## Data Encryption

- Data encryption translates data into another form or code so that only people with access to a secret key (decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plain text.
- currently, encryption is one of the most popular & effective data security methods used by organizations.
- Mainly two types of encryption -
  i) Symmetric encryption.
  ii) Asymmetric encryption (public-key encryption).

## Need for encryption

The purpose of data encryption is to protect digital data confidentially as it is stored on computer systems and transmitted using the internet or other computer networks. The outdated data encryption standard (DES) has been replaced by modern encryption algorithms that play a critical role in the security of IT systems and communications.

These algorithms provide confidentiality and drive key security initiatives including authentication. Authentication allows for the verification of message's origin & integrity provides proof that a message's contents have not changed since it was sent. Additionally, non-repudiation ensures that a message sender cannot deny sending the message.

## procedure of data encryption:

- Data or plaintext is encrypted with an encryption algorithm and an encryption key. The process results in ciphertext, which only can be viewed in its original form if it is decrypted with the correct key.
- Symmetric key ciphers use the same secreat key for encrypting and decrypting a message or file. While symmetric-key encryption is much faster than asymmetric the encryption, the sender must exchange the encryption key with the recipient before he can decrypt it. As companies find themselves needing to ~~security~~ surely distribute and manage huge quantities of keys, most data encryption services have adapted and use an asymmetric algorithm to exchange the secreat key after using a symmetric algorithm to encrypt data.
- On the other hand asymmetric cryptography sometimes reffered to as public-key cryptography uses two different keys, one public & one private key, as it is named, may be shared with every one, but the private key must be protected. ~~Three Rivest~~
- * ~~The Rivest-Shamir-Adleman (RSA) algorithm~~ is cryptosystem used ~~to secure sensitive~~ data,

09.04.20

# Architecture (block diagram) of mobile Communication Network :=>

- Mobile communication Network architechture mainly based on (i) MSC (1), (ii) HLR (3), (iii) VLR (4), (iv) BSC (2) / v) EIR

## 1) Mobile Switching Centre (MSC) :

- The Mobile switching centre or MSC is a sophisticated telephone exchange which provides circuit switched calling, ~~mobility~~ mobility management, & GSM services to the mobile phones, roaming within the area that it serves. This means voice, data & fax services, as well as SMS and call divert.

### * Mobile switching centre Types :

a) Gateway M.S.C. :→ It determines which visited MSC the subscribers who is being called is currently located. It also interfaces with the Public switched Telephone Network. All mobile to mobile calls and PSTN to mobile calls are routed through a GMSC.

b) Visited MSC : The visited MSC is the MSC where a customer is currently located. The VLR associated with this MSC will have the subscriber's data in it.

c) Anchor MSC : The Anchor MSC is the MSC from which a handover has been initiated.

d) Target MSC : The target MSC is the MSC toward which a handover would take place.

Tasks of the MSC :

- Delivering calls to subscribers as they arrive based on information from the VLR
- Connecting outgoing calls to other mobile subscribers or the PSTN
- Delivering SMS's from subscribers to the SMSc and vice-versa.
- Arranging handovers from BSC to BSC
- Carrying out handovers from this MSC to another
- Supporting supplementary services such as conference calls or call hold.
- Collecting billing information.

2. BSC (Base station Controller) : The BSC controls multiple BTSs. It handles allocation of radio channels, frequency administration, power and signal measurements from MS and hand over from one BTS to another (if both BTSs are controlled by the same BSC).

- A BSC also functions as a 'funneler'. It reduces the number of connections to the MSC and allows for higher capacity connection to the MSC.
- A BSC may be collected with or BTS or it may be geographically separate. It may even be collected with the MSC.




Scanned with CamScanner

# Home Location Register (HLR)

- The Home Location Register or HLR is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network.
- HLR stores details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI .
- HLR is a single database but can be maintained as separate databases when the data to be stored is more than the capacity.
- The HLR data is stored for as long as a subscriber remains with the mobile phone operator.

Contd.

## Data that are stored in the HLR are

- GSM services that the subscriber has requested or been given.
- GPRS(General packet radio service) settings to allow the subscriber to access packet services.
- Current Location of subscriber .
- Call divert settings applicable for each associated MSISDN.

If the HLR fails, then the mobile network is effectively disabled as it is the HLR which manages the Location Updates as mobile phones ream around.

Contd

## The HLR connects to the following elements:

- The Gateway MSC (G-MSC) for handling incoming calls.
- The VLR for handling requests from mobile phones to attach to the network.
- The SMSC for handling incoming SMS.
- The voice mail system for delivering notifications to the mobile phone that a message is waiting .

## Visitor Location Register (VLR)

- The Visitor Location Register or VLR is a temporary database of the subscribers who have roamed into the particular area which it serves. Each Base Station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time.

The data stored in the VLR has either been received from the HLR, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface.

## Data stored in VLR are

Contd.

- IMSI (the subscriber's identity number)
- Authentication data .
- MSISDN (the subscriber's phone number)
- GSM services that the subscriber is allowed to access .
- The HLR address of the subscriber

## The VLR connects to the following elements:

- The Visited MSC (V-MSC) to pass data needed by the V-MSC during its procedures, e.g. authentication or call setup.
- The HLR to request data for mobile phones attached to its serving area.
- Other VLRs to transfer temporary data concerning the mobile when they roam into new VLR areas.

## The primary functions of the VLR are:

Contd.

- To inform the HLR that a subscriber has arrived in the particular area covered by the VLR.
- To track where the subscriber is within the VLR area (location area) when no call is ongoing.
- To allow or disallow which services the subscriber may use
- To allocate roaming numbers during the processing of incoming calls
- To delete the subscriber record if a subscriber becomes inactive whilst in the area of a VLR. The VLR deletes the subscriber's data after a fixed time period of inactivity and informs the HLR.
- When the phone has been switched off and left off or when the subscriber has moved to an area with no coverage for a long time.
- To delete the subscriber record when a subscriber explicitly moves to another MSC, as instructed by the HLR.

# Equipment Identity Register and Billing Centre

**Equipment Identity Register (EIR): The EIR is often integrated to the HLR. The EIR keeps a list of mobile phones (identified by their IMEI) which are to be banned from the network or monitored. This is designed to allow tracking of stolen mobile phones. In theory all data about all stolen mobile phones should be distributed to all EIRs in the world through a Central EIR.**

**The Billing Centre (BC) is responsible for processing the toll tickets generated by the VLRs and HLRs and generating a bill for each subscriber. it is also responsible for to generate billing data of roaming subscriber.**