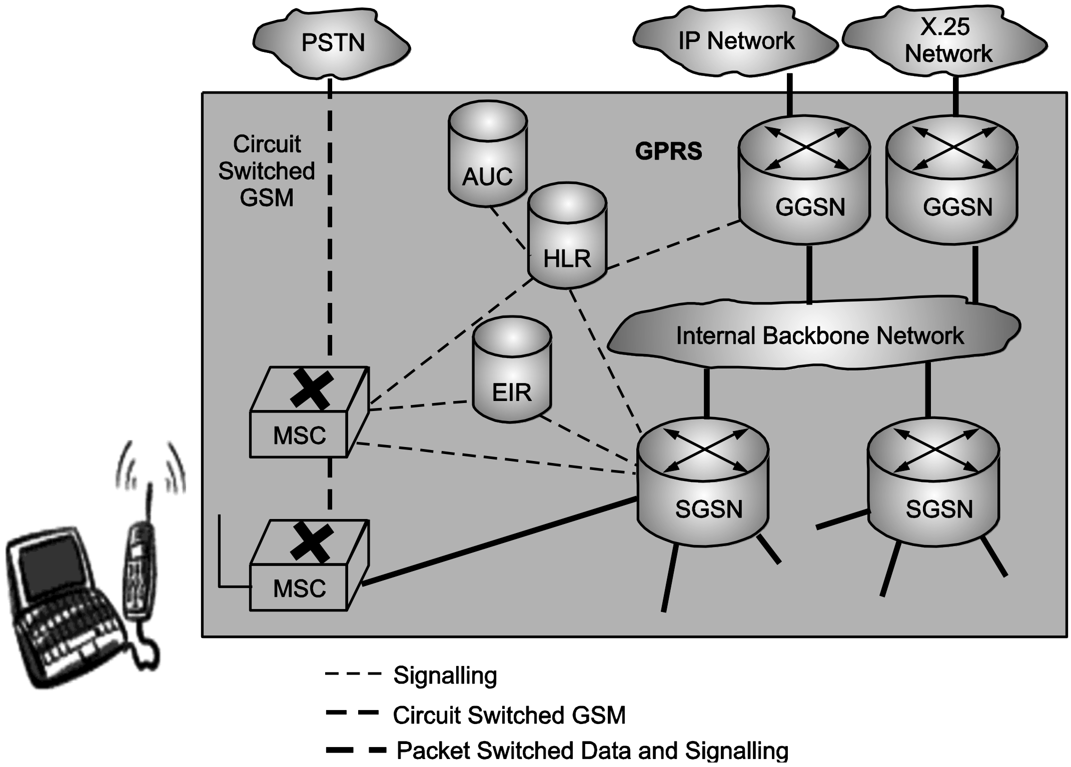


Fig.: GPRS Architecture

- The MS and the BSS communicate via the Um interface. The BSS and the SGSN are connected by the Gb interface using frame relay. Within the same GPRS network, SGNS/GGSN are connected through the Gn interface. When SGSN and GGSN are in different GPRS networks, they are interconnected via the Gp interface. The GGSN connects to external networks through the Gi interface. The MSC/VLR communicates with the BSS using the existing GSM A interface, and with the SGSN using the Gs interface. The HLR connects to the SGSN via the Gr interface, and to the GGSN via the GC interface. Both Gr and GC follow the GSM Mobile Application Part (MAP) protocol. The HLR and the VLR are connected through the existing GSM D interface. Interfaces A, Gs, Gr, GC, and D are used for signaling, without involving user data transmission in GPRS. Note that the A interface is used for both signaling and voice transmission in GSM. Interfaces Urn, Gb, Gn, Gp and Gi are used for both signaling and transmission in GPRS.

Q.6. Answer any FOUR of the following: 16

a) What is co channel Interference? How it can be controlled?

Co-channel interference (2M Explanation)

- Due to frequency reuse, several cells in a same coverage area use same frequency. These cells are known as co-channel cell.
- The interference between signals from these co-channel cells is called co-channel interference.
- Co-channel interference cannot be reduced by simply increasing the carrier power of transmitter.
- If we increase transmit power of carrier, it will increase interference to neighbouring channel cell.

How to avoid: **(2M Explanation)**

To reduce co-channel interference, co-channel cell can be physically be separated by minimum distance.

b) How a signal is processed in GSM?(Diagram 2M, Explanation 2M)

GSM signal is processing from transmitter to receiver.

1. Speech coding:

The GSM speech coder is based on the Residually Excited Linear Predictive Coder (RELP), which is enhanced by Long Term Predictor (LTP).

The coder provides 260 bits for each 20 ms block speech, which means a bit rate of 13 kbps.

In the normal conversation, each person speaks on average for less than 40% of the time. By incorporating Voice Activity Detector (VAD) in speech coder, GSM system operates in a discontinuous transmission mode (DTX) which provides longer battery life and reduced radio interface since the GSM transmitter is not active in silent period.

A Comfort Noise Subsystem (CNS) at the receiving end introduces background acoustic noise to compensate for the annoying switched muting which occurs due to DTX.

2. Channel Coding (TCH/FS, SACCH and FACCH):

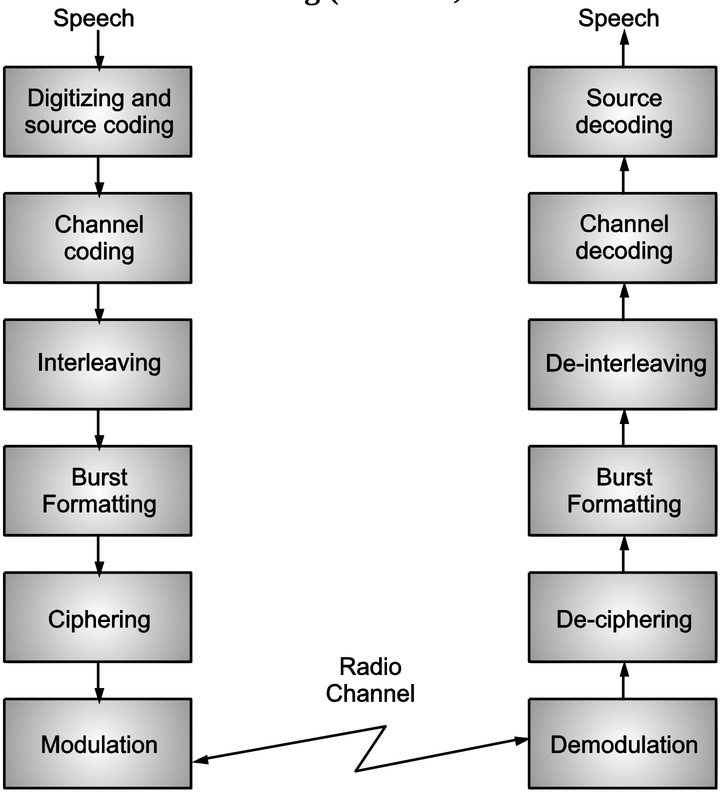


Fig: GSM operations from speech input to speech output

The output bits of speech coder are grouped for error protection, 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. This facilitates the detection of non-correctable error at the receiver.

The next 132 bits along with first 53 (50 types Ia bits + 3 parity bits) appended by four zero bits, thus, providing a data block of 189 bits. This block is then encoded for error protection. It provides a sequence of 378 bits. The least important 78 bits do not have any error protection and are concatenated to the existing sequence of block of 456 bits in 20 ms frame error protection coding increases the gross data rate of GSM speech signal, with channel coding to 22.8 kbps.

Interleaving:

In order to reduce the effect of sudden fades on the received data, the total 456 encoded bits within each 20 ms speech frame or control message frame are broken into eight 57 bits subblocks.

These eight sub-blocks which make up a single speech frame are spread over eight consecutive TCH time slots.

If a burst is lost due to interference or fading, channel coding ensures that enough bits will still received correctly to allow error correction. Fig. 2.6 shows that how speech frames are diagonally interleaved within the time slots.

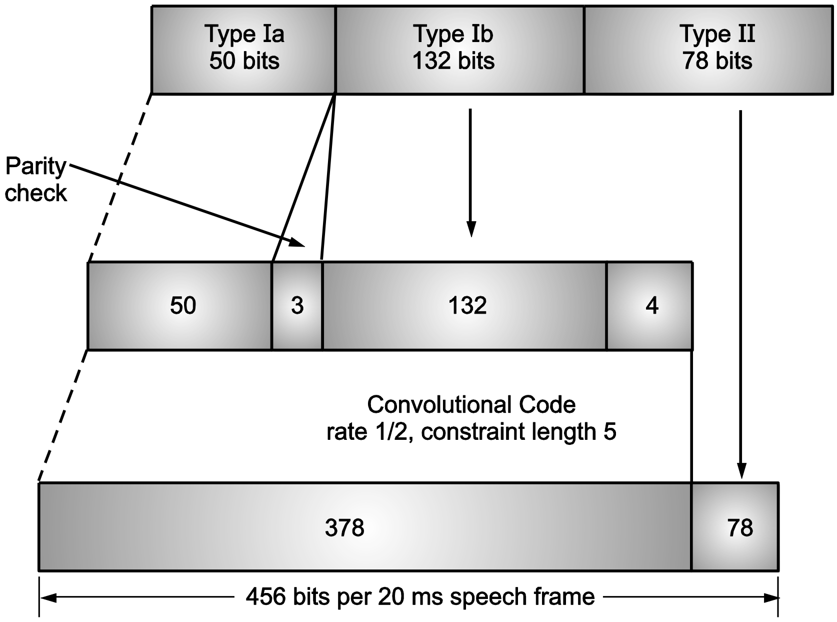


Fig.: Error protection for speech signals in GSM

Ciphering:

Ciphering made changes in a content of eight interleaved blocks through the use of encryption technique. Security is also enhanced by the changes in encryption algorithm call to call Two types of security algorithm called A3 and A5 are used in GSM to prevent unauthorised network access. A5 algorithm is used to authenticate each mobile by verifying user password within SIM (Subscriber Identity Module). A5 algorithm provides the scrambling for the 114 coded data bits.

Burst formatting:

Burst formatting adds binary data to ciphered block, in order to help synchronization of the received signal.

Modulation:

Modulation technique used by GSM is 0.3 GMSK, where 0.3 describes the 3 dB bandwidth. GMSK is a special type of FM modulation. Binary once and zeros are represented in GSM by shifting the radio frequency carrier by ± 67.708 kHz. This minimise the bandwidth occupied by the modulated spectrum and hence improved channel capacity.

Frequency hopping:

Under normal condition, data belong to particular physical channel is transmitted using same frequency. Some time user in a particular cell have served with multipath problem, then the cell can be called as hopping cell by the network operator, in that case slow frequency hopping is carried out to cope up with multipath. Frequency hopping is carried out frame by frame. Frequency hopping is specified by the service provider.

Equalization:

Equalization is performed at receiver end with the help of training sequences transmitted in midamble of every time slots. Type of equalization is not fixed in GSM, it depends upon manufacturer.

Demodulation:

At receiver's end, appropriate TS is demodulated with the aid of synchronization data provided by the burst formatting. After demodulation the binary data is deciphered, de-interleaved, channel decoded and speech decoded.

c) What is GSM Location update? When it is occurred?
(2M Explanation)

- GSM "location update" is a part of registration. GSM networks keep track of the location area (LA) where the MS is operating. When receiving an incoming call, the MS is paged in all cell of its current location area.
- GSM mobile do a location update when entering to new location area and at periodic interval. In addition to this, MS also updates location in ease of activation and deactivation performed by the users.

When it occurred: (2M Explanation)

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.

d) Describe step procedure for VLR failure Restoration.

(2M Diagram 2M Explanation)

VLR Failure Restoration

After VLR failure, the service information of VLR record is recovered by first contact between the VLR and the HLR of the corresponding MS. The location information is recovered by the first contact between the VLR and the MS. The mobile station information is recovered either from HLR or MS.

VLR restoration procedure is initiated by one of the following three events.

− MS registration.
− MS call origination.
− MS call termination.

1. MS registration:

Since the record in the VLR get erased due to the failure, then the normal registration procedure define in inter-VLR movement is applied to recovered the VLR record. In this case, TMS1 sends from the MS to the VLR that is not recognised, and MS asked to send IMSI over the air.

2. MS call origination:

When VLR receives the call origination request MAP_SEND_INFO_FOR_ OUTGOING_CALL from the MSC, then the VLR record for the MS is not found. VLR considers this situation as a system error, with cause "unidentified subscriber". Request is then rejected and MS indicate the location registration procedure, then the VLR record is recovered.

3. MS call termination:

The call termination message flow is illustrated in Fig.

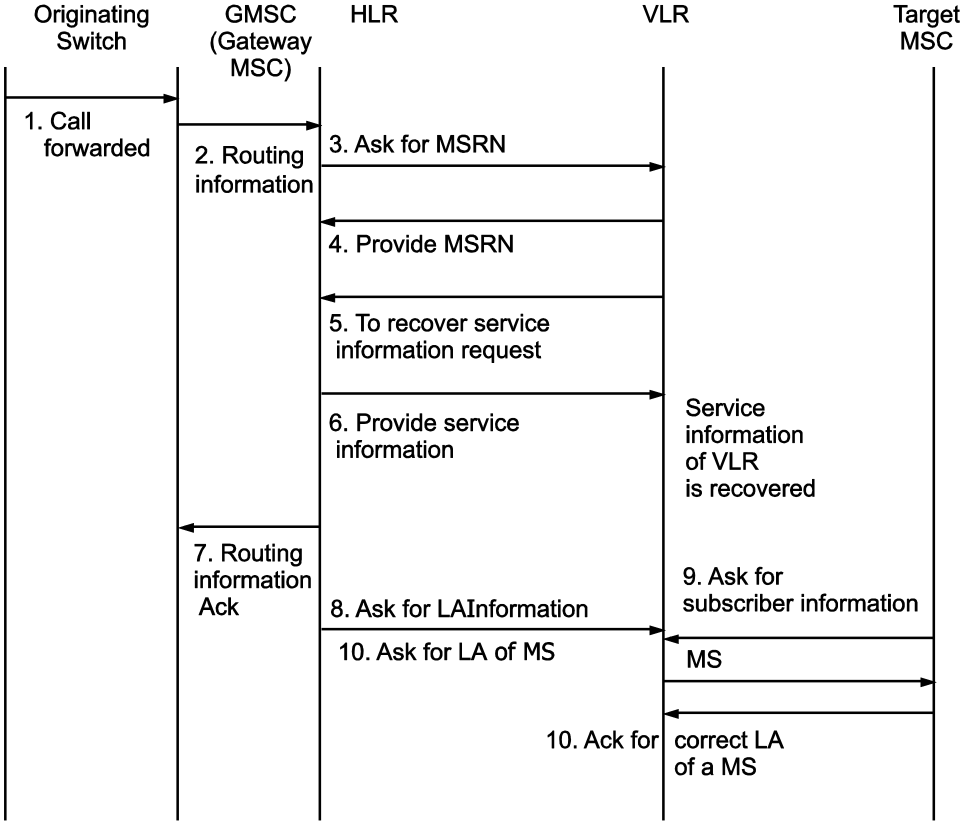

Originating Switch
GMSC (Gateway MSC)
HLR
VLR
Target MSC
1. Call forwarded
2. Routing information
3. Ask for MSRN
4. Provide MSRN
5. To recover service information request
6. Provide service information
Service information of VLR is recovered
7. Routing information Ack
8. Ask for LAInformation
9. Ask for subscriber information
10. Ask for LA of MS
MS
10. Ack for correct LA of a MS

Fig. VLR failure restoration

Step 1: When the MS ISDN is dialed the call is forwarded to GMSC (Gateway Mobile Switching Centre), GMSC is a switch which ask the HLR for routing information. The HLR request to VLR of the MS to provide the routing address for the MSRN (Mobile Station Roaming Number).

Step 2: The VLR returns the MSRN to the GMSC through the HLR.

Step 3: The GMC uses the MSRN to route the call to the MS through the visited MSC (Mobile Switching Centre).

[Note that the IMSI - (International Mobile Subscriber Identity) and the MSC number are provided in the message which is send from HLR to VLR].

Then the VLR searches MS record, but the record is erased due to the failure because of this the search PS fails the VLR creates a new VLR record for the MS.

Neither the service nor the location information is available in this record. Steps 4 and 5 are executed parallelly.

Step 4 and 5 :

VLR does not have routing information; it uses MSC number to create MSRN. The number is sent back to gateway MSC to set up the call in Step 8.

Step 6 and 7:

The VLR recovers service information by sending MAP_RESTORE_DATA message to HLR. Then HLR sends service information to VLR by using MAP_INSERT_SUBSCRIBER_DATA message.

At this point service information of VLR record has been recovered. Still the location information specifically the LAI number, still not available.

Step 8: After gateway MSC receive the MSRN in Step 7, the target MSC does not have LA information of the MS. In order to proceed to set up the call and asked for LAI information. Unfortunately VLR does not have LAI information. Hence, VLR ask MSC to determine the LA of MS by sending MAP_SEARCH_ FOR_MOBILE_SUBSCRIBER message.

Step 9: The MSC initiate paging of MS in all LAS. If the paging is successful, the current LA address of MS is sent back to VLR. At this point LA information of VLR record is recovered.

e) Describe data services used in GPRS.
(Explanation 4M)

At higher speeds GPRS is designed to provide packet-data Services at higher speeds than those available with standard GSM circuit switched data services. In theory GPRS could provide speeds of upto 171 kbps over the air interface, although such speeds are never achieved in practical network. In fact, the practical maximum speed is a little over 100 kbps.

- GPRS speeds are far greater than the 9.6 kbps maximum provided by standard GSM. The greater speeds provided by GPRS are achieved over the same basic air interface (i.e., the same 200 kHz channel, divided into eight time slots). With GPRS, the mobile station (MS) can have access to more than one time slots. Moreover the channel coding for GPRS is somewhat different from that for GSM. In fact, GPRS defines a number of different channel coding schemes, the most commonly used coding scheme for packet-data transfer is Coding Scheme 2 (CS-2), which enables a given time slot in carry data at a rate of13.4 kbps. If a single user has access to multiple time slots, then speeds such as 40.2 or 53.6 kbps become available to that user. lists the various coding schemes available and the associated data rates for single time slot.

Coding scheme with data rates

Coding Scheme	**Air-interface Data Rate (kbps)**	**Approximate Usable Data Rate (kbps)**
CS-1	9.05	6.8
CS-2	13.4	10.4
CS-3	15.6	11.7
CS-4	21.4	16.0

- The air-interface rates are given in Table The transmission of data in GPRS involves a number of layers above the air interface, with each layer adding certain amount of overhead, the amount of overhead generated by each layer depends on a number of factors, such as the size of the application packed to be transmitted for a given amount of data to be transmitted, smaller application packet sizes cause a greater net overhead than larger packet sizes. The result is that the rate for usable data is approximately 20 to 30 percent less than the air-interface rate.
- The most commonly used coding scheme for user data is CS-2. This scheme provides error correction over the air interface. Although CS-3 and CS-4 provide higher throughput, they are more susceptible to errors on the air interface. In fact, CS-4 provides no error correction at all on the air interface.
- The biggest advantage of GPRS is not simply the fact that it allows higher speeds. Perhaps the greatest advantage of GPRS is the fact that it is a packet switching technology.
- This means that a user consumes RF resources only when sending or receiving data. If a user is not sending data at a given instant, then the time slots on the air interface can be used by another user for example. a user that is browsing the Web. Data is transferred only when a new page is being

requested or sent, Nothing is being transferred while the subscriber just reading the contents of a page. During this time, same other user can access in the air-interface resources with no effect on Web-browsing friend. Clearly this is a very efficient use of scarce RF resources. The advantages of GPRS are that multiple users can share air-interface resources. The functionality of GPRS is such that this request-allocation procedure is well hidden from the user; and the service appears to be "always on".

f) Explain UMTS in detail.
(UMTS Explanation 4M)

- 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, 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.