Chapter 3 : ADHOC and WSN

Q. 1 What is Adhoc network ? Explain challenges in designing Routing Protocol for Adhoc wireless networks. May 18, Dec. 19

Ans. :

Definition :

- A Wireless ad hoc network is a group of independent terminals or nodes which communicate with each other by forming a multihop radio network.

Design Issues / Challenges in Routing Protocol :

- The major design issues in adhoc networks are :
  1. Mobility of nodes
  2. Error-prone shared broadcast radio channel
  3. Resource constraints
  4. Bandwidth constraints

1. Mobility of nodes :

- In adhoc wireless networks, routing protocols should perform effective and efficient management of mobility of nodes.
- Due to movement of nodes, network topology becomes highly dynamic which results in the frequent path breaks in an ongoing session.
- Disturbance occurs in the network due to movement of end nodes or intermediate nodes in the path.
- The routing protocols of wired network cannot be used in adhoc wireless networks.

2. Error-prone shared broadcast radio channel :

- The routing protocols in Adhoc network should be able to search path with minimum congestion.
- A unique challenge in adhoc wireless networks is the broadcast nature of the radio channel.
- Time-varying characteristics of wireless links are link-capacity and link-error probability.
- The adhoc wireless routing protocols should interacts with MAC layer in order to find alternate routes through better link quality.
- In ad hoc network , the collision of data and control packets takes place at the time of transmission. This problem comes under hidden terminal problem.

3. Resource constraints :

- Two main and limited resources in an adhoc wireless network are processing power and battery life.
- The devices used in adhoc network requires portability and hence they have weight and size constraints.
- The nodes in ad hoc network becomes bulky and less portable by increasing the battery power and processing ability.
- These resource problems should be managed in routing protocols in ad hoc network.

4. Bandwidth constraints :

- Large amount of bandwidth is available in wired networks due to the advent of fiber optics and the utilization of WDM technologies .
- A wireless networks provides less data rate as compared to wired network because of limited radio band.
- To overcome these bandwidth constraints such routing protocols are required that use optimum bandwidth by keeping overhead as low as possible.
- The limited bandwidth availability creates limitation on routing protocol in order to maintain the topological information.
- Due to dynamic topology, it is very difficult to maintain topological information at each node that occupies more control overhead that results in wastage of bandwidth.

Q. 2 Differentiate between infrastructure network and infrastructure less network and what are issues in Adhoc wireless network ? May 18, Dec. 18, Dec. 19

Ans. :

Comparison of Infrastructure and Ad hoc Networks :

- Table 3.1 gives the comparison of infrastructure and ad hoc networks.

Table 3.1 : Comparison of Infrastructure and Ad hoc Networks

Sr. No.	Parameter	Infrastructure N/W	Ad hoc / infrastructure-less N/W
1.	Communication	Through an access point	Directly between devices
2.	Range	Determined by the range and number of access points	Restricted to the range of individual devices on the network.

Sr. No.	Parameter	Infrastructure N/W	Ad hoc / Infrastructure-less N/W
3.	Speed	Faster	Slower
4.	Unique IP address	Yes	Yes
5.	Security Options	More	Less

Issues and Challenges in Ad hoc Networks :

- To design an adhoc wireless networks, the following are major challenges and issues which affect the design, operation and performance of an ad hoc wireless system :
  1. Routing protocols.
  2. Multicasting.
  3. Transport layer protocol.
  4. Pricing schemes.
  5. Medium access scheme.
  6. Self-organisation.
  7. Security.
  8. Quality of service.
  9. Management of energy.
  10. Scalability.
  11. Discovery of service and addressing.
  12. Deployment considerations.

Q. 3 What are the MAC layer and Routing Layer Design goals ? **Dec. 18**

Ans. :

Design Goals of a MAC Protocol :

- The important design goals for a medium access control (MAC) protocol for ad hoc wireless networks are as follows :
  1. Its operation should be distributed.
  2. To provide QoS support for real-time traffic.
  3. The access delay, should be as short as possible. Access delay is the average delay experienced by any packet to get transmitted.
  4. To provide efficient utilization of the available bandwidth.
  5. It should fairly allocate the bandwidth to nodes.
  6. To minimize the control overheads.
  7. To minimize the effects of hidden and exposed terminal problems.
  8. The protocol must be scalable to large networks.
  9. There should be a power control mechanism for efficiently managing the energy consumption of the nodes.
  10. There should be mechanisms for adaptive data rate control. The adaptive rate control is ability to by considering the factors such as load in the network and the status of neighbor nodes.

Design Goals of Routing Protocols :

- The routing protocols for Adhoc wireless network should have following characteristics :

1. Fully distributed :

- It should be fully distributed. The centralized routing involves the risk of single point failure. The distributed routing is more fault-tolerant as compared to centralized routing.

2. Adaptive to frequent in topology :

- The routing protocol should be adaptive to frequent topology changes.

3. Connection set up time :

- Route calculation and maintenance in the network should involve minimum number of nodes. Minimum connection set up time is required because each node in the network must have quick access to routes.

4. Localized :

- The routing protocol should be localized as a huge state propagation control overhead is involved in a global state maintenance.

5. Loop free :

- The routing protocols in ad hoc network should be loop free and free from stale routes.

6. Reliable transmission :

- The packet transmission should be reliable, in order to reduce message loss and to prevent the occurrence of stale routes,.

7. Quick convergence of routes :

- The convergence should be fast. Once the network topology becomes stable, it should cover best possible routes.

8. Use of limited resources :

- It should use the limited sources like bandwidth, computing power, memory and battery power.

9. Information storage :

- Each node in the ad hoc network should try to store information regarding the stable local topology.

10. Quality of service :

- The routing protocol should provide a certain level of quality of service and provide support for the time-sensitive traffic.

Q. 4 Write short note on MACAW protocol.

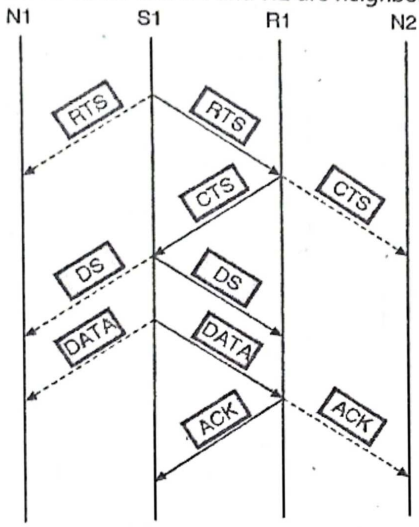
May 18, May 19, Dec. 19

Ans. :

- The operating principle of MACAW protocol is based on the MACA.

Operation of MACAW :

- Refer Fig. 3.1 to understand the operation of the MACAW protocol in which S1 is the source node, R1 is the receiver node and N1 and N2 are neighbor nodes.



(G-2029) Fig. 3.1 : Operation of MACAW

- Node S1 transmits RTS which is heard by R1 and overheard by node N1. Hence N1 waits until node S1 receives the CTS packet.
- Similarly node N2 overhears the CTS transmitted by node R1 and it postpones its transmission until node R1 receives the data packet.
- On receiving the CTS packet, node S1 sends DS message which carries the expected time required for the data packet transmission.
- After hearing this packet node N1 will backs off until the data packet is transmitted.
- As soon as R1 receives the data packet, it sends the acknowledgement of reception i.e. ACK packet to node S1. The MACAW gives a significantly improved performance as compared to MACA.

Summary of MACAW operation :

- The MACAW protocol was designed based on following four observations :
  1. The congestion always takes place at the receiver node and not at the sender. Therefore it is necessary to use the RTS-CTS-DATA exchange mechanism of MACA. This mechanism is further improved in MACAW by using the RTS-CTS-DS-DATA-ACK exchange mechanism.
  2. The congestion depends on the location of the receiver. Therefore, MACAW introduces separate back-off parameters for each flow.
  3. The process of learning about congestion at various nodes must be a collective effort. Therefore, MACAW has introduced the notion of copying back-off values from overheard packets.
  4. In order to allow the nodes to contend effectively for the channel, the synchronization information needs to be conveyed to the concerned nodes at appropriate times. MACAW does this by using the DS and RRTS packets.

Q. 5 Describe DSDV routing protocol.

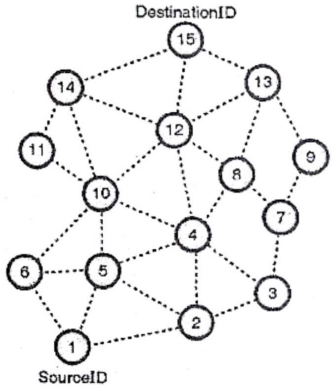
May 18, Dec. 18, May 19, Dec. 19

Ans. :

- DSDV is table driven routing protocol that is first protocol for adhoc wireless networks.
- DSDV is improved version of Bellman Ford algorithm where each node keeps a table, which contains shortest distance and the first node on the shortest path to every other node in the network.

Route establishment in DSDV :

- Fig. 3.2 shows route establishment in DSDV.



(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	162
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

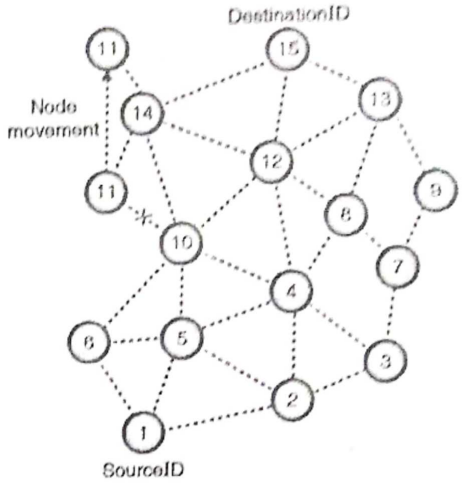
(b) Routing table for node 1

(G-1690) Fig. 3.2 : Route establishment in DSDV

- In Fig. 3.2(a), node 1 is the source node and node 15 is the destination node.
- The route already exists as shown in Fig. 3.10.1(b) because all the nodes maintains global topology information.
- The routing table of source node 1 shows that smallest route to the destination node 15 exists through node 5 and its minimum distance is 4 hops as shown in Fig. 3.2(b).

Route maintenance in DSDV :

- The protocol handles the reconfiguration of path used by on-going data transfer in the following way :
- The last node of broken link begin a table update message with the weight of broken link assigned to ∞ and with a sequence number larger than the registered sequence number for that destination node.
- Once, a node get an update table with weight '∞', each node immediately circulate it to its adjacent nodes to broadcast the broken link data to the entire network.
- Hence, breaking of single link leads to the propagation of table update information to the entire network.
- A node assigns an odd sequence number to the link break update to distinguish it from the even sequence number generated by the destination node.
- Consider the case when node 11 moves from its current location, is as shown in Fig. 3.3(a).
- When an adjacent node observe the link break, it establishes all the paths passing through the broken link with distance as '∞'.



(a)

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	162
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b)

(G-1691) Fig. 3.3 : Route maintenance in DSDV

- For example, when node 10 is aware of the link failure, it sets the path to node 11 as ∞ and transmits its routing table to its neighboring nodes.
- The neighboring nodes finding important changes in their routing tables retransmit it to their neighbors. In this way, broken link information spreads all over the network.
- Node 1 also establish the distance to node 11 as '∞'.

- When node 14 gets a table update message from node 11, it informs the neighbors about shortest distance to node 11. This information is circulated throughout the network.
- After receiving new update message with higher sequence number, all nodes saves the new distance to node 11 in their corresponding tables.
- Fig. 3.3(b) shows updated table at node 1, where the current distance from node 1 to node 11 is increased from 3 to 4 hops.

Q. 6 Write short note on : DSR.

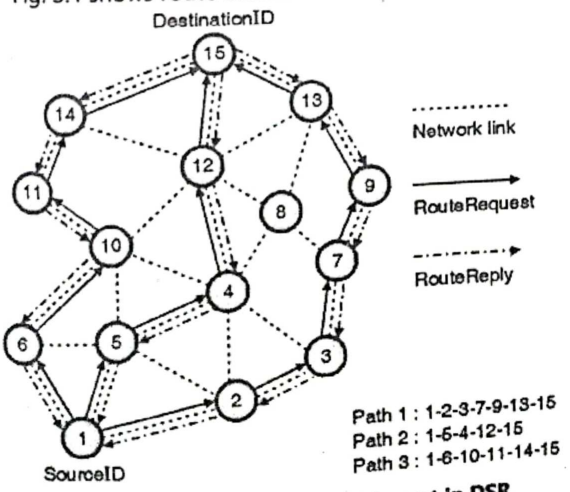
Dec. 14, Dec. 15, May 16, Dec. 19

Ans. :

- Dynamic Source Routing Protocol (DSR) is an on demand routing protocol.
- DSR is designed to control the bandwidth consumed by control packets in adhoc networks by removing the periodic table update messages needed in the table driven method.
- DSR protocol do not need periodic packet transmissions as DSR is beacon-less.
- A node uses periodic beacon packet to inform its presence to the neighboring node.

Route establishment in DSR :

- Fig. 3.4 shows route establishment in DSR.

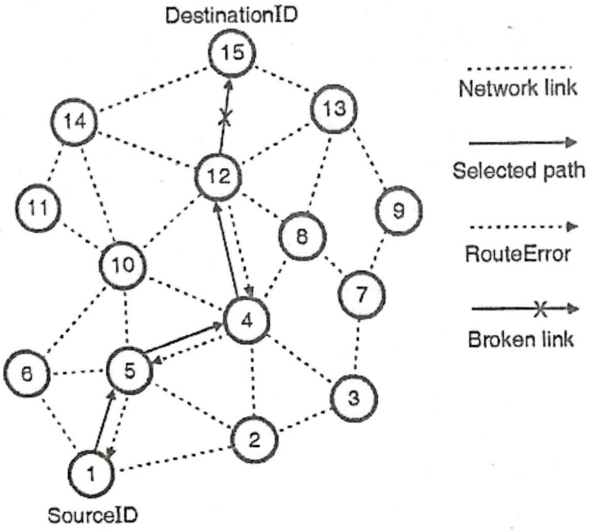


(G-1692) Fig. 3.4 : Route establishment in DSR

- During the route establishment phase, DSR establish a route by flooding RouteRequest packets in the network.
- After receiving RouteRequest packet, destination node responds to the source node by sending a RouteReply packet.
- RouteReply packet carries the route traversed by the received RouteRequest packet.
- Let a source node do not have a route to the destination.
- The sender node initiates RouteRequest packet when it has data packet to be sent to destination.
- This RouteRequest packet is flooded into the entire network.
- After receiving RouteRequest packet, each node retransmits the RouteRequest packet to its neighbors if it has not forwarded already or if the node itself is not destination node provided Time to Live (TTL) counter of packet is not exceeded.
- Each RouteRequest packet carries sequence number generated by the source node and its traversed path.
- Before forwarding RouteRequest packet node checks the sequence number of the packet.
- The packet is forwarded only if it is not duplicate RouteRequest packet.
- The sequence number on the packet is used to avoid loop formations and to prevent more transmission of the similar RouteRequest packets by intermediate node, which receives RouteRequest packet through many routes.
- Hence, all nodes except destination node forward a RouteRequest packet during the route establishment phase.
- A destination node afterreceiving first RouteRequest packet, responds to the source node through the reverse path traversed by RouteRequest packet as shown in Fig. 3.4.
- As shown in Fig. 3.4, to obtain a path for destination node 15, source node 1 initiates RouteRequest packet.
- DSR protocol uses a route cache, which stores all possible data obtained from the source route contained in a data packet.
- Nodes can know about the neighboring nodes routes traversed by data packets if nodes are operated in the promiscuous mode. (The mode in which node can receive the packet which are neither transmits nor addressed to itself).
- This route cache is also useful during the route establishment phase.
- If RouteRequest packet is received by intermediate node, it has route to the destination node in its route cache.
- Then intermediate node respond to the source node by sending RouteReply with all route data from the source to the destination node.

Route maintenance in DSR :

- If the node 10 in Fig. 3.5 has a path to the destination node through node 14, it sends the RouteReply to the source node.



(G-1693) Fig. 3.5 : Route maintenance in DSR

- The source node selects the best and latest route and uses that route for transmitting data packets.
- Each data packet carries the entire path to its destination node.
- When intermediate node is out of path, it causes link break (E.g. link between node 12 and 15).
- The neighboring node of failed link generates the RouteError message to inform the source node.
- The source node restarts the route establishment process.
- After receiving RouteError message, the cached entries at intermediate node and source node are removed.
- If a wireless link fails due to movement of edge node (Node 1 and node 15), the source node again starts the route discovery process.

Q. 7 Write short note on : AODV.

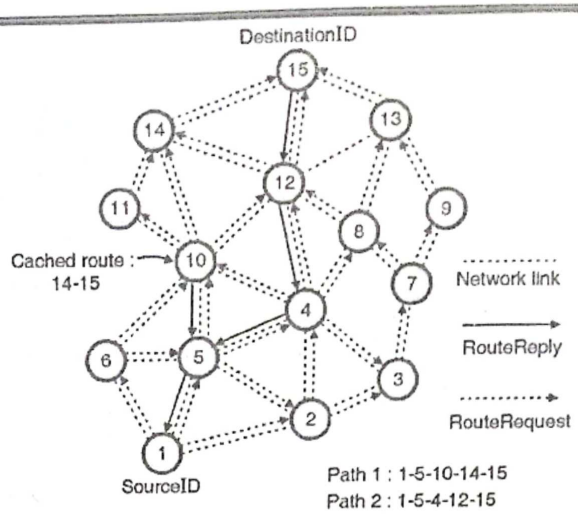
Dec. 15, Dec. 16, Dec. 18, May 19

Ans. :

- AODV routing protocol uses on demand method for discovering routes. i.e. route is created only when it is needed by source node for sending data packets.
- AODV protocol makes use of destination sequence number to identify the latest path.

Route establishment in AODV :

- The route establishment in AODV is as shown in Fig. 3.6.



(G-1688) Fig. 3.6 : Route establishment in AODV

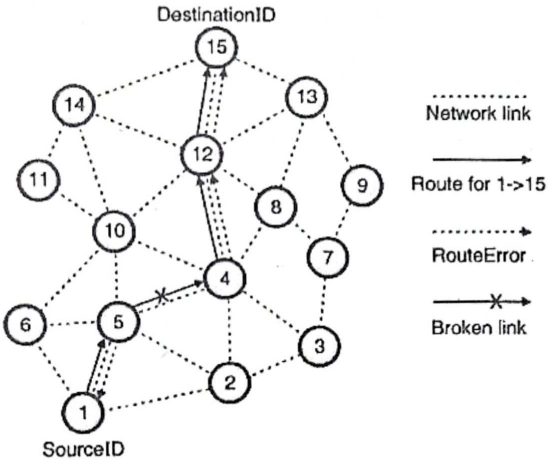
- As shown in Fig. 3.6 source node 1 starts a path discovery process by initiating RouteRequest to the destination node 15 in the network.
- Node 1 assumes that RouteRequest consists of the destination sequence number as 3 and source sequence number as 1.
- When nodes 2, 5 and 6 gets RouteRequest packet, these nodes checks their routes to the destination node.
- If the routes to node 15 do not exist, they further send RouteRequest packet to their neighbouring node.
- As shown in Fig. 3.6 node 3, node 4 and node 10 are the neighbours of node 2, node 5 and node 6 respectively.
- It is assumed that node 3 and node 10 have already existing routes to destination node 15. The route exists as 10-14-15 and 3-7-9-13-15 respectively.
- If the DestSeqNum at node 10 is 4 and at node 3 is 1, then only node 10 is permitted to reply along with the cached route to the source node 1.
- This is because intermediate node 3 has an older route to destination node 15 as compared to the route available at the source node 1.
- The DestSeqNum at node 3 is 1, whereas source node 1 has DestSeqNum 3.
- At the same time node 10 has recent route with DestSeqNum 4 to the destination.
- If the RouteRequest reaches the destination node 15 through the path 4-12-15 or any other alternative route the destination node 15 sends a RouteReply to the source node 1.
- In this case multiple RouteReply packets reach the source node.
- All intermediate nodes after receiving RouteReply packet update their route tables with the latest

DestSeqNum. All intermediate nodes also update the routing information if it leads shortest path between source and destination node.

- AODV does not repair a damaged path locally.

Route maintenance in AODV :

- The end nodes (i.e source and destination nodes) are notified when a wireless link breaks, that is determined by monitoring periodical beacons or through the link level acknowledgements.
- When the source node learns about the path break. then it restarts the route to the destination node if required by the higher layers.
- If path break is found at intermediate node, the intermediate node update the source and destination nodes by sending unsolicited RouteReply with the value of hop count as '∞'. As shown in Fig. 3.7, if the path breaks between the nodes 4 and 5, both the nodes initiate RouteError messages to inform their end nodes about the link break.



(G-1689) Fig. 3.7 : Route maintenance in AODV

- The end node removes the related entries from their tables. The source restarts the path finding process with new broadcast identifier and previous DestSeqNum.

Q. 8 List any six applications of sensor network. **Dec. 14**

Ans. :

- Some of the important applications of WSN are as follows :
  1. WSN is used in an environment network to determine the value of some parameters such as the temperature, atmospheric pressure, amount of sunlight and the relative humidity at a number of locations.
  2. WSN is used in vehicular network to detect the occurrence of events of interest and estimate parameters of the detected event or events. In the traffic sensor network, it detects a vehicle moving through an intersection and calculates approximately the speed and direction of the vehicle.
  3. It detects the type of vehicle in a traffic sensor network whether it is a car, a mini-van, a light truck or a bus.
  4. It is used in a military sensor network to track an enemy tank as it moves through the geographic area covered by the network.
  5. It is used in military applications which includes battlefield surveillance monitoring, guidance in intelligent missiles, nuclear, biological and chemical attack detection, battle damage assessment etc.
  6. It can detect and characterize chemical, biological, radiological, nuclear and explosive (CBRNE) attacks and material used.

Q. 9 Explain different design constraints of WSN. **May 15**

Ans. :

Different design constraints of WSN :

1. Power consumption 2. Communication
3. Computation
4. Uncertainty in measured parameters

1. Power consumption :

- As WSN have limited power supply, designer has to consider energy conservation constraint while designing the protocol.

2. Communication :

- Due to limited bandwidth of WSN, network may be forced to use a noisy channel and communication channel may be forced to transfer data over unprotected frequency band. This affects on quality of service, security and capacity of network.

3. Computation :

- Limited computing power and memory resources of WSN restricts on the types of data processing algorithms that can be used.

4. Uncertainty in measured parameters :

- In a WSN, the detected or collected signals may have an element of uncertainty and may contain noise / interference. Replacement of node may change or damage operation and individual readings.

Q. 10 Which are different task and characteristics of transceiver ? May 15

Ans. :

- Following are the tasks and characteristics of transceiver :

Service to upper layer :

- A receiver has to provide services to MAC – Medium Access Control layer.
- These services are packet oriented, bit interface, byte interface to the microcontroller.
- Transceiver is an interface which allows MAC layer to start frame transmission and to give packet from memory of sensor node to transceiver.
- On the other hand, incoming packets should be streamed into buffers which are accessible by MAC protocol.

Consumption of power and energy efficiency :

- Energy efficiency is energy required to send and receive a single bit.
- In WSN, transceivers should be able to switch between different states such as active and sleeping state.
- The power consumption in each of these states and during switching between them is important.

Carrier frequency and multiple channels :

- Transceivers are available for various carrier frequencies in order to meet the requirements of WSN applications and regulatory restrictions.
- If transceivers give several carrier frequencies to relieve congestion problems in WSN, it is often useful in WSN.

State change times and energy :

- A transceiver may operate in various modes such as sending or receiving mode, they use various frequency bands as "channel" or are in various power safe modes.
- The time and energy needed to change between two states are important figures of merit in many cases.
- The changing time between sending and receiving is important for medium access protocols (MAC).

Data rates :

- The carrier frequency and used bandwidth together with modulation and coding decides the gross data rate.
- Typically data rate is few tens of kbps which is less than data rate in broadband wireless communication but it is sufficient for WSNS.
- We can achieve different data rates by using different modulations or changing the symbol rate.

Modulation :

- Transceivers supports various modulation techniques such as ASK, FSK etc.
- If there are several modulations available, then it is convenient for various experiments.

Transmission power control :

- Some transceivers provide control over the power required to transmit. Some needs external circuit for power control.
- The maximum output power is determined by using regulations.

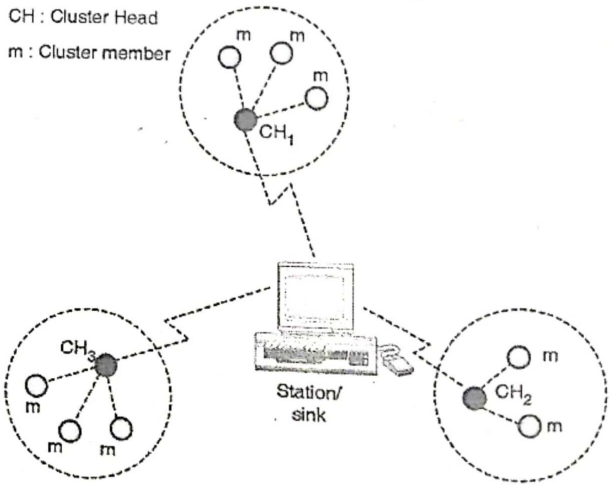
Gain :

- It is the ratio of output signal power to input signal power and is expressed in dB.
- Amplifiers with high gain are used in order to achieve good efficiency.
- Some other characteristics of transceiver are receiver sensitivity, voltage range, frequency stability, coding, noise figure etc.

Q. 11 Write short note on : LEACH. Dec. 15

Ans. :

- LEACH is a clustering based protocol, which reduces dissipation of energy in sensor networks.
- LEACH randomly selects the nodes as cluster heads (CHs) and the high energy dissipation in communicating with the base station (BS) is spread across all nodes in the network. Round is repetition of selection of CHs.
- Fig. 3.8 shows the LEACH architecture.



(G-1654) Fig. 3.8 : Leach architecture

- As shown in Fig. 3.23.1, three clusters CH_1, CH_2 and CH_3 and members m are formed in setup phase of the LEACH.

- Members m communicate with the CHs in steady-state phase. CH collects the data and forwards that data to the base station or sink.

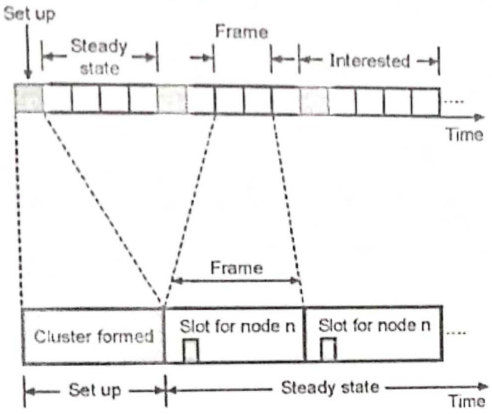
Goals of LEACH :

1. To increase network lifetime.
2. To reduce energy consumption by each sensor node.
3. Use of data aggregation for reducing the number of communication messages.

Q. 12 Explain set up phase and steady state phase of LEACH protocol. Dec. 14

Ans. :

- Fig. 3.9 shows the phases of LEACH.



(G-2425) Fig. 3.9 : Phases of LEACH

- Two phases of LEACH are :
  1. Setup phase. 2. Steady state phase.

1. Set up phase :

- The setup phase includes cluster head selection and cluster formation.
- As compared to steady state, phase duration of the set up is shorter to minimize overhead.
- The setup phase procedure is as follows :
  1. At the start of each round, each node advertises its probability to be the CH, to all other nodes. The probability depends on its current energy level.
  2. Nodes with higher probabilities are selected as the CHs.
  3. Using CSMA MAC protocol, CHs broadcast an advertisement message (ADV).
  4. Each non-CH node determines its CH for this round based on the received signal strength.
  5. By using a CSMA MAC protocol, each non-CH sends a join-request message (Join-REQ) back to its selected CH.
  6. CH node sets up a TDMA schedule, for the data transmission within the cluster,.

2. Steady state phase :

- The steady state phase includes data transmission.
- The time required by steady state phase is longer than the set up phase to minimize overhead.
- The steady state phase procedure for data transmission is as follows :
  1. TDMA schedule is used to send data from node-to CH.
  2. CH combines the data received from node clusters.
  3. Communication takes place through direct-sequence spread spectrum (DSSS). To reduce the inter-cluster interference each cluster uses a unique spreading code.
  4. The data is sent from the CH nodes to the base station by using a fixed spreading code and CSMA.
- The network goes into the setup phase again after a certain period of time spent on the steady-state phase and it enters into another round of CH selection.

Q. 13 What are different design issues of MAC protocol of WSN ? May 15

Ans. :

Design Issues for Medium Access Protocols :

- A MAC protocol for WSN needs to be designed for solving many difficult problems.
- MAC protocols should maximize the throughput and minimize the delay and energy consumption.
- It should handle switched off devices, so that nodes do not have to waste any energy because reducing the energy consumption is the biggest problem.
- The nodes spend much higher energy in an active mode than in sleep mode. However, it is surprising that a node spends more energy while receiving or even simply listening to the channel than while sending.
- This implies that the listening mode time should be minimized.

Q. 14 State different MAC protocol in sensor network ? Dec. 15

Ans. :

Different MAC protocols in sensor network :

1. Self-organizing medium access control for sensor networks (SMACS).
2. Eavesdrop-and-register (EAR) algorithm.
3. Adaptive transmission rate control (ARC).

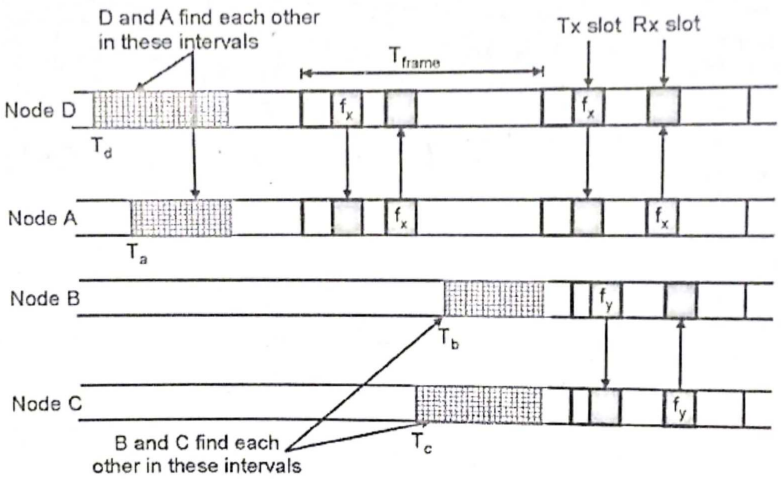
Q. 15 Explain SMACS MAC protocol in sensor network ? Dec. 15

Ans. :

- Self-organizing medium access control for sensor networks (SMACS) is a distributed infrastructure-building protocol.
- It allows nodes to find out their neighbours and set up transmission or reception schedules for communication without the need for any local or global master nodes.
- The neighbor discovery and channel assignment stages are combined in SMACS so that they would have formed a connected network by the time nodes listen all their neighbors.
- A communication link consists of a pair of time slots operating at a randomly selected fixed frequency.
- In sensor networks this is a reasonable option because the available bandwidth is much higher than the maximum data rate for sensor nodes.
- This protocol avoids the requirement of wide synchronization for the network, even though communicating neighbours in a subnet need to be time-synchronized.
- The power conservation is achieved by using a random wake-up schedule during the connection phase and by turning OFF the radio during idle time slots,.

Operation of SMACS :

- Fig. 3.10 shows the basic procedure of SMAC.



Tx : Transmitter, Rx : Receiver

(O-935) Fig. 3.10 : Communication schedule in SMACS

- As shown in Fig. 3.10, nodes A and D wake up at random time T_a and T_d respectively and starts a process to discover nearby devices.
- During the discovery stage, the devices discover each other and negotiate the time slots used and frequencies to be used for the communication between the devices.
- The device will negotiates two time slots which are used to transmit to one direction.
- This means that during the first time slot, node A transmits to node D and during the second time slot node D transmits to node A.
- The different frequency bands are employed to allow multiple devices pairs to use the same time slots for the transmission.
- When new devices afterwards generate a link between themselves, they do not need to take into account the time slots the other pairs are using.
- As shown in Fig. 3.10, nodes B and C can be able to use colliding time slots for communication because they are using different frequency bands.
- If new links are produced, the devices do not know the frequency bands the other links are using.
- Therefore, it is possible for the devices to start using the same frequency band as some nearby device with the time slots.
- There is less probability of collisions where two links are produced with same time slots and same frequencies because it is also required for all the devices to listen to each other before the transmission starts to get corrupted.
- This probability is small as the random frequencies are selected from a large pool of possible frequencies.
- Once the devices have agreed on the used time slot and frequency, the devices start by using these for communication.

- As shown in Fig. 3.10, the transmission occurs every T_{frame} seconds. This is a property of a system and is constant for each node of the network.
- Now, the devices can be turn OFF their transceivers when they do not want to transmit or receive and turn ON for the new round of transmissions.

Q. 16 Explain EAR MAC protocol in sensor network ?

Dec. 15

Ans. :

- EAR is a time slot assignment scheme. The EAR algorithm enables mobile sensors to maintain connectivity to a wireless stationary sensor network while avoiding extensive energy consumption at the stationary nodes.

Principle of operation :

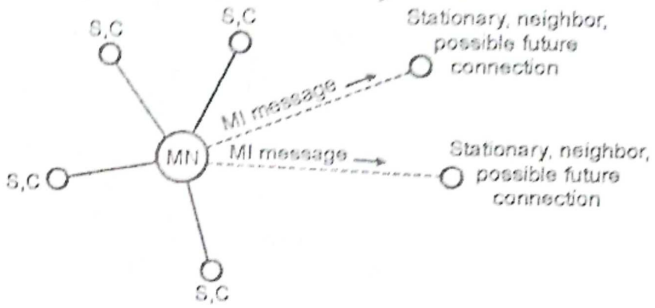
- The EAR protocol operates in the three phases :
  1. Registration phase
  2. Connection phase
  3. Disconnection phase

1. Registration :

- After receiving the BI message, the MN will try to enter the corresponding node's information into its registry simply as a neighbour.
- Continuous registration of multiple stationary nodes will enable the mobile node to decide approximate relative closeness to the various stationary nodes.
- If a BI message received from a stationary node which has already been registered, the MN will update the required information such as signal quality and update the time in the registry.
- Additional updates of received signal quality are provided to the MN to use open-loop power control mechanism for communicating with stationary nodes.

2. Connection :

- The information required to determine the connection selection is included in the registry.
- When a connection is needed, the mobile network will scan the registry for the best possible connection, which is determined by checking a received signal quality threshold.
- The wish to form a connection occurs in one of the following two ways :
  1. In the first case, BI messages received from neighbours can trigger a received signal-to-noise ratio (SNR) to increase above the connection threshold which results in a connection REQ.
  2. In the second case, the mobile node will be allowed to disconnect from the current connection and create a new one, as a received SNR of current connection drops below the disconnect threshold.
- A new connection REQ cannot be made until a current connection fails.
- The connections are formed and the mobile is connected to the maximum allowable number of stationary nodes.
- Fig. 3.11 shows a mobile activity in EAR.



S,C : Stationary, connected

(O-936) Fig. 3.11 : Mobile activity in EAR

- The MN will send an MI message to the stationary node to request a connection.
- The MN along with REQ, will offer the stationary node selection of possible channels for communications (slot pairs and frequencies).
- These slots connected with the stationary node will not be given to another node until the channels drops to possible communication channels.
- The stationary node will decide its wish to participate after receiving the MI message.
- While selecting a subset of communication channels from the provided set, the stationary node registers the MN if a connection is possible and it responds to the MN during the next selected slot with an MR message.
- Here the channels not selected by the stationary node are not committed and can be used to invite other nodes.
- The MR message represents the only particular message introduced to the stationary node by the EAR protocol.
- If a connection is not desired, the stationary node is not required to transmit an MR message and it discards the MI message from the MN.

- The MN will wait for some predetermined time and then drops the possibility of connection.

3. Disconnection :

- Once connection is formed with a stationary node, the mobile node will continue to update the corresponding entry in the registry by receiving data and BI messages.
- Either of two actions will cause a disconnection :
  1. If the received SNR will drop below the disconnect threshold or
  2. If the stationary node will disappear.
- The node disappears if no data or BI message has been received within a preset time limit or because of node failure or deep fades (due to shadowing or multipath interference).
- In such case, the MN will send an MD message to notify the stationary node about the connection failure.
- The EAR protocol tries to provide continuous service to the MNs under both mobile and stationary conditions,.
- The MNs consider full control of the connection process and also determine when to drop connections, by minimizing messaging overhead.
- Full control over connections are assumed by mobile nodes and when they move away they drop connections.
- EAR protocol handles mobility support and it establishes seamless connection of nodes in the mobile and stable conditions.
- As mobility is independently handled by EAR it is transparent to SMACS.
- A disadvantage of EAR protocol is that if members already belongs to different subnets might never get connected.

Q. 17 Explain ARC MAC protocols in sensor network ? **Dec. 15**

Ans. :

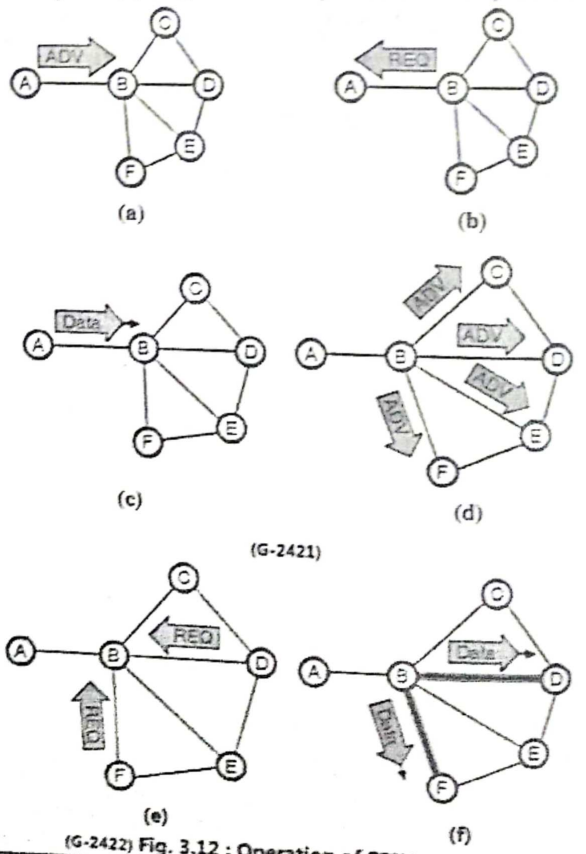
- ARC scheme achieves medium access fairness by making balance of the rates of originating and route-through traffic.
- In ARC protocol, the nodes closer to the access point are not favoured as that of the nodes available deep down into the network.
- The ARC protocol controls the data origination rate of a node which allows the route-through traffic to broadcast. The progressive signaling mechanism is used in ARC which informs the nodes to lower their data originating rate.
- The ARC protocol uses a linear increase and multiplicative decrease approach. Even though, the linear increase results in more aggressive channel competition, the multiplicative decrease controls penalty of transmission failure.
- The associated penalty is less than that for originating data transmission failure as dropping route-through traffic is costly.
- This makes sure that route through traffic is preferred over an originating traffic.
- The computational nature of ARC scheme is more energy-efficient as compared to the handshaking and messaging schemes using the radio.
- The ARC protocol tries to reduce the problem of hidden nodes in a multihop network.
- It reduces the problem by continuously tuning the transmission rate performing phase changes, so that periodic streams are less likely to collide frequently.

Q. 18 Explain the operation of SPIN protocol.

Ans. :

Operation of SPIN Protocol :

- Fig. 3.12(a) to (f) shows the operation of SPIN protocol.



(G-2421)

(G-2422) **Fig. 3.12 : Operation of SPIN protocol**

Step 1 : Sensor node A sends ADV message to its immediate neighbor B to advertise its data which contains the metadata as shown in Fig.3.12(a).

Step 2 : If Node B is interested in the advertised data it sends REQ message as shown in Fig. 3.12(b).

Step 3 : Node A sends data to B as shown in Fig.3.12(c).

Step 4 : The node B sends ADV message to its immediate neighbors i.e. C, D, E and F as shown in Fig.3.12(d).

Step 5 : Only two of these neighbors D and F are interested in the data. They send REQ message to node B as shown in Fig.3.12(e).

Step 6 : Node B sends data to node D and F as shown in Fig.3.12(f).

Q. 19 Compare SPIN, directed diffusion and LEACH.

Ans. :

Comparison of routing protocols :

- Table 3.2 gives comparison of routing protocols.

Table 3.2 : Comparison of routing protocols

Sr. No.	Parameter	Directed diffusion	SPIN	LEACH
1.	Classification	Data centric	Data centric	Hierarchical
2.	Mobility	Limited	Yes	Fixed BS
3.	Scalability	Limited	Limited	Good
4.	Data aggregation	Yes	Yes	Yes
5.	Power usage	Limited	Limited	Maximum
6.	Query based	Yes	Yes	No

Chapter 4 : Introduction to Network Security

Q. 1 State and explain the three security goals.

Ans. :

- The three letters in "CIA triad" stand for confidentiality, integrity and availability. The CIA triad is a widely used information security model.
- The aim of CIA triad model is to guide organizations about efforts and policies for the data security.

1. Confidentiality :

- The meaning of message confidentiality or privacy is that the sender and the receiver expect confidentiality and only the intended receiver should be able to decode the transmitted message correctly.
- To all others, the message must look like garbage.

2. Integrity :

- The meaning of message integrity is that the received data at the receiver must exactly be the same as were sent.
- The transmitted data must not changes during the transmission, neither accidentally nor maliciously.
- The message integrity is important for all the monetary exchanges occurring over the Internet.

3. Availability :

- The information should not be available to any unauthorized person but it should be always available to an authorized entity.

Q. 2 Explain different types of attacks on the message integrity.

Ans. :

- The four types of attacks on integrity are modification, masquerading, replaying and repudiation.

1. Modification :

- In this type of attack, the attacker modifies the intercepted data to make it beneficial to himself.

2. Masquerading :

- Masquerading is also called as spoofing. In this type of attack, the attacker impersonates somebody else. For example, stealing the PIN of a credit card and pretending to be the customer.

3. Replaying :

- In this type of attack, the attacker obtains a copy of the message sent by a user and tries to replay it for his own benefit. This type of attack is often seen in the messages related to the bank transactions.

4. Repudiation :

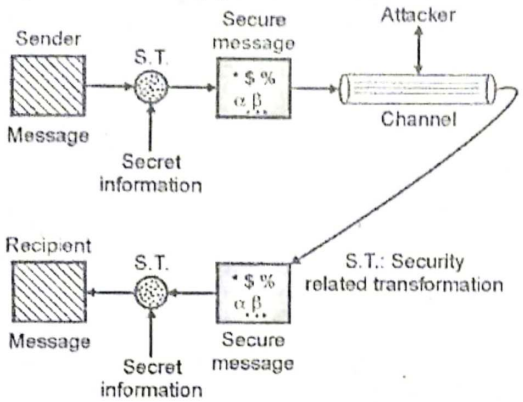
- In this type of attack either the authorized sender or the authorized receiver is involved.
- The sender of a message may later on deny that he has sent that message or the receiver after actually receiving the message, may deny that he has received the message.

Q. 3 With neat block diagram explain Network Security model.

Ans. :

Block diagram :

- Fig. 4.1 shows a very general model of network security.



(G-2862) Fig. 4.1 : Model for Network Security

- One party wants to transfer a message to another across some sort of internet.
- These parties are called as the principals in this transaction.
- Both principals must cooperate to ensure a successful exchange of information.
- A logical information channel is established between the two principals by defining a route through the internet and using communication protocols such as TCP/IP.
- We need to consider the security aspects when it is necessary or desirable to protect the transmitted information from an opponent or attacker who may present a threat to confidentiality, authenticity etc.
- All the techniques that may be used for providing security have the following two components:
  1. As shown in Fig. 4.1, it is necessary to carry out a security-related transformation such as encryption or addition of a code based on the information, on the information to be sent.
  2. Some secret information which is known only to the two principals and, unknown to the opponent such as an encryption key.

Third party :

- We may need a trusted third party (sender, receiver, arbiter, distributer of secret information) to achieve secure transmission.
- A trusted third party may be given tasks like distributing the secret information only to the two principals while keeping it from any opponent.
- We may also need a trusted third party to arbitrate disputes between the two principals related to the authenticity of a message transmission.

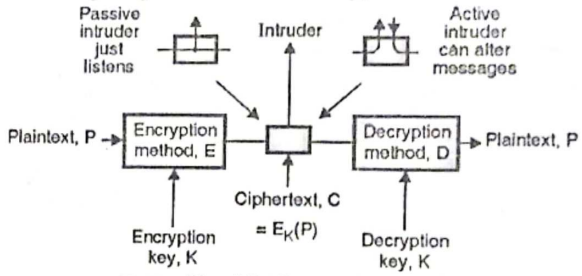
Q. 4 With the help of block diagram explain the following cryptography components :

1. **Plaintext**
2. **Ciphertext**
3. **Decryption**
4. **Ciphers**
5. **Encryption**

Ans. :

Block diagram :

- Cryptography is Greek word which means "secret writing". Fig. 4.2 shows the encryption model.



(G-674) Fig. 4.2 : Encryption model

Plaintext :

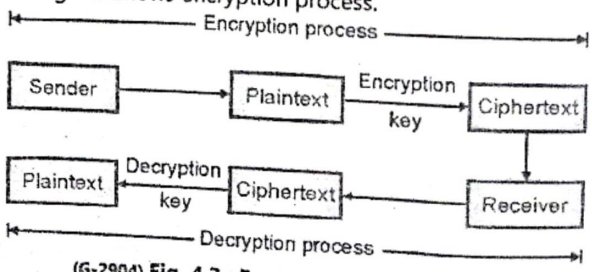
- The original message produced by the sender is called as plaintext. It is data before transmission.

Ciphertext :

- The plaintext is transformed into ciphertext. The encryption program converts the plaintext into ciphertext.

Encryption :

- Encryption is the process of converting the plaintext into ciphertext. The sender uses Key to Encrypt Plaintext to Ciphertext.
- Fig. 4.3 shows encryption process.



(G-2904) Fig. 4.3 : Encryption and Decryption

Decryption :

- Decryption is a process which is exactly opposite to encryption. The decryption algorithm at the receiver transforms the ciphertext back to plain text.
- Receiver uses Key to Decrypt Ciphertext to Plaintext
- Fig. 4.3 shows decryption process.

Ciphers :

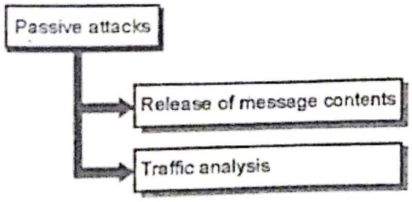
- The encryption and decryption algorithms together are referred to as ciphers. This term is also used to refer to different categories of algorithms in cryptography.
- It is not necessary to have a separate cipher for each sender or receiver pair. Instead it is possible to use public ciphers with secret keys for millions of pair of sender and receiver.

Q. 5 State and explain passive attacks.

Ans. :

Definition :

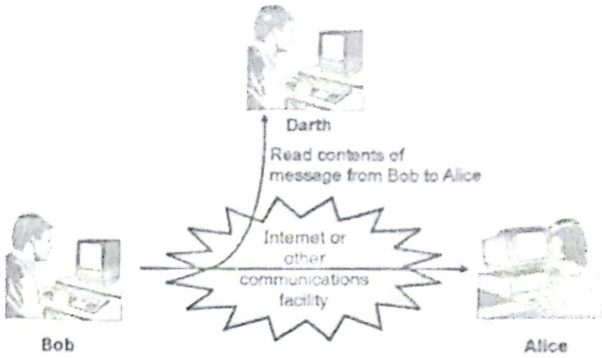
- Passive attack is defined as the type of security attack where, the attacker makes attempt to collect information from the system but does not modify or alter the system data or resources.
- Examples of passive attacks are eavesdropping (extracting information) or monitoring of network traffic. The goal of attacker is to gain the information that is being transmitted.
- This is the easiest form of attack and can be performed without difficulty.
- The two types of passive attacks are shown in Fig 4.4.
  1. Release of message contents 2. Traffic analysis



(G-2859) **Fig 4.4 : Types of Passive attacks**

1. Release of message contents :

- We may want to prevent the attacker from learning sensitive and confidential information through transmissions that take place through telephone calls or email messages or files transferred on network.
- When we send a confidential email to our friend, we want only him to access this mail. However, if this mail is accessed by unauthorized users then contents of message are released to somewhere else.
- This type of attack is called release of message contents, which is shown in Fig. 4.5.

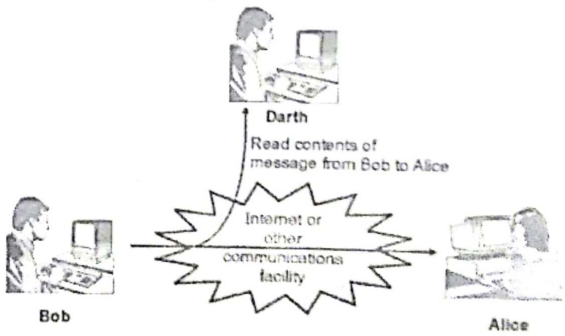


(G-2854) **Fig. 4.5 : Release of message contents**

- There are different security mechanisms available to prevent such type of attacks.

2. Traffic analysis :

- Low imagine that we mask the contents of the message using encryption. Now the attacker can capture the contents of the message but cannot extract any information from it
- Then he might observe a pattern of messages, to get some information like the location, or any clue regarding the origin of message.
- This type of passive attack is known as traffic analysis and is shown in Fig. 4.6.



(G-2854) **Fig. 4.6 : Traffic analysis**

- The message is sent and received in normal manner and neither sender nor receiver is aware that someone else has read message or observed pattern of messages. We can prevent such attacks by means of encryption.
- While dealing with the passive attacks the emphasis is on prevention rather than detection.

Q. 6 Write a short note on : Unauthorized Access.

Ans. :

Definition :

- When a person enters into a computer network, system, application software, data, or other resources without permission, that access is an unauthorized access.

- An access to an information system that violates the owner or operator's stated security policy is considered as unauthorized access.
- When legitimate users access a resource that they do not have permission to use is also considered as an unauthorized access. Unauthorized access occurs if a user tries to access an area of a system they should not be accessing.
- While attempting to access that area, they would be denied access and possibly see an unauthorized access message.
- Some administrators set up alerts to let them know the attempt of an unauthorized access attempt, so that they can investigate the reason.
- These set up alerts can help to stop hackers from gaining access to a secure or confidential system.
- Many secure systems can also lock an account with too many failed login attempts.
- The common reasons for unauthorized access are :
  1. To Steal sensitive information
  2. To cause damage to system or data
  3. To hold data hostage as part of a ransomware attack
  4. To play a prank
- The three main objectives of preventing unauthorized access are : Confidentiality, Integrity andAvailability.

Q. 7 Explain DDos.

Ans. :

Definition :

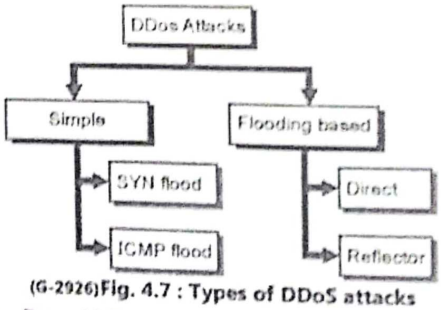
- A distributed denial-of-service (DDoS) attack is a malicious attempt to disturb the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- The goal of DDos attacks is to target websites and online services and to render the website or service inoperable.
- These attacks make computer systems inaccessible by flooding networks, servers or end user systems with useless traffic so that legitimate users can no longer gain access to those resources.
- In this type of attack, useless traffic is flooded in the networks, servers or end user systems making computer systems inaccessible. Due to flooding of useless traffic, legitimate users can no longer gain access to those resources.
- In a typical DDoS attack, a large number of compromised hosts collectively send useless packets in the networks or systems.
- A denial of service (DoS) attack comes from a single host or network node and it attempt to prevent legitimate users of a service from using that service.
- DDoS attacks are more serious threat as DDos achieves effectiveness by using multiple compromised computer systems as sources of attack traffic.
- In a DDoS attack, an attacker launch an attack on the target by recruiting a number of hosts throughout the Internet to simultaneously or in a coordinated fashion.
- A DDoS attack tries to consume the resources of target so that it cannot provide service.
- Typical targets for DDoS attacks are :
  1. Routers
  2. Firewalls and defence systems
  3. Links
  4. Infrastructure of Victim
  5. Operating system of Victim
  6. Current Communications and applications of victim
  7. Internet shopping sites
  8. Online casinos
  9. Any business or organisation that depends on providing online services

Q. 8 Classify DDos attacks. Explain any one.

Ans. :

Types of DDoS attacks :

- Fig. 4.7 shows the types of DDoS attacks.



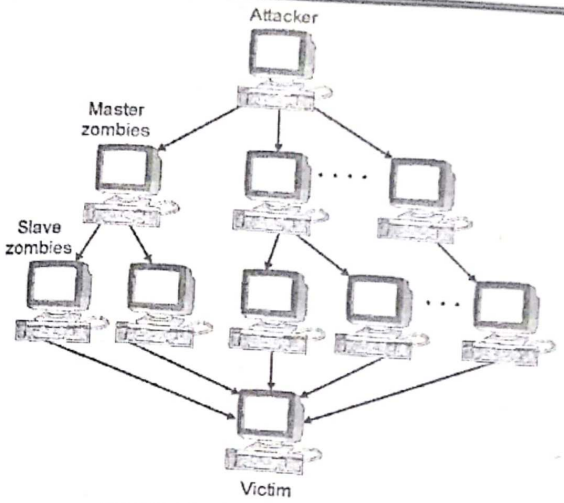
(G-2926)Fig. 4.7 : Types of DDoS attacks

Flooding-Based DDoS Attacks :

- Flooding-Based DDoS Attacks are classified into :
  1. Direct DDoS attack
  2. Reflector DDoS attack

1. Direct DDoS attack :

- The zombies perform attacks by given order from control and command server.
- Fig. 4.8 shows a direct DDoS attack.
- As shown in Fig. 4.8, the attacker inserts a zombie software on a number of sites distributed throughout the Internet.

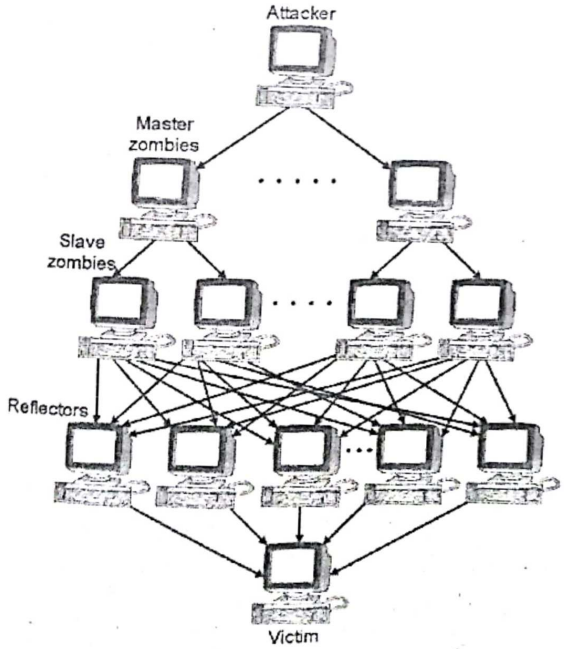


(G-2929) **Fig. 4.8 : Direct DDos attack**

- The DDoS attack involves master zombies and slave zombies.
- The hosts of both master zombies and slave zombies will get infected with malicious code.
- The attacker coordinates and triggers the master zombies. Then the master zombies coordinate and trigger the slave zombies.
- The use of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers.

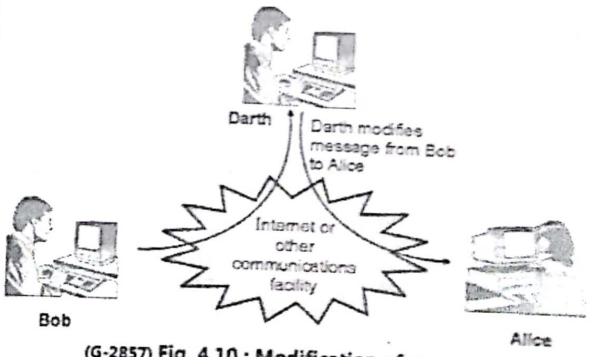
2. Reflector DDoS attack :

- Fig. 4.9 shows a reflector DDoS attack.



(G-2930) **Fig. 4.9 : Reflector DDos attack**

- A reflector DDoS attack adds another layer of machines (Reflectors) in a direct DDos attack.
- The slave zombies in this type of attack constructs packets requiring a response that contain the IP address of target as the source IP address in the packet's IP header.
- These packets are sent to uninfected machines called as reflectors.
- The reflector machines gives response with packets directed at the target machine.
- A reflector DDoS attack involves more machines and traffic as compared to a direct DDoS attack which results in more damaging.
- As the attack comes from widely scattered uninfected machines, tracing back the attack or filtering out the attack packets is more difficult.
- Q. Write a short note on : Man-in-the-middle Attack.
- This attack allows an attacker to intercepts the communication between the client and server.
- Due to this, an attacker can read, insert and modify the data in the intercepted connection.
- In modification, the original data sent by the authentic user is disrupted or modified by the attacker to make it non meaningful for the receiver.
- Usually the content sequence in the message is changed. Thus in modification of message as shown in Fig. 4.10, the attacker modifies the contents of message after sender sends it but before it reaches to indented recipients.



(G-2857) **Fig. 4.10 : Modification of messages**

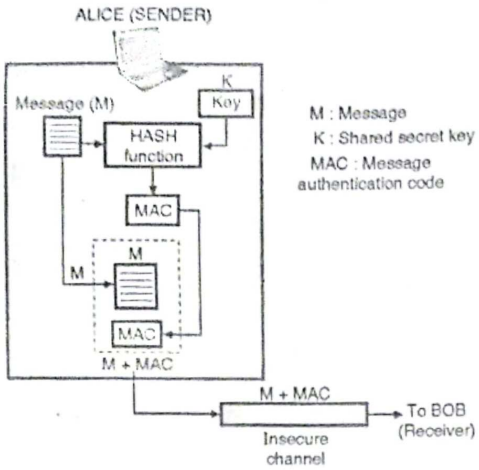
Q. 9 Write a short note on : Message Authentication.

Ans. :

- We know how does the message digest can be used to protect the integrity of the message. The second important aspect to be considered is to ensure the authentication of the data origin.
- That means to ensure that the sender himself is the originator of the message and someone else is not pretending to be the originator of the message.

At the sender :

- This can be ensured by creating a Message Authentication Code (MAC). Fig. 4.10(a) shows the generation of MAC at the sender (Alice) site.

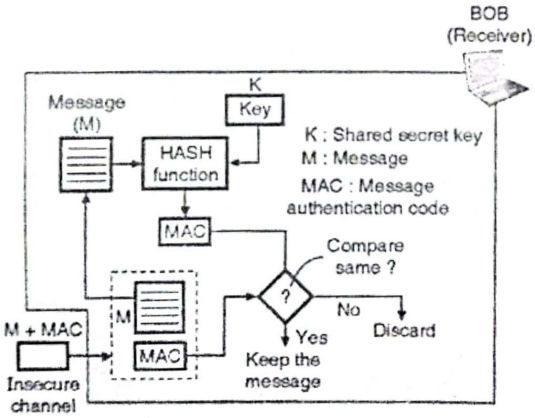


(G-2346) Fig. 4.10(a) : Generation of Message Authentication Code (MAC)

- The message (M) is applied to the hash function algorithm along with a shared secret key (K) to produce MAC.
- ALICE then sends the message and the MAC (M + MAC) over an unsecure channel to BOB (receiver).

At the receiver :

- Fig. 4.10(b) shows process taking place at the receiver (BOB) for keeping only the authentic message and discard all the other.



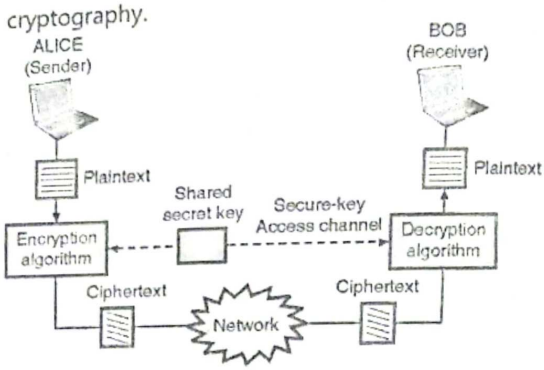
(G-2347) Fig. 4.10(b) : Process of keeping only the authentic message at the receiver

- At the receiver (Bob), the message (M) plus MAC (M + MAC) is received over the unsecure channel from Alice.
- The message (M) and MAC are then separated from each other. The hash function algorithm uses this message (M) alongwith the shared secret key (K) to create a new MAC.
- This new MAC and the received MAC are compared with each other. If they are same then the message (M) is kept because it is authentic, otherwise it is discarded.

Q. 10 With the help of block diagram, explain the symmetric key cryptography.

Ans. :

- It is also called as the secret key cryptography.
- Fig. 4.11 shows the block schematic of symmetric key cryptography.



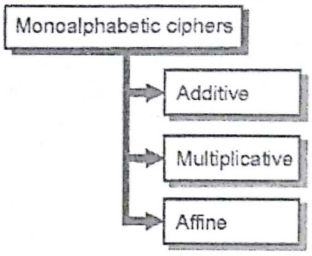
(G-2339) Fig. 4.11 : Symmetric key cryptography

- In the symmetrical key cryptography, the same key (shared secret key) is used by the sender and receiver.
- The same secret key is used at the sending end as well as at the receiving end as shown in Fig. 4.11.
- The sender uses this key along with the encryption algorithm to encrypt the data, and the receiver uses it along with the decryption algorithm to decrypt the data.
- The encryption algorithm makes use of a combination of addition and multiplication to encrypt the data whereas the decryption algorithm uses a combination of subtraction and division in order to carry out the decryption.
- The encryption and decryption algorithms are thus inverse of each other.
- Thus Encryption is equivalent to locking the message in a box while Decryption is equivalent to unlocking the box.
- In the symmetric key ciphers, the same key (Shared key) is used for locking as well as unlocking.

Q. 11 List the types of monoalphabetic ciphers. Explain any one.

Ans. :

- The different techniques based on monoalphabetic ciphers are as shown in Fig. 4.12.



(G-2931)Fig. 4.12 : Types of Monoalphabetic Ciphers

Additive (Shift / Caesar) Cipher :

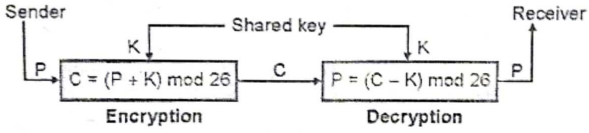
- Additive Cipher is the simplest monoalphabetic cipher. It is also referred as a shift cipher or a Caesar cipher.
- Assume that the plaintext and ciphertext consists of lowercase letters (a to z) and uppercase letters (A to Z) respectively.
- Assign numerical values to each letter (lower or uppercase) in order apply mathematical operations on the plaintext and ciphertext, this is shown in Fig. 4.13.
- Each character (lowercase or uppercase) in Fig. 4.13 is assigned an integer in Z_{26}.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(G-2932)Fig. 4.13 : Plaintext and ciphertext characters in Z_{26}

Encryption and Decryption :

- Fig. 4.14 shows the process of encryption and decryption in Additive cipher.



(G-2934)Fig. 4.14 : Additive cipher

- In the encryption algorithm the key (K) is added to the plaintext character (P), in the decryption algorithm the key (K) is subtracted from the ciphertext character(C). This is illustrated in Fig. 4.14.
- The formulae for encryption and decryption is :
- C = (P + K) mod 26 and P = (C – K) mod 26
- If the cipher is additive, the plaintext, ciphertext, and secret key are integers in Z_{26}.

Why the name shift cipher ?

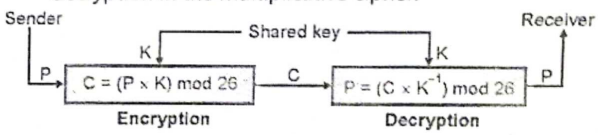
- The encryption algorithm is "shift key characters down" and the decryption algorithm is "shift key character up".
- For example, if the key is 5. the encryption algorithm shifts 5 characters down towards the end of the alphabet and the decryption algorithm shifts 5 characters up towards the beginning of the alphabet.
- We wrap around, when we reach the end or the beginning of the alphabet.
- Due to this reason, the additive ciphers are known as shift ciphers.

Q. 12 Explain multiplicative cipher with example.

Ans. :

Encryption and Decryption :

- Fig. 4.15 shows the process of encryption and decryption in the multiplicative cipher.



(G-2935)Fig. 4.15 : Multiplicative cipher

- In the encryption algorithm the plaintext is multiplied by the key(K) whereas in the decryption algorithm the ciphertext is divided by key (K). This is illustrated in Fig. 4.15.
- The result to be mapped to Z_{26} since the operations are in Z_{26}.
- The division by key during the decryption means the multiplication by the multiplicative inverse of the key in Z_{26} (i.e, K^{-1}).
- The following are formulae used to encrypt the plaintext (P) and decrypt the ciphertext (C) respectively.

$$C = (P \times K) \bmod 26$$
$$\text{and } P = (C \times K^{-1}) \bmod 26$$

- In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26} and the key needs to be integer in inverse of Z_{26}.
- The possible multiplicative inverses of Z_{26} are : 1, 3, 5, 7, 9, 11,15, 17, 19, 21, 23 and 25.
- Table 4.1 gives the inverses of 12 key values.

(G-2933) Table 4.1

K	1	3	5	7	9	11	15	17	19	21	23	25
K^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

How to find multiplicative inverse for decryption ?

- If we have the key 'a' then to find the multiplicative inverse (b) of a mod c, calculate the a × b mod c from 0 to c – 1 till a × b mod c becomes 1.

E.g. If a =5, c = 26

5 × 0 mod 26 =0 mod 26

5 × 1 mod 26 =5 mod 26

5 × 5 mod 26 =25 mod 26

:

5 × 21 mod 26 =1 mod 26 .....(Inverse found)

- ∴ The multiplicative inverse of 5 in Z_{26} is 21.

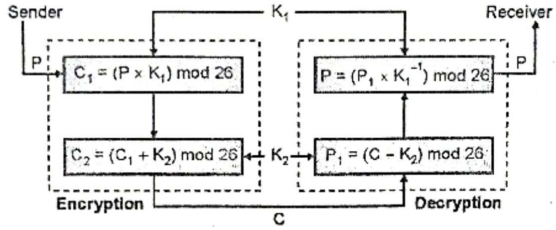
Q. 13 Explain affine cipher with example.

Ans. :

- An Affine Cipher is a combination of the additive and multiplicative ciphers.
- It uses a combination of both ciphers with a pair of keys K_1 and K_2.
- The first key K_1 is used for the multiplication and the second key K_1 is used for the addition.

Encryption and decryption :

- Fig. 4.16 shows the process of encryption and decryption in an affine cipher.



(G-2936)**Fig. 4.16 : Affine cipher**

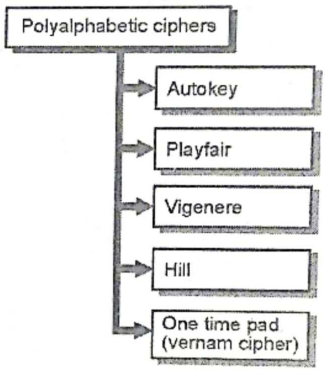
- In the encryption algorithm, the plaintext s(P) is first encrypted using the multiplicative cipher and key K_1, it results in the temporary ciphertext $(C_1) = (P * K_1)$ mod 26.
- The temporary ciphertext C_1 is again encrypted by using the additive cipher and key K_2 to obtain the final ciphertext $(C) = (C_1 + K_2)$ mod 26.
- In the decryption algorithm, it first decrypts the received ciphertext (C) using the additive cipher and additive inverse of the key K_2 in Z_{26} $(-K_2)$ to obtain a temporary plaintext $(P_1) = (C - K_2)$ mod 26.
- The temporary plaintext P_1 is again decrypted using the multiplicative cipher and multiplicative inverse of the key K_1 in Z_{26} (K_1^{-1}) to obtain the original plaintext $(P) = (P_1 \times K_1^{-1})$ mod 26.
- Note that, if the second cipher is the additive cipher in encryption, then the subtraction should be the first cipher in decryption. Similarly, if the second cipher is the multiplicative cipher in encryption, then the multiplicative inverse should be the first cipher in decryption.
- The relationship between Plaintext and ciphertext is as follows :

$$C = (P \times K_1 + K_2) \bmod 26$$
$$P = [(C - K_2) \times K_1^{-1}] \bmod 26.$$

Q. 14 List the types of polyalphabetic ciphers. Explain any one.

Ans. :

- The different techniques based on Polyalphabetic ciphers are as shown in Fig. 4.17.



(G-2937) **Fig. 4.17 : Types of Monoalphabetic Ciphers**

Autokey Cipher :

- In this type of cipher, the key used is a group of subkeys ($K1_1$, K2, K3,..., K_n). Here each subkey is used to encrypt the corresponding character in the plaintext.
- That means, the first subkey is used to encrypt the first plaintext character, the second subkey is used to encrypt the second plaintext character and so on.
- The cipher is named as Autokey cipher because the subkeys are generated automatically during the process of encryption. The first subkey is predetermined value, its value is selected by the sender and the receiver.
- The second subkey is the value of the first plaintext character (between 0 and 25), the third subkey is the value of the second plaintext character and so on.

Encryption :

- During the encryption process, a plaintext character (P_i) is added with the respective subkey (K_i) and the result is mapped to Z_{26}, using modular arithmetic in order to obtain the corresponding ciphertext character(C_i).

$$C_i = (P_i + K_i) \bmod 26$$

Decryption :

- During the decryption process, a ciphertext character (C_i) is added with the additive inverse of the respective subkey ($-K_i$) to obtain the corresponding plaintext character (P_i).

$$P_i = (C_i - K_i) \bmod 26$$

Steps involved in Autokey Cipher :

1. Replace each character in the given plaintext by its integer value.
2. The first subkey is added to generate the first ciphertext character.
3. The rest of the keys are generated as the plaintext characters are used.

Q. 15 Explain playfair cipher with example.

Ans. :

- The playfair cipher is also known as Playfair square.
- The secret key in playfair cipher is made of 25 alphabets organized into a 5 × 5 matrix.
- While encrypting, the letters I and J are considered as 5 × 5 matrix and inserted in the same cell in the matrix.
- Different secret keys can be obtained from different possible arrangements of alphabets in the matrix.
- The first step in the playfair encryption technique is to create and fill the matrix. Initially, a keyword is selected by the sender and receiver that may not necessarily contain all the 25 alphabets.

Secret key :

- To organize this keyword in the matrix, enter the letters row wise(i.e. from the top left position to right, and from top to bottom). Each letter of the keyword is entered only once, the duplicate letters in the keyword are dropped.
- In the remaining empty positions of the keyword matrix, the alphabets (in order) that are not included in the keyword are filled. This is shown
- While filling the empty positions of the matrix, if either I or J appears in the keyword, both are ignored. If neither I nor J appears in the keyword, both are placed at the same position in the matrix.
- This arrangement of 25 alphabets in the matrix becomes the secret key for encryption and decryption. This is as shown in Fig. 4.18 for the word "MONARCHY".

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

(G-2939)Fig. 4.18 : Secret key matrix

Encryption and Decryption :

- The next step is the encryption of the plaintext.
- Before encryption, the plaintext message is broken into group of two characters.
- If both characters in a pair are the same, then insert a bogus letter (X) between them to distinguish.
- In case the plaintext consists of an odd number of characters, then also a bogus character is inserted at the end of the plaintext in order to make the number of characters even.
- Consider the example : GREETING.
- In this plaintext, we have four groups of two letters each as GR, EE, TI and NG.
- In this example, the second pair of the message contains repeated letter E, the bogus letter X is inserted between two E's.
- Now, the pairs of the message become GR, EX, ET, IN and G.
- Now, to make the number of characters even, the bogus character X is inserted at the end, making the last pair as GX.

Rules :

Encryption :

- The playfair cipher uses the following rules :
  1. If the two letters in a pair are located in the same row of the keyword matrix, they must be replaced with the letters at their immediate right positions. If the any of the letters appears at the end of the row, we should wrap around to the beginning of the row.
  2. If the two letters in a pair appear in the same column of the keyword matrix, they must be replaced with the letters at their immediate below positions. If any of the letters is the last letter in the column, we should wrap around to the beginning of the column.
  3. If the two letters in a pair do not appear in the same row or column of the keyword matrix, each of them must be replaced with the letter placed at the intersecting position of its own row and the column of another.

Decryption :

- The ciphertext is decrypted using the same rules as for encryption, with some differences.
- If the two letters of a pair in the ciphertext satisfy the condition of rule 1, they are replaced with the letters at their immediate left positions.

- If the two letters of a pair in the ciphertext satisfy the condition of rule 2, they are replaced with the letters at their immediate above positions.
- The rule 3 is same for decryption.
- The bogus letters are also removed during decryption.

Q. 16 Explain Hill cipher with example.

Ans. :

- The plaintext in the Hill cipher is first divided into equal-size blocks.
- Then, the blocks are encrypted in such a way that each block element (character) participates in the encryption of other block elements in the block.
- In a Hill cipher, the blocks are encrypted one at a time.
- In this type of cipher, the key (K) is used in the form of a square matrix of size n × n.
- Where n is the block size. Each element of the key matrix is represented as Kij as shown in Fig. 4.19. Where $1 \le i, j \le n$.

$$K = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1n} \\ K_{21} & K_{22} & \cdots & K_{2n} \\ \vdots & \vdots & & \\ K_{n1} & K_{n2} & \cdots & K_{nn} \end{bmatrix}$$

(G-2944)Fig. 4.19 : Key matrix in the Hill cipher

$$\begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1n} \\ K_{21} & K_{22} & \cdots & K_{2n} \\ \vdots & \vdots & & \\ K_{n1} & K_{n2} & \cdots & K_{nn} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{bmatrix} \quad \text{(G-2945)}$$

- Consider a plaintext block (P) contains n characters to be encrypted.
- Let $P_1, P_2, \ldots, P_n$ are the plaintext characters in this block and their corresponding ciphertext characters are $C_1, C_2, \ldots, C_n$.
- Then, we get the ciphertext as :

$$C_1 = (P_1K_{11} + P_2K_{21} + \ldots + P_nK_n) \bmod 26$$
$$C_2 = (P_1K_{12} + P2K_{22} + \ldots + P_nK_{n2}) \bmod 26$$
$$\vdots$$
$$Cn = (P_1K_{1n} + P_2K_{2n} + \ldots + P_nK_{nn}) \bmod 26$$

- The above equations can be expressed as :
- The encryption in the Hill cipher can be expressed as C = K P mod 26
- To perform the decryption , the inverse of the key is determined in Z_{26}, and then the ciphertext is decrypted as $P = K^{-1} C \bmod 26$.

Q. 17 Differentiate between monoalphabetic and polyalphabetic ciphers.

Ans. :

Table 4.2 : Comparison of Monoalphabetic and Polyalphabetic Cipher

Sr. No.	Parameter	Monoalphabetic	Polyalphabetic
1.	Number of characters used at a time	One	More than one
2.	Relation Between Characters in P and C	One to one	One to many
3.	Types	additive, multiplicative, affine	Autokey, Playfair, One time pad, Hill, Vigenere.
4.	Key dependancy	The value of k_i does not depend on the position of the plaintext character	The value of k_i depends on the position of the plaintext character
5.	Strength	Low	Medium
6.	Complexity	Low	Medium
7.	Time required for encryption / decryption	Less	More

Q. 18 Explain Rail-Fence Technique.

Ans. :

- The Rail fence technique is also called as Zigzag or Keyless transposition .
- An example of transposition cipher is Rail Fence technique.
- It uses simple algorithm, the steps involved in the Rail Fence technique are as follows :
  1. Write the plaintext message as a sequence of diagonals.
  2. Read the plaintext message written in step 1 row wise.

Example of Rail Fence technique :

- Consider the plaintext message "This is a secret message".

- **Plaintext :** This is a secret message
- To encode this message first write over two lines (the "rails of the fence") as follows :

T		i		i		a		e		r		t		e		s		g	
	h		s		s		s		c		e		m		s		a		e

(G-2925)

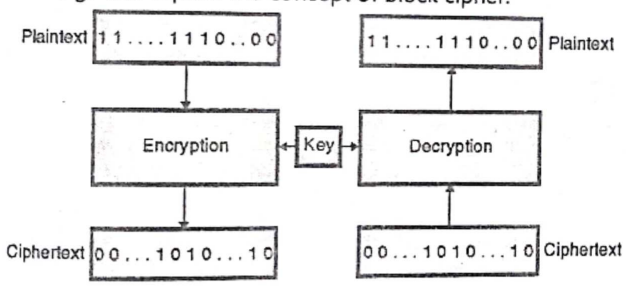
- Now read the text row by row and write it sequentially.

Ciphertext : Tiiaertesghssscemsae

Q. 19 Explain the block ciphers.

Ans. :

- The traditional ciphers encrypt and decrypt every single character or symbol in the plaintext. But the modern ciphers use a block of bits as the unit of encryption or decryption.
- That means both the plaintext and the ciphertext are blocks of bits. The blocks of symbols or characters and encrypted into another completely different block of symbols or characters.
- Fig. 4.20 explain the concept of block cipher.

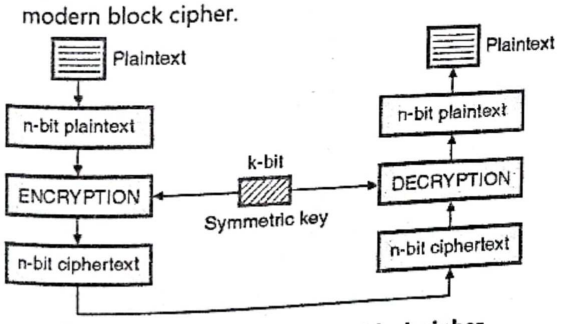


(G-678) **Fig. 4.20 : Block cipher**

Q. 20 With the help of neat block diagram, explain the principle of operation of modern block cipher.

Ans. :

- Fig. 4.21 shows the simplified block schematic of a modern block cipher.



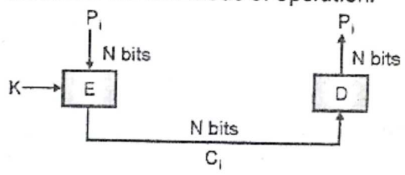
(G-2340) **Fig. 4.21 : A modern block cipher**

- It is a symmetric key modern block cipher. The plaintext is converted into blocks of n-bits.
- Each such n-bit plaintext is encrypted into an n-bit ciphertext with the help of a k-bit key.
- A common (symmetric) k-bit key is used by both encryptor and decryptor as shown.
- The decryption algorithm is exactly the inverse of the encryption algorithm and uses the same symmetric key to obtain the original n-bit plaintext.
- In the event of the message having less than n-bits, padding must be done to make an n bit block.
- For a plaintext message with more than n-bits, it should be divided into multiple n-bit blocks.
- For modern block ciphers the typical values of n are 64, 128, 256 and 512 bits.
- Modern block ciphers are **substitution ciphers** when seen as a single block.
- But the modern ciphers are not designed as one whole block.
- Instead it is a combination of multiple transposition units (also called as P-boxes), substitution units (also called as S-boxes), EX-OR operations as well as swapping elements, switching elements and combining elements.

Q. 21 Write a short note on : Electronic Code Book (ECB) mode.

Ans. :

- This mode is a purely block cipher technique.
- Fig. 4.22 shows the ECB mode of operation.



(G-2917) **Fig. 4.22 : ECB Mode**

- Where,
- E : Encryption algorithm, D : Decryption algorithm
- K : Secret key, Pi : Plaintext block i,
- Ci : Ciphertext block i
- Encryption : $C_i = E_K(P_i)$, Decryption : $P_i = D_K(C_i)$
- The plaintext in ECB mode is divided into blocks of N bits.
- The secret key is used to encrypt the plaintext block to form a ciphertext block.
- Two identical plaintext blocks, then, will always generate the same ciphertext block.
- Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.

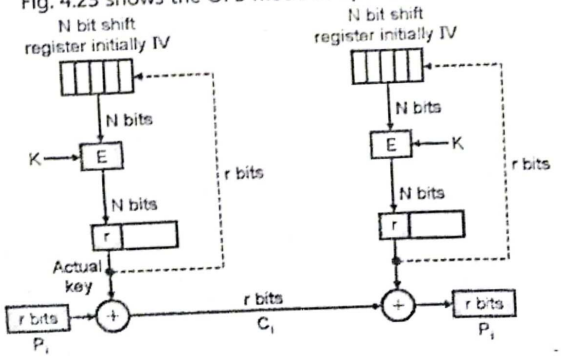
Characteristics of ECB mode :

1. The blocks in the plaintext and the ciphertext become equal because the key and the encryption/decryption algorithm used are the same. For example, if plaintext blocks 1, 3, and 7 are the same then the ciphertext blocks 1, 3, and 7 will be the same. This become a security problem as the rival can guess that the plaintext blocks are the same if the corresponding ciphertext blocks are the same.
2. With reordering of the plaintext block, the ciphertext block is also reordered.
3. Blocks are independent on each other and is encrypted or decrypted independently. If a problem occurs in encryption or decryption of a block, it does not affect other blocks.
4. An error in one block is not circulated to other blocks. The corruption of one or more bits during transmission only affects the bits in the corresponding plaintext after decryption.

Q. 22 Write a short note on : Output Feedback (OFB) mode.

Ans. :

- Fig. 4.23 shows the OFB mode of operation.



(G-2920)Fig. 4.23 : OFB Mode

- Where,
- E : Encryption algorithm,
- K : Secret key, P_i : Plaintext block i,
- C_i : Ciphertext block i, IV : Initialization vector
- The OFB and CFB mode are very similar with only one difference.
- Each bit in the ciphertext is independent of the preceding bit, which avoids error propagation.
- If an error occurs during transmission, it does not affect the future bits.
- In OFB mode, the sender and the receiver use the encryption algorithm.
- The OFB mode makes use of the block ciphers such as DES or AES to create the key stream.
- The feedback for generation of the next bit stream comes from the previous bits of the key stream instead of the ciphertext.
- The ciphertext does not take part in generation of the key stream.

Characteristics of the OFB mode :

1. The ciphertext will be different with the change in IV from one encryption to another using the same plaintext.
2. The ciphertext depends on plaintext.
3. The errors occurring in one or more bits of the ciphertext block will not affect the future ciphertext blocks.

Q. 23 Compare various block cipher modes.

Ans. :

Table 4.3 : Comparison of block cipher modes

Sr. No.	Parameter	ECB	CBC	CFB	OFB
1.	Type of cipher	Block	Block	Stream	Stream
2.	Initialization Vector	No	Yes	Yes	Yes
3.	Security	Less	High	High	High
4.	Decryption	Yes	Yes	No	No
5.	Complexity	Low	High	High	High
6.	Implementation cost	Low	High	High	High
7.	Parallelism	Yes	No	No	No

Chapter 5 : Cryptographic Algorithm

Q. 1 Define Algebraic Structures. Briefly define a group, ring and a field.

Ans. :

Definition :

- The combination of a set of integers and the operations that are defined on the elements of the set is called as an algebraic structure.

Groups :

- A Group (G) is a set of elements along with a binary operation " • " performed on each ordered pair (x, y) of elements of G such that x • y satisfies four properties Closure, Associativity, Existence of identity and Existence of inverse.
- A group (G) is denoted as G = <{...}, • >.

Properties of Groups :

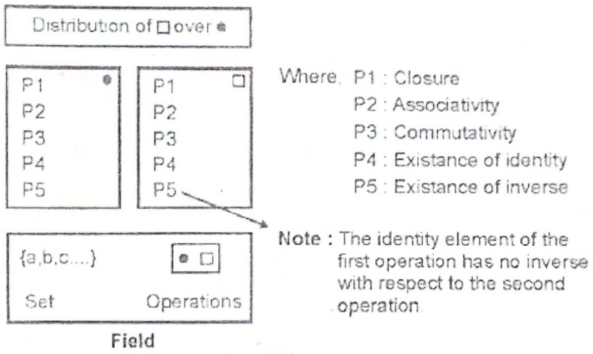
- The following are the four properties of Groups :
  1. Closure
  2. Associativity
  3. Existence of identity
  4. Existence of inverse

Rings :

- A ring is a set of elements with two binary operations, " · " and " □ ".
- A ring R is denoted by R = < {. . . }, ·, □ >.
- Note that □ can be an operator such that . (product) or + (addition) etc.
- The first operation should satisfy all properties required for an Abelian group.
- In other words, "·" should satisfy the properties closure, associativity, commutativity, existence of identity, and existence of inverse.
- The second operation "□" should satisfy two properties closure and associativity.
- In addition, the second operation (□) must be distributed over the first operation (·).

Fields :

- A field F is denoted by F = < {. . . }, ·, □ >.
- A field F is a set of elements with two binary operations, " · " and "□ ", such that F is a commutative ring where the second operation (□) satisfies all the five properties defined for the first operation (·) except that there is no inverse for the identity element of the first operation with respect to the second operation.
- Fig. 5.1 shows the field.



(G-2971)Fig. 5.1 : Concept of Field

Q. 2 Explain the term prime numbers.

Ans. :

Definition :

- A prime number is a positive integer greater than 1 which is divisible by only two integers, 1 and itself.
- For example, the numbers 2, 3, 5, 7, 11, 13, 17 and 19 are all prime numbers, whereas the numbers 4, 6, 8 and 10 are composite (means not prime), because they have more than two divisors.
- The smallest prime number is 2, which is divisible by 2 itself and 1. The integer 1 is not a prime because a prime must be divisible by two different integers, no more, no less and the integer 1 is divisible only by itself.

Relatively prime / Coprimes :

- Two positive integers a and b are said to be relatively prime or co-prime, if gcd(a, b)= 1.
- The gcd stands for Greatest common divisor.
- GCD of two positive integers is the largest integer that can fully divide both the integers.
- E.g. GCD (5, 10) is 5. GCD of (11, 13) is 1.
- Two numbers are said to be relatively prime if they have no common factors except the integer 1. For example, the integers 14 and 15 are relatively prime; however, the integers 14 and 16 are not relatively prime as they have a common factor other than the integer 1.
- The integer 1 is relatively prime with any integer.
- Also, if p is a prime number, all integers ranging from 1 to p−1 are relatively prime to p .

How to check Primeness of number :

- To check the primeness of number, apply the divisibility test, where we check whether the number n is divisible by any of the prime numbers less than $\sqrt{n}$.

Q. 3 Check whether 89 is a prime.

Ans. :

- The floor of $\sqrt{89} = 9$.
- The integral value of 89 is 9.
- The prime numbers less than 9 are {2, 3, 5, 7}. As 89 is not divisible by any of these numbers, it is a prime number.

Q. 4 State the advantages and disadvantages of Symmetric Key Cryptography.

Ans. :

Advantages of Symmetric Key Ciphers :

1. The major advantages of symmetric key algorithm is that it is more efficient than the public key algorithms. It takes less time to encrypt a message using the symmetric key algorithm. This is because this key is of smaller size (length).
2. The symmetric key algorithms can be used for encryption and decryption of long messages.

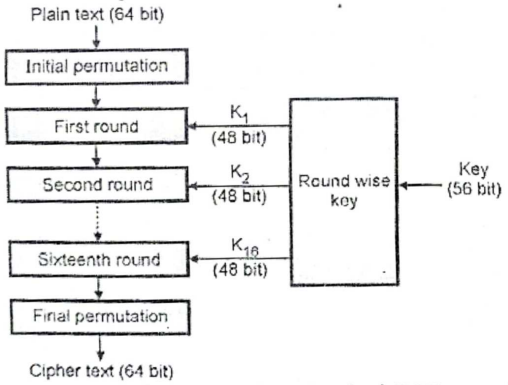
Disadvantages of Symmetric Key Ciphers :

1. The first disadvantages is that the sender and receiver both should have a unique symmetric key. So a large number of keys are required when the numbers of users increases.
2. The distribution of keys between two users can be difficult.

Q. 5 Write a note on : Data encryption standards.

Ans. :

- The elements of DES cipher at the encryption have been shown in Fig. 5.2.



(G-680) Fig. 5.2 : Data Encryption Standard (DES) general structure

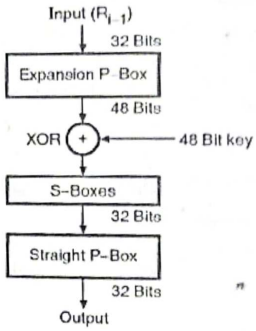
- The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. DES is based on a symmetric-key algorithm that uses a 56-bit key.
- The DES at the sending site takes in the 64-bit plaintext, works on it using a 56 bit symmetric key and produces a 64 bit ciphertext.
- At the receiving end, the DES takes the 64-bit ciphertext, works on it using the same 56 bit key and produces the 64 bit plaintext again.

Rounds :

- As shown in Fig. 5.2, there are 16 rounds in a DES, each one of which is an invertible transformation. Each round consists of upto two cipher elements namely the swapper and the mixer. Both of them are invertible.
- Each rounds take L_{i-1} and R_{i-1} (Left and Right parts of 32 bit each) from the previous round and produces its own L_i and R_i parts of 32 bits each. The output of the sixteenth round is applied to the **Final Permutation** block which produces the 64 bit ciphertext.

DES function :

- Fig. 5.3 shows the block diagram of DES function, which is the heart of DES.



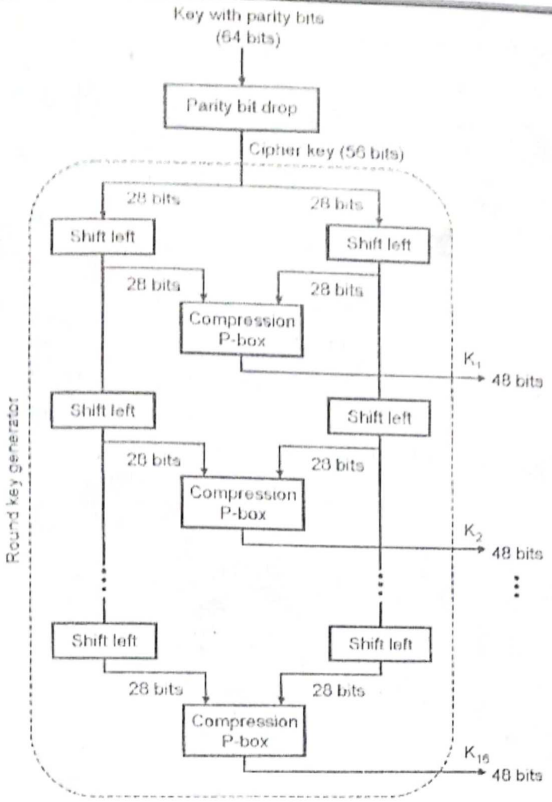
(G-2341) Fig. 5.3 : Block diagram of DES function

- As shown a DES function consists of four sections :
  1. An expansion P-box.
  2. A whitener to add key.
  3. S-boxes.
  4. Straight P-box.
- A DES function applies a 48-bit key to the rightmost 32 bits (R_{i-1}) and produces a 32 bit output.
- The input (R_{i-1}) is 32 bit long and the key has 48 bits. Therefore the input is expanded to 48 bits using the expansion P-box. After expansion, the XOR operation is used on the expanded right section and the 48 bit key.
- Real mixing takes place at the S-boxes. The straight permutation is carried out in the straight P-box to produce the final 32-bit output.

Q. 6 Explain the key generation steps in DES.

Ans. :

- Fig. 5.4 shows the key generation during each round.



(G-2963)Fig. 5.4 : Key generation during each round

- The round key generator uses the 56-bit cipher key and performs the following steps to generate the key for that round.

1. The plaintext is divided into two halves of 28 bits each.
2. The circular left shift operation is performed on each 28-bit half. Shift either 1 or 2 bits, depending on the round number. For the rounds 1, 2, 9 and 16, shifting is done by 1 bit, whereas in the case of the other rounds, shifting is done by 2 bits.
3. After performing the shifting, both halves are combined again to form a 56-bit part. These 56 bits are applied to the compression P-box.
4. The compression P-box, compresses the 56-bit input to produce 48-bit output. This 48-bit output generated from the P-box is used as a key for the round.

Q. 7 Explain triple DES with Three Keys.

Ans. :

- Three keys K1, K2 and K3 of 56 bits each are used in this version.
- A different key is used for encryption/decryption in each step.

Encryption :

- During the encryption, the plaintext P is encrypted to generate ciphertext $C = E_{K3}(D_{K2}(E_{K1}(P)))$

Decryption :

- During the decryption, to obtain the original plaintext P from the ciphertext C, the keys are used in the reverse order from that of encryption process.

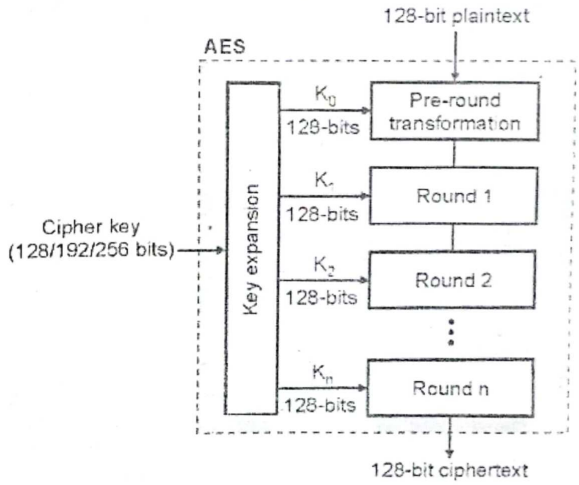
$$P = D_{K1}(E_{K2}(D_{K3}(C)))$$

- 3-DES version becomes more secure as the use of three different keys increases the key length to 168 bits.
- It results in an increased overhead due to managing and transporting one more key.
- In 3-DES, the backward compatibility with DES is provided by having either K1 = K2 or K2 = K3.

Q. 8 Explain the general design for AES algorithm.

Ans. :

- Fig. 5.5 shows the general design for AES encryption algorithm (AES cipher).
- The design of AES decryption algorithm (AES inverse cipher) is also similar, except that the round keys are used in the reverse order from that of encryption.
- In AES, Each round consists of many stages, each of which transforms the 16-byte data block.
- In AES, the term 'data block' is used at the beginning and end of the cipher, while the term 'state' is used before and after each stage to refer to a data block.
- A state is also 16-bytes long and includes the data before and after the transformation.



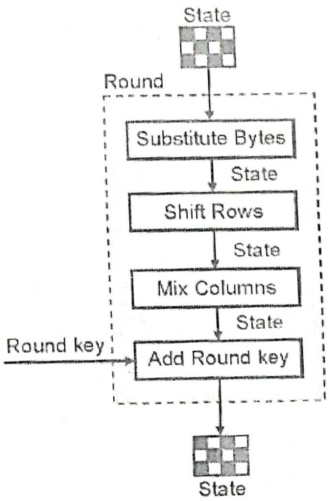
(G-2967) Fig. 5.5 : AES Encryption Cipher

- Usually, a 16-byte state (S) is organized as a 4 × 4 bytes matrix.
- Each element of the matrix is referred to as S_{ij} ($0 \le i \le 3$ and $0 \le j \le 3$), where i and j are the row and column number respectively.

Q. 9 With neat diagram explain the structure of an encryption round in AES.

Ans. :

- The structure of an encryption round is as shown in Fig. 5.6.



(G-2964) Fig. 5.6 : Structure of an Encryption Round

- In the encryption process, each round, except the last one, involves the following four transformations :
  1. Substitute Bytes
  2. Shift Rows
  3. Mix Columns
  4. Add Round Key
- Each transformation accepts a state, make changes in it and creates a new state.
- The created new state is given as input to the next transformation or the next round. The last round includes only three transformations, except the Mix Columns transformation.
- Additionally, one Add Round Key transformation is applied before the first round.
- It is mentioned as pre-round transformation in Fig. 5.5.
- In AES, the nature of each transformation is invertible and during decryption, the inverse of these transformations, namely, Inverse Substitute Bytes, Inverse Shift Rows, Inverse Mix Columns and Add Round Key are used.
- The transformation add round key is self-invertible.

Algorithm :

1. **Key Expansion :**
   - Round keys are derived from the cipher.
2. **Initial Round : Add Round Key :**
   - Each byte of the state is combined with the round key using bitwise xor.
3. **Rounds :**
   a. **Sub Bytes :** a non-linear substitution step where each byte is replaced with another according to a lookup tables.
   b. **Shift Rows :** a transposition step where each row of the state is shifted cyclically a certain number of steps.
   c. **Mix Columns :** a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   d. **Add Round Key**
4. **Final Round (no MixColumns) :**
   1. SubBytes 2. ShiftRows 3. AddRoundKey

Q. 10 State advantages and disadvantages of public key cryptography.

Ans. :

Advantages :

1. There is no compulsion of using (sharing) the same key by the sender and receiver.
2. The number of keys required reduces drastically.

Disadvantages :

1. The algorithms used are highly complex.
2. It takes a long time to calculate ciphertext from plaintext. Therefore it is very slow.
3. It is necessary to verify the association between a sender and this public key.

Q. 11 Compare secret key system and public key cryptosystems.

Ans. :

Table 5.1 : Comparison of Symmetric and Asymmetric Key

Sr. No.	Parameter	Symmetric key (Public key) cryptosystem	Asymmetric (Private) key cryptosystem
1.	Number of secret keys required in the community of n people.	n (n – 1)/2 (very large)	Only n (small)

Sr. No.	Parameter	Symmetric key (Public key) cryptosystem	Asymmetric (Private) key cryptosystem
2.	Types of keys used	The sender and receiver have to use the same secret key.	The sender uses the public key for encryption while the receiver uses the private key for decryption.
3.	Principle of operation	Based on the substitution and permutation of symbols.	Based on the application of mathematical function to the numbers.
4.	Plaintext and ciphertext	Are in the form of symbols.	Are in the form of numbers.
5.	Speed of operation	Fast	Slow
6.	Suitable for	Encryption and Decryption of long messages.	Encryption and Decryption of short messages.
7.	Examples	Substitution cipher, block ciphers, transposition ciphers, stream ciphers etc.	RSA algorithm.

Q. 12 Write a note on : RSA.

Ans. :

- RSA is the most widely used public key algorithm. It is named after its creators – Rivest, Shamir and Adleman.
- The principle of RSA is simple.
- It is based on a fact that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back.
- The algorithm is as follows :

1. Take two very large prime numbers A and B of equal lengths and obtain their product (N).

$$\therefore \quad N = A \times B \qquad ...(1)$$

2. Subtract 1 from A as well as B and take the product T.

$$\therefore \quad T = (A-1)(B-1)$$

3. Choose the public key (E) which is a randomly chosen number such that it has no common factors with T.
4. Obtain the private key (D) as follows

$$D = E^{-1} \bmod T \qquad ...(2)$$

5. The rule (algorithm) for encryption of a block of plaintext M into ciphertext (C) is as follows :

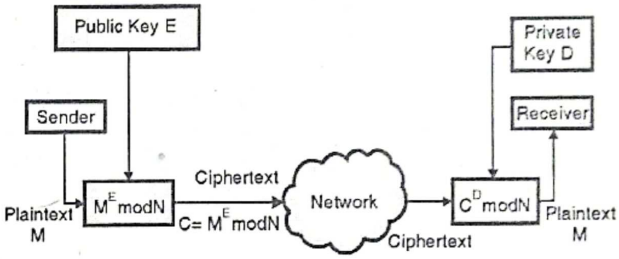
$$C = M^E \bmod N \qquad ...(3)$$

- That means the plaintext M is raised to the power of E (public key) and then divided by N.
- The mod term in Equation (3) tells us that the remainder of this division is sent as the ciphertext C as shown in Fig. 5.7.

6. The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule (algorithm).

$$M = C^D \bmod N \qquad ...(4)$$

- The encryption and decryption process using the RSA algorithm is illustrated diagrammatically in Fig. 5.7.



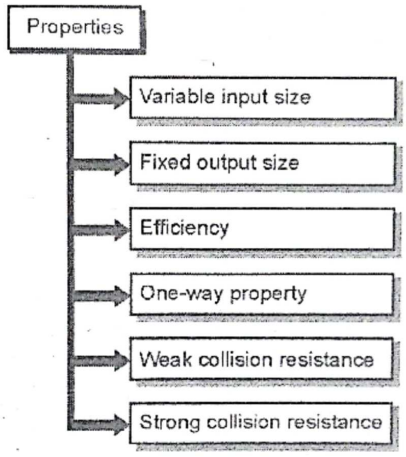
(G-682) Fig. 5.7 : Encryption and decryption in RSA

Q. 13 Explain various characteristics of hash functions.

Ans. :

Characteristics of hash functions :

- Fig. 5.8 shows the properties or requirements of Hash function.



(G-2965)Fig. 5.8 : Properties of Hash Function

- The hash function must have the following properties in order to be used for message authentication.

1. **Variable input size :**
- Hash function H can be applied to a block of data of any size.

2. **Fixed Output size :**
- The output generated by the hash function should always be of fixed length.

3. **Efficiency :**
- It is easier to generate the hash code for any given message or block of data. That means for a given message, H(M) should be easily computable making the hardware and software implementation, feasible.

4. **One-way property :**
- It is nearly impossible to determine the corresponding message or block of data for any given hash value .
- That means, one should not be able to determine M if h is given, such that H(M)= h . This is referred to as one-way property .
- This property is mainly important when a secret value is being used in the authentication. Even though the secret value is not sent, the attacker can still easily find out the secret value if the used hash function does not show the one-way property.

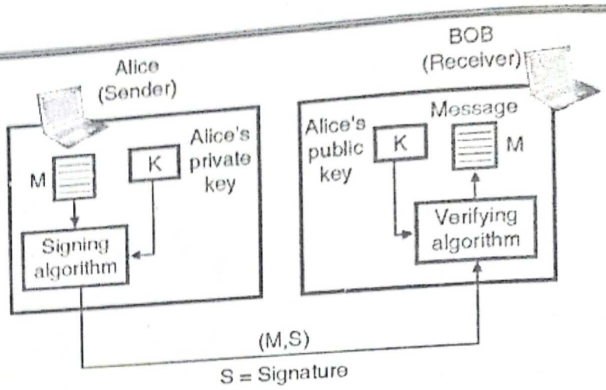
5. **Weak collision resistance :**
- It should not be computationally possible to determine another message or block of data generating the same hash code as that of the given message or block of data.
- That means, for given M_1, there is no other M_2 (where $M_1 \neq M_2$) such that $H(M_1) = H(M_2)$. This property is referred to as weak collision resistance .

6. **Strong collision resistance :**
- There should not be same hash code for two messages or blocks of data, even being almost similar.
- That means, it is almost impossible to determine a pair (M_1, M_2) such that $H(M_1) = H(M_2)$. This property is referred to as strong collision resistance .
- Out of these six properties, if the first five properties are satisfied, then the hash function is called a weak hash function.
- If all the six properties are satisfied, then the hash function is called a strong hash function. Because the sixth property protects the hash function from the birthday attack.

Q. 14 Write a note on : Digital signature process.

Ans. :

- The digital signature process is as shown in Fig. 5.9.



(G-2348) Fig. 5.9 : Digital signature process

- A signing algorithm is used by Alice to sign the message (M). And the message is sent along with the signature (S) on the unsecure channel. At the receiver, the message and signature (M, S) are applied to a verifying algorithm. If the result is true the message is accepted, otherwise it is rejected.
- Alice uses her private key (which is known only to her) applied to the signing algorithm to sign the document.
- Bob applies the public key (which is available to everyone) to the verifying algorithm to confirm the digital signature. Thus anybody can verify the digital signature but only Alice can sign it using her own private key.
- It is important to note that we cannot use a **secret key** to sign and verify a signature.

Q. 15 Explain use of digital signature in providing messages integrity and message authenticity.

Ans. :

- The digital signature system can directly provide the following three services :
  1. Message integrity
  2. Message authentication
  3. Non repudiation
- However the message confidentiality is not provided directly by digital signature. For that the encryption and decryption has to be done.

1. **Message Authentication :**
- A digital signature provides message authentication in exactly the same way as provided by the conventional signature. This is also called as the data origin authentication.

- That means Bob can verify the received message is indeed originated by Alice because he uses Alice's public key for such verification.

2. **Message Integrity :**

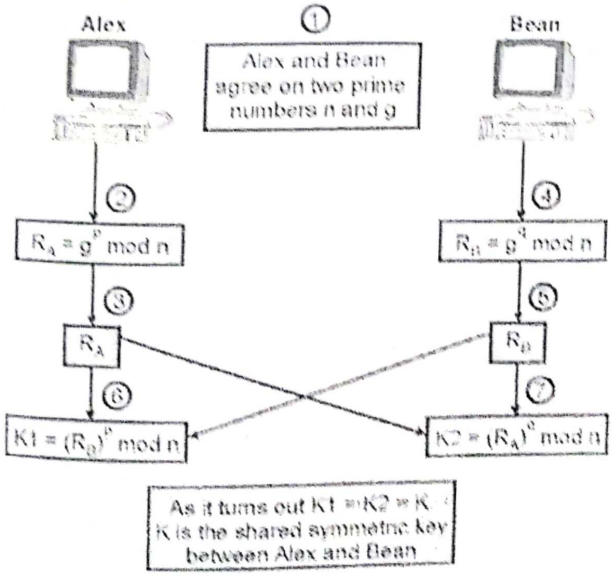
- By signing either the message itself or the message digest, we can preserve the message integrity.
- This is because, if an unauthorized entity changes a part of the message, then we won't get the same digest. Thus a digital signature scheme preserves the integrity of a message.

Q. 16 Explain Diffie-Hellman Key Exchange Algorithm in steps.

Ans. :

Diffie-Hellman Key Exchange Algorithm :

- Consider two users Alex and Bean want to communicate with each other securely over an insecure network.
- Initially, both the users Alex and Bean need to agree upon a key that is to be used for encryption and decryption of the messages that would be exchanged between them.
- For this, they can follow the Diffie-Hellman key exchange algorithm as shown in Fig. 5.10.



(G-2973)Fig. 5.10 : Diffie-Hellman key exchange algorithm

- The Diffie-Hellman key exchange algorithm works as follows :

1. Select two large prime numbers n and g by the mutual agreement of Alex and Bean. There is no need to keep these two numbers secret. The values of n and g are public.
2. Alex selects a random number p and calculates the value of R_A such that $R_A = g^p \bmod n$.
3. Alex sends the value of R_A to Bean .
4. Bean selects a random number q and calculates the value of R_B such that $R_B = g^q \bmod n$.
5. Bean sends the value of R_B to Alex.
6. Now, Alex calculates the secret key K1 as follows

$$K1 = (R_B)^p \bmod n$$

7. Bean calculates the secret key K2 as follows :

$$K2 = (R_A)^q \bmod n$$

- This means that K1 = K2 = K is the symmetric key, which Alex and Bean must keep secret and can use for encrypting/decrypting their messages.

Proof of algorithm :

- To show that both Alex and Bean have calculated the same secret key, we need to prove that the calculation of K by Alex and Bean which creates the identical results.

$$K1 = (R_B)^p \bmod n$$

$$= (g^q \bmod n)^p \bmod n$$

$$= (g^q)^p \bmod n$$

...[using the rule of modular arithmetic]

$$= g^{pq} \bmod n$$

$$= (g^p \bmod n)^q \bmod n$$

... [using the rule of modular arithmetic]

$$= (R_A)^q \bmod n$$ Hence, proved.

Q. 17 Write a short note on : Key Distribution Center.

Ans. :

- KDC is a trusted third party used for secret key distribution. The procedure of key distribution is as under.
- Each person establishes a shared secret key with the KDC and a secret key is established between the KDC and each of its members.

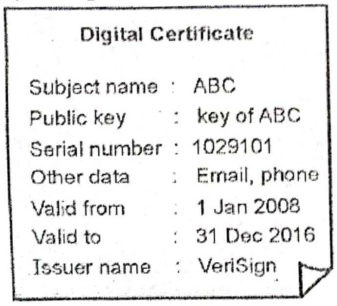
- Now using the KDC how a confidential communication would take place between Alice and Bob ? The stepwise process is as follows :
  1. Alice sends a request to KDC and tells that she wants a temporary secret key for the communication between herself and Bob.
  2. KDC tells Bob about Alice's request.
  3. If Bob is ready to communicate, then KDC creates a temporary (session) secret key between the two.
- This secret key will authenticate both Alice and Bob to KDC and prevents any attacker from impersonating Alice or Bob.

Q. 18 What are the typical contents of a digital certificate ?

Ans. :

Contents of a digital certificate :

- A digital certificate is a small computer file used to establish a relation between both the user and his or her public key.
- It is an electronic document that provides information to prove the identity of an entity.
- A digital certificate contains the user name and his or her public key. So that we can identify that the particular key belongs to the particular user.
- This concept of digital certificates is shown in Fig. 5.11.



(G-2975)Fig. 5.11 : Conceptual view of a digital certificate

- A digital certificate contains the following information :
  1. Subject name
  2. Public key
  3. Serial number
  4. Other data like email, phone, etc
  5. Valid from
  6. Valid to
  7. Issuer name
- Here subject name is the name of the user. The public key is the photograph and signature.
- The serial number is the number of a digital certificate.
- Other data contain some personal information of user.
- Validity field shows the validity of a particular digital certificate.
- The issuer's name is the name of the person who issues a digital certificate for a user.

Q. 19 Write a short on : Certification Authority in Digital Certificate.

Ans. :

Certification Authority in Digital Certificate :

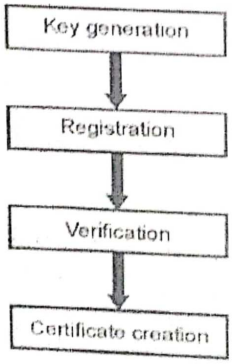
- A certification authority is a trusted agency that issues digital certificates.
- A certificate authority (CA) should be the trusted one. The governments in the various countries decide who can and who cannot be a CA.
- Generally, a CA is a reputed organization like a post office, financial institution, software company, etc.
- A certification authority issues digital certificates to individuals and organizations.
- They can use those certificates in asymmetric key cryptographic applications. The VeriSign and Entrust are world's most famous CAs.

Q. 20 Explain the four key steps in the creation of a digital certificate.

Ans. :

Steps in the creation of a digital certificate :

- The steps in the creation of a digital certificate are summarized in Fig. 5.12.



(G-2979)Fig. 5.12 : Creation of Digital Certificate

- Following are the steps involved in the creation of digital certificate.

1. Key generation
2. Registration
3. Verification
4. Certificate creation

Step 1 : Key Generation :

- In this step, the key is generated by either user or registration authority. A key can be generated using two approaches.

Approach 1 :

- In this approach, the user creates a private and public key. Users must keep their private key secret. A user sends the public key with additional information to the registration authority (RA). RA is an intermediate between the CA and the user.

Approach 2 :

- RA generates a key pair for a user. This approach is required when the user is unaware of the technical and software knowledge. The disadvantage of this approach is RA can find out the private key of the user.
- The disadvantages of this approach are RA can find out the private key of the user and the scope for this key to be exposed to others while in transit after it is generated and sent to the appropriate user.

Step 2 : Registration :

- If the user generates the pair of key, then only this step is required.
- If RA generates the pair of a key for the user, then key registration is done in the first step only.
- A user sends his/her public key and some other information to the RA. This software provides a wizard where users enter details and submit.
- After that the data travel through the network and reach to the RA. After that user request for the certificate will be registered, and the format for the certificate request has been standardized. This process is known as CSR (Certificate Signing Request).

Step 3 : Verification :

- After the completion of registration process, RA identifies the user credentials.
- It verifies the user's credentials such as the evidences provided are correct and that they are acceptable.
- It also ensures that the user who is requesting for the certificate does really possess the private key corresponding to the public key that is sent as a part of the certificate request to the RA.

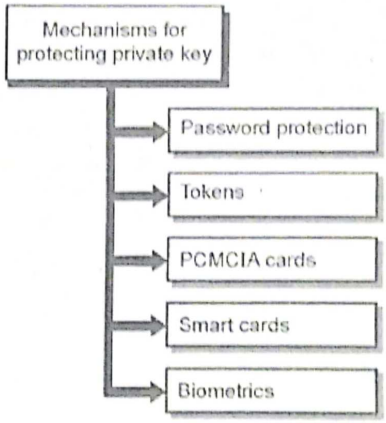
Step 4 : Certificate Creation :

- After completion of all the above steps, RA passes all the details to the CA.
- CA cross-checks all the details and generates a digital certificate for the user.
- CA sends the certificate to the user and keeps one copy of certificate with itself to keep the records.
- The Copy of the certificate is stored in the certificate directory.

Q. 21 Write a short note on Mechanisms for Protecting Private Keys.

Ans. :

- A private key be protected by using the several mechanisms as shown in Fig. 5.13.



(G-2978)Fig. 5.13 : Mechanisms for Protecting Private Keys

- Following are the mechanisms for Protecting Private Keys :

1. Password protection :

- The password protection is the simplest and most common method to protect a private key.
- IN this mechanism, the private key is stored on the hard disk of the user's computer as a disk file.
- The user can access this file only with the help of a password or a Personal Identification Number (PIN).
- But, this method is considered as the less secure method because anyone who can guess the password correctly can access the private key.

2. Tokens :

- The token stores the private key in an encrypted format.
- A one-time password is required to decrypt and access the key. A one-time password is valid only for that particular access, this password becomes invalid next time, and another OTP must be used.
- This is a more secure method.

3. **PCMCIA cards :**

- PCMCIA stands for the Personal Computer Memory Card International Association (PCMCIA). These cards are chip cards.
- The private key is stored on PCMCIA card, which means there is no need to store key on user's hard disk. This reduces the chances of key being stolen.
- There is scope for key being captured by an attacker as, in case of signing or encryption operation, the key must travel from the PCMCIA card to the memory of the user's computer.

4. **Smart cards :**

- A smart card stores the private key of the user in a tamperproof card.
- A computer chip is also included in the smart card, which can perform cryptographic functions like signing and encryption. The main advantage of this scheme is that the private key never leaves the smart card.
- The disadvantage of the smart card is that the user must carry the smart card with her and only compatible smart card readers can access it.

5. **Biometrics :**

- In this mechanism, the private key is associated with a unique characteristic of an individual.
- Unique characteristic of an individual can be a fingerprint, retina scan or voice comparison.
- This method is similar to the token, but here the user need not carry anything with him.

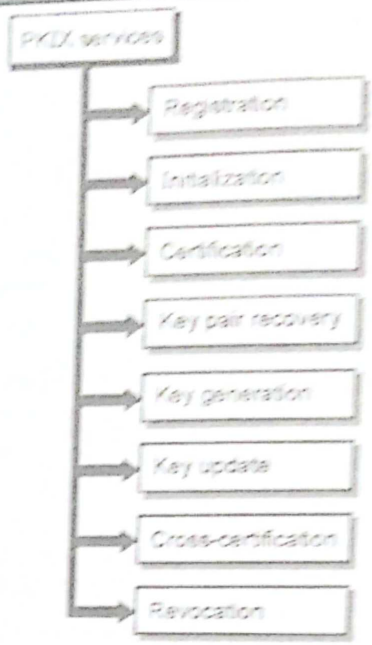
Use of PKCS#12 standard :

- In many situations, the private key of the user might be required to be transported from one location to another.
- E.g. Suppose the user wants to change his/her PC.
- To handle such situations, there is a cryptographic standard PKCS#12 which allows a user to export her digital certificate and private key in the form of a computer file.
- The certificate and the private key should be protected as they are moved to another location.
- The PKCS#12 (Public Key Cryptography standard#12) guarantees that the certificate and the private key are encrypted using a symmetric key which is derived from the user's private key protection password.

Q. 22 Explain services provided by PKIX.

Ans. :

- The services provided by PKIX are as shown in Fig. 5.14.



(G-2381) **Fig. 5.14 : PKIX Services**

Registration :

- In this process, an end-entity (subject) makes itself known to a CA through RA.

Initialization :

- This service deals with the basic problems, such as how the end-entity is sure that it is talking to the right CA?

Certification :

- The CA produces a digital certificate for the end-entity and returns it to the end-entity.
- It maintains a copy for with it for its own record and also copies it in public directories, if required.

Key pair recovery :

- To decrypt some old documents, the Keys used for encryption may be required to be recovered at a later date.
- The CA or an independent key recovery system provides the key archival and recovery services.

Key generation :

- PKIX model specifies that the end-entity should be able to generate private and public key pairs or the CA/RA should be able to generate private and public key pairs for the end-entity.
- The generated private and public key pairs are then distribute to the end-entity securely.

Key update :

- It is a process where the expired key of the digital certificate is automatically renewed and replaced with a new key pair.
- Here, the provision is made for manual digital certificate renewal requests and responses.

Cross-certification :

- In this process the end entities that re-certified by different CA, can cross verify each other. It helps in establishing trust models.

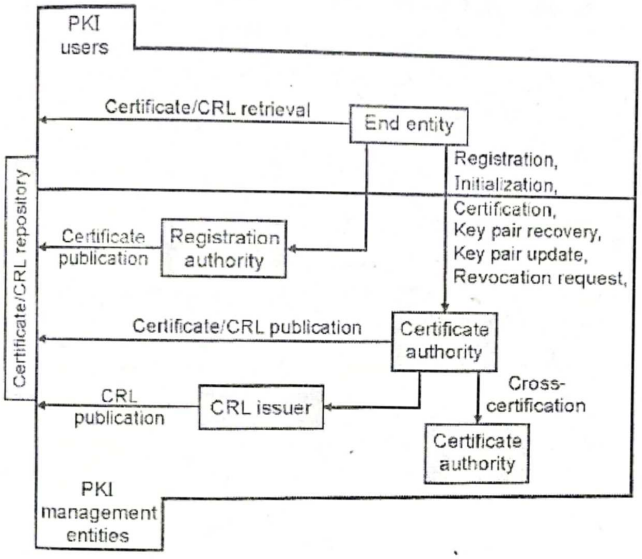
Revocation :

- PKIX model provides support for the checking the status of the certificate in two modes : online by using Online certificate status protocol (OCSP) or offline by using the Certificate Revocation List (CRL).

Q. 23 Explain PKIX model.

Ans. :

- Fig. 5.15 shows the interrelationship between the key elements of the PKIX model.



(G-2982)Fig. 5.15 : Components of PKIX model

- The key elements of PKIX model are as follows :
  1. End entity
  2. Certification authority (CA)
  3. Registration authority (RA)
  4. CRL issuer
  5. Repository

1. End entity :

- The subject field of a public key certificate identifies a general term used to denote end users, devices (e.g., servers, routers), or any other entity.
- The function of an end entity is to consume and/or support PKI-related services.

2. Certification authority (CA) :

- The CA is the issuer of certificates and usually certificate revocation lists (CRLs).
- CA supports administrative functions, even though these are often delegated to one or more Registration Authorities.

3. Registration authority (RA) :

- Registration authority is an optional part that can assume a number of administrative functions from the CA.
- The RA is always associated with the registration process of end entity. It can assist in a number of other areas as well.

4. CRL issuer :

- CRL issuer is an optional component that a CA can hand over to publish CRLs.

5. Repository :

- The repository component stores the certificates and CRLs so that they can be retrieved by end entities.

Chapter 6 : Introduction to Cyber Security

Q. 1 Define cyber security. State its importance.

Ans. :

Definition of cyber security :

- Cyber security is the process of protecting critical systems and sensitive information from digital attacks.

Importance of cyber security :

- Following are the reasons why cyber security is so important in the digital world :
  1. Cyber attacks can be expensive for businesses to continue.
  2. In addition to financial damage suffered, a data breach can also causes countless reputational damage.
  3. Cyber-attacks these days are becoming increasingly critical. Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- Due to the above reasons, cyber security has become an important part of the business or an individual.
- The focus now is on developing appropriate response plans to minimize the damage in the event of a cyber attack.

Q. 2 Why do cyber attacks happen ?

Ans. :

- The cyber attacks happen because criminals are interested in :
  1. Customers financial details (e. g credit card data).
  2. Sensitive personal data.
  3. Customers email addresses and login credentials.
  4. Customer databases.
  5. Clients lists.
  6. IT infrastructure.
  7. IT services (e.g. the ability to accept online payments).
  8. Intellectual property (e.g. trade secrets or product designs).
  9. Financial details of businesses.

Q. 3 What are the challenges in cyber security ? Explain in brief.

Ans. :

- The Cyber Security Challenges are as follows :
  1. Ransomware Evolution
  2. IoT Threats
  3. Blockchain Revolution
  4. Server-less Apps Vulnerability
  5. AI Expansion

1. Ransomware Evolution :

- Ransomware is a type of malware which locks the information on a victim's computer and payment is demanded before the ransomed data is unlocked.
- Access rights returned to the victim after successful payment.
- Ransomware is the nuisance of cyber security, data professionals, IT and executives.
- Day by day, ransomware attacks are growing rapidly in the areas of cybercrime.
- Business leaders and IT professionals need to have a powerful recovery strategy against the malware attacks in order to protect their organization.
- The strategy involves proper planning to recover corporate and customer's data and application.
- DRaaS solutions are the best protection against the ransomware attacks.
- With DRaaS solutions we can automatically back up our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

2. IoT Threats :

- Internet of Things (IoT) is a system of interconnected physical devices which can be accessible through the internet.
- The physical devices in IoT have a unique identifier (UID) and have the capability of transferring data over a network without any requirements of the human-to-human or human-to-computer interaction.
- The firmware and software running on IoT devices make consumer and businesses highly vulnerable to cyber-attacks.
- So every organization needs to work with cyber security professionals to make sure the security of their password policies, session handling, user verification, authentication and security protocols to help in risk managment.

3. Blockchain Revolution :

- Blockchain technology is the most important development in computing era.
- The blockchain technology allows crypto currencies like Bitcoin.
- It is global platform which allows two or more parties to do a transaction or do business without need of a third party for trust establishment.
- What blockchain systems will offer in regards to cyber security is difficult predict.
- The cyber security professionals can make some educated predictions regarding blockchain.
- There will be a tension but also balancing integrations with traditional, proven, cyber security approaches as the cyber security context emerges application and utility of blockchain.

4. Serverless Apps Vulnerability :

- Serverless apps depend on third-party cloud infrastructure or on a back-end service like google cloud function, Amazon web services (AWS) lambda etc.
- The serverless apps invite the cyber attackers to spread threats easily because the users access the application locally or off-server on their device.
- Therefore the user should take care for the security precautions while using serverless application.

- The serverless apps cannot do anything to keep the attackers away from our data.
- The serverless application will not help if an attacker gains access to our data through vulnerability such as leaked credentials, a compromised insider or by any other means.
- It is possible to run software with the application that provides best possibility to beat the cybercriminals.
- The size of the serverless application is small. It helps software developers to launch their applications easily and quickly.
- The web-services and data processing tools are examples of the serverless apps.

5. AI Expansion :

- Artificial Intelligence (AI) is the science and engineering of making intelligent machines, especially intelligent computer programs.
- The formation of intelligent machines with AI can work and react like humans.
- Artificial intelligence includes activities like speech recognition, learning, planning, problem-solving, etc.
- When the malicious attack starts, AI has the ability to protect and defend an environment which mitigates the impact.
- AI takes instant action against the malicious attacks at an instant when a threats impact a business.
- AI is considered as a future protective control that will allow our business to stay ahead of the cyber security technology curve.

Q. 4 Write a short note on : CIA Triad.

Ans. :

- The three letters in "CIA triad" stand for confidentiality, integrity and availability. The CIA triad is a widely used information security model.
- The aim of CIA triad model is to guide organizations about efforts and policies for the data security.

1. Confidentiality :

- The meaning of message confidentiality or privacy is that the sender and the receiver expect confidentiality and only the intended receiver should be able to decode the transmitted message correctly.
- To all others, the message must look like garbage..

2. Integrity :

- The meaning of message integrity is that the received data at the receiver must exactly be the same as were sent. The transmitted data must not changes during the transmission, neither accidentally nor maliciously.
- The message integrity is important for all the monetary exchanges occurring over the Internet.

3. Availability :

- The information should not be available to any unauthorized person but it should be always available to an authorized entity.

Q. 5 Explain seven layers of cyber security.

Ans. :

Seven layers of cyber security :

- Fig. 6.1 shows the seven layer architecture of cyber security.

Layer 7	The human layer
Layer 6	Perimeter security
Layer 5	Network security
Layer 4	Endpoint security
Layer 3	Application security
Layer 2	Data security
Layer 1	Mission critical assets

(G-2986) Fig. 6.1 : Layers of cyber security

- The following are seven layers of cyber security :
  1. Mission-Critical Assets
  2. Data Security
  3. Endpoint Security
  4. Application Security
  5. Network Security
  6. Perimeter Security
  7. The Human Layer

Layer 1 : Mission-Critical Assets :

- This is the data that is very critical to protect. The businesses faces the malicious forces daily.
- An example of mission-critical assets in the Healthcare industry is Electronic Medical Record (EMR) software. In the financial sector, it is customer's financial records.

Layer 2 : Data Security :

- Data security controls will protect both the transfer and the storage of data.
- There should be backup security measure to prevent the loss of data. Data security needs the use of encryption and archiving.
- Data security is an important focus for all businesses as a breach of data can have horrible consequences.

Layer 3 : Application Security :

- Application security involves the security features that control access to an application and that application's access to your mission critical assets.
- This layer includes the internal security of the application itself.
- Most of the time, applications are designed with security measures which provides protection when the app is in use.

Layer 4 : Endpoint Security :

- Endpoint security controls protect the connection between the devices and the network.
- This layer makes sure that the endpoints of user devices are not exploited by breaches.
- This layer protects mobile devices, desktops, and laptops. This layer allows protection either on a network or in the cloud depending on the needs of a business.

Layer 5 : Network Security :

- Network security layer controls protect the business's network.
- The main goal of this layer is to prevent unauthorised access to the network.
- It is important to regularly update all systems on the business network with the essential security patches, including encryption.
- It is always best to disable unused interfaces for the further protection against any threats.

Layer 6 : Perimeter Security :

- Perimeter security layer makes sure that both the physical and digital security methods protect a overall business. It includes firewalls that protect the business network against external forces.

Layer 7 : The Human Layer :

- The human layer is a very important layer, in spite of being known as the weakest link in the cyber security chain.
- It includes management controls and phishing simulations as an example.
- The aim of human management control is to protect the part which is critical to a business in terms of security.
- This layer controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Q. 6 Define Vulnerability. State its examples.

Ans. :

Definition :

- Vulnerability is defined as the weakness in an information system, system processes or internal controls of an organization.
- It can be exploited by one or more attackers.

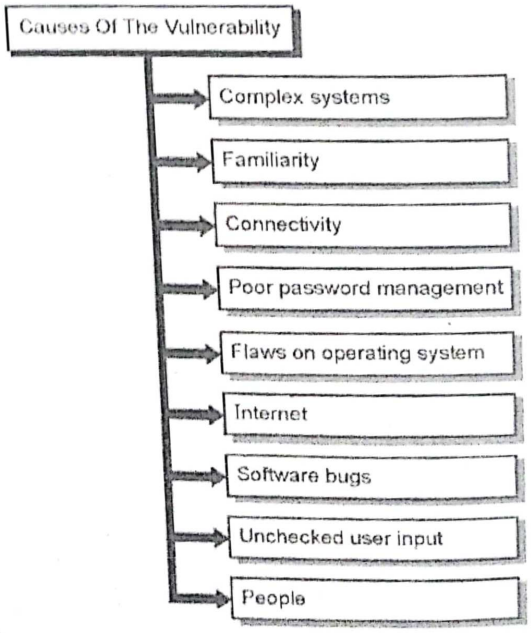
Examples of Vulnerabilities :

- Following are some examples of vulnerability :
  1. Due to a weakness in a firewall, malicious hackers can enter into a computer network.
  2. Lack of security cameras.
  3. Unlocked doors at businesses.
- With these weaknesses, anyone can harm a business or its assets.

Q. 7 What are the causes of the Vulnerability.

Ans. :

- The following are the causes of Vulnerabilities :



(G-2990) Fig. 6.2 : Causes of the vulnerability

1. **Complex Systems :**
- If the system is complex, it increases the probability of misconfigurations, flaws, or unintended access.

2. **Familiarity :**
- Cyber attackers may be known with common code, operating systems, hardware, and software which lead to known vulnerabilities.

3. **Connectivity :**
- The devices connected to the internet becomes more prone to vulnerabilities.

4. **Poor Password Management :**
- If the password used is weak and reused, it leads from one data breach to several.

5. **Flaws on Operating System :**
- The flaws in the Operating systems and unsecured OS can give users full access and become a target for viruses and malware.

6. **Internet :**
- The internet can be installed automatically on computers because internet is full of spyware and adware.

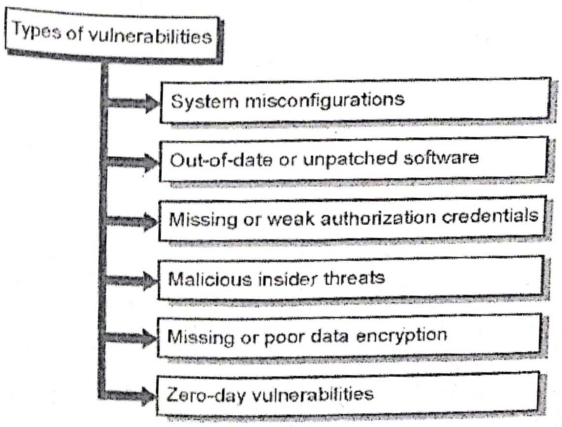
7. **Software Bugs :**
- Programmers sometimes accidentally, leave an exploitable bug in the software that leads to system vulnerability.

8. **Unchecked user input :**
- If website or software assumes that all input by user is safe, it can run unintended SQL injection.

9. **People :**
- The biggest threat to the majority of organizations is social engineering. That means, humans can be one of the biggest causes of vulnerability.

Q. 8 State and explain the types of Vulnerabilites.

Ans. :



(G-2984)Fig. 6.3 : Types of vulnerabilities

1. **System Misconfigurations :**
- The network assets having different security controls or vulnerable settings can result in system misconfigurations.
- Cybercriminals commonly search networks for system misconfigurations. The network misconfigurations are increasing due to the rapid digital transformation.
- Therefore, it is important to work with experienced security professionals when implementing new technologies.

2. **Out-of-date or Unpatched Software :**
- Cybercriminals exploit unpatched vulnerabilities to carry out attacks and steal valuable data. In order to minimize these types of risks, it is necessary to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

3. **Missing or Weak Authorization Credentials :**
- A common method of attackers use is to gain access to systems and networks through brute force like guessing credentials of employee.
- So it is important that employees should be educated on the best practices of cyber security so that their login credentials are not easily exploited.

4. **Malicious Insider Threats :**
- Unknowingly or with malicious intention, employees who have access to critical systems can share information that allows cybercriminals to breach a network.
- Insider threats can be very difficult to trace since all actions will appear legitimate.
- To help such types of threats, one should invest in network access control solutions, and divide the network according to employee seniority and expertise .

5. **Missing or Poor Data Encryption :**
- In case of poor or missing encryption, it becomes easy for attackers to intercept communication between systems and breach a network .
- In case of poor or unencrypted information, cyber adversaries are able to remove critical information and insert false information onto a server. This can weaken an organization's cyber security compliance efforts and lead to substantial fines from regulatory bodies.

6. **Zero-day Vulnerabilities :**
- Zero-day vulnerabilities are specific software vulnerabilities known to the attacker but have not yet been identified by an organization or user.

This means, there are no available fixes or solutions since the vulnerability has not yet been detected or notified by the system vendor.

These are dangerous attacks as there is no way to defend against them until after the attack has been carried out. Hence, it is important to remain careful and continuously monitor your systems for vulnerabilities in order to minimize zero-day attacks.

Q. 9 Write a short note on : Vulnerability Remediation.

Ans. :

The vulnerability remediation process is a workflow which fixes or neutralizes detected weaknesses.

It includes following steps :

1. Find 2. Prioritize
3. Fix 4. Monitor

1. Find :

- It continuously monitors software inventory to be aware of which software components are being used and what needs immediate attention will significantly prevent malicious attacks.

2. Prioritize :

- The organizations must have prioritization policies. First, the risk of the vulnerabilities needs to be calculated going through the system configuration, the likelihood of an occurrence, its impact, and the security measures that are in place.

3. Fix :

- After knowing, the security vulnerabilities that require immediate attention, it is time to map out a timeline and work plan for the fix.

4. Monitor :

- Monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications through all the relevant channels.

Q. 10 Define Threat. Explain the Sources of Cyber security Threats.

Ans. :

Definition of Threat :

- A cyber security threat is malicious and intentional attack by an individual or organization in order to gain unauthorized access to another individual's or organization's network to damage, interrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive information.

Sources of Cyber security Threats :

1. Hackers / Crackers :

- The motivation behind hacking is personal gain, revenge, aggravation, financial gain and political activism.
- They explore various cyber techniques to breach defenses and develop vulnerabilities in a computer system or network. Hackers or crackers develop new types of threats for the pleasure of challenge or bragging rights in the hacker community.

2. Nation States :

- Cyber attacks by a nation states can cause harmful impact. They can disrupt communications, military activities and everyday life.

3. Terrorist Groups :

- The terrorist do cyber attacks to destroy, get into, or exploit critical infrastructure to threaten national security, compromise military equipment, disturb the economy, and cause mass losses.

4. Criminal Groups :

- The aim of criminal groups is to get into systems or networks for financial gain. Criminal groups use phishing, spam, spyware, and malware attacks to conduct identity theft, online fraud, and system extortion.

5. Malicious Insiders :

- Malicious Insiders can be an employee, third-party vendors, contractors, or other business associates.
- Malicious Insiders have valid access to enterprise assets but they misuse that access to steal or destroy information for financial or personal gain.

6. Corporate Spies :

- Corporate spies do industrial or business spying.
- The motive behind the corporate spies is to make a profit or disturb a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

7. Hacktivists :

- The reason behind the cyber attacks by the hacktivists is political cause rather than financial gain. Hacktivists target industries, organizations or individuals who don't support with their political ideas and plans.

Q. 11 Differentiate between treat and vulnerability.

Ans. :

- Table 6.1 gives the difference between Treat and Vulnerability.

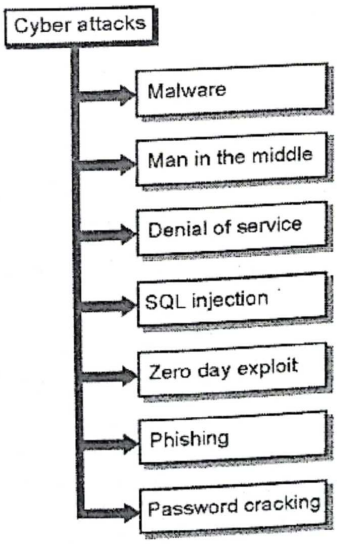
Table 6.1 : Comparison of Treat and Vulnerability

Sr. No	Threat	Vulnerability
1.	Threat take advantage of vulnerabilities in the system and can steal and damage data	Vulnerability is the weakness in hardware, software, or designs, which might allow cyber threats to happen.
2.	Can't be controlled	Can be controlled.
3.	It may or may not be intentional.	Generally, unintentional.
4.	Can be blocked by managing the vulnerabilities.	Vulnerability management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order.
5.	Threat can be detected by anti-virus software and threat detection logs.	Vulnerability can be detected by penetration testing hardware and many vulnerability scanners.

Q. 12 List the types cyber attacks.

Ans. :

- Fig. 6.4 shows the common types of cyber Attacks.

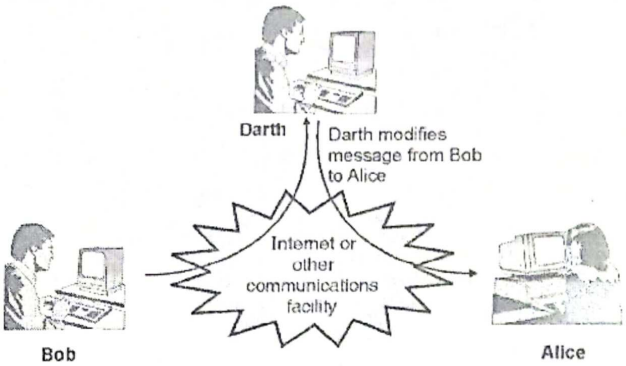


(G-2905) Fig. 6.4 : Types of cyber Attacks

Q. 13 Write a short note on : Man in the middle attack.

Ans. :

- This attack allows an attacker to intercepts the communication between the client and server.
- Due to this, an attacker can read, insert and modify the data in the intercepted connection.
- In modification, the original data sent by the authentic user is disrupted or modified by the attacker to make it non meaningful for the receiver.
- Usually the content sequence in the message is changed.
- Thus in modification of message as shown in Fig. 6.5, the attacker modifies the contents of message after sender sends it but before it reaches to indented recipients.



(G-2857) Fig. 6.5 : Modification of messages

Q. 14 Write a short note on : SQL injection.

Ans. :

SQL Injection :

- It this attack, some data will be injected into a web application to manipulate the application and get the required information.
- A structured query language (SQL) injection attack targets the database of a website and tricks the server into providing access to modify the data by unauthorized criminals.

Q. 15 Write a short note on : Phishing and password cracking.

Ans. :

Phishing :

- Phishing attack tries to steal sensitive information of uses like user login credentials and credit card number.
- The phishing attacks steals the identity and the personal information like username, password, and credit card

number etc. of the user that can steal money from the user account.

- In Vishing (voice phishing) attack, a telephone is used as a medium for identity theft.
- In Smishing (Sms phishing) attack, a sms is used to attract the customers.

Password Cracking :

- In this type of attack, attackers try to crack the password of a user by trying out all possibilities or using tools.
- John the ripper, hashcat aid the criminals etc. are the password cracking tools.
- These attacks are typically possible through the use of software that expedites cracking or guessing passwords.

Q. 16 Write a short note on : Challenges to Internet Governance.

Ans. :

- The challenges to Internet Governance are as follows :
  1. Speed and changing nature of the internet
  2. Internet as part of digitalization
  3. Concentration of digital power
  4. Digital geopolitics and the environment
  5. Shaping the digital future
  6. The future of regulation
  7. Multistakeholderism
  8. Participation in decision-making
  9. Managing critical Internet Resources
  10. Access and Diversity
  11. Security, Openness and privacy
- Q. Write a note on : Computer Criminals.
- Computer crime is also referred as cybercrime, e-crime, electronic crime, or hi-tech crime.
- Computer criminals have access to huge amounts of hardware, software, and data.

Definition :

- Computer (Cyber) crime is defined as a crime performed by a knowledgeable computer user, sometimes referred as a hacker who illegally browses or steals a company's or individual's private data.
- Computer criminals can use a device to access a user's personal information, confidential information of business, government information, or disable a device. They can sell or explicit the above information online.

Q. 17 What are the causes of Cybercrimes. State its types.

Ans. :

Causes of Cybercrimes :

- In most cases, someone commits a cyber crime to obtain goods or money.
- They target rich people or rich organizations like banks and financial firms where a large amount of money flows daily. They hack sensitive information.
- Some people commit a computer crime because they are pressured, or forced, to do so by another person.
- Some people also opt a computer crime to prove they can do it.
- It is difficult to catch such criminals.
- Hence, the numbers of cyber crime are increasing across the world.
- Computers are vulnerable, so laws are required to protect and safeguard them against cybercriminals.

Types of Cybercrimes :

- Following are the types of cyber-crimes :
  1. Hacking
  2. Child pornography and Abuse
  3. Piracy or Theft
  4. Identity Theft
  5. Computer Vandalism
  6. Malicious Software
  7. Fraud Calls/E-Mails
  8. Fake news sharing in social media
  9. Online illegal selling (Dark Web)

Q. 18 Write a short note on : Assets and Threat.

Ans. :

Assets :

- An asset is any data, device or other component of an organization's systems which is valuable.
- An asset is valuable because it contains sensitive information or can be used to access such information.
- An asset contains hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.
- Assets should be protected from illegal access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization

Example of Asset :

- The desktop computer, laptop or company phone of employee is considered an asset.
- Similarly, critical infrastructure such as servers and support systems are assets.
- An information asset is most common asset of organization.
- The databases and physical files are assets and they store sensitive data.
- Information is stored in an information asset container.

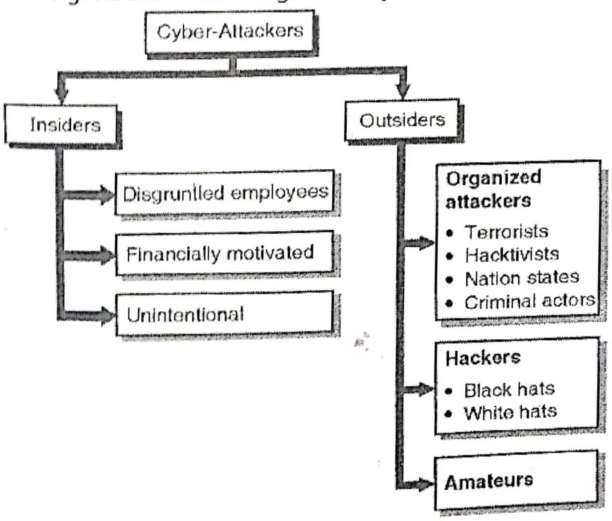
Threat :

- A threat is any event that could negatively affect an asset if it's lost, knocked offline or accessed by an unauthorized party.
- Threats can be classified as conditions that compromise the confidentiality, integrity or availability of an asset and can either be intentional or accidental.
- An intentional threat contains criminal hacking or a malicious insider stealing information.
- An accidental threat involves employee error, a technical malfunction or an event causing physical damage, such as a fire or natural disaster.

Q. 19 Write a short note on : Categories of Cyber Attackers.

Ans. :

- Fig. 6.6 shows the categories of cyber-attackers.



(G-2988) Fig. 6.6 : Categories of Cyber Attackers

Cyber attackers can be broadly classified into two types :

1. Insiders
2. Outsiders

1. Insiders :

- Insider cyber attackers act within an organization.
- The three basic categories of insiders are :
  1. Disgruntled employees
  2. Financially motivated insiders
  3. Unintentional insiders

Disgruntled employees :

- Disgruntled employees can launch disciplinary attacks or threaten the safety of internal systems.

Financially motivated Insiders :

- Financially motivated insiders (Thieves) can misuse company assets or manipulate the system for personal gain.
- Some financially motivated insiders can be acting on ethical grounds or for other reasons.

Unintentional insiders :

- Unintentional insiders can unintentionally make possible outside attacks, but are not strictly primary attackers.

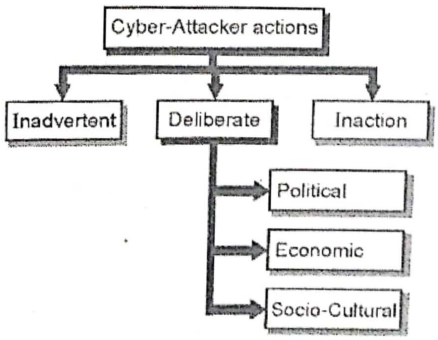
2. Outsiders :

- Outsider cyber attackers attempt to penetrate an organization from the outside.
- Based on organization, motives and professional level, outsider cyber attackers can be classified into the following three types :
  1. Organized attackers
  2. Hackers
  3. Amateurs

Q. 20 Explain the motive behind cyber attackers.

Ans. :

- The categories of cyber-attackers allow us to better understand the motivation of attackers and the actions they take. Fig. 6.7 shows the types of cyber-attacker actions and their motivations.



(G-2989) Fig. 6.7 : Types of cyber-attacker actions and their motivations

- The operational cyber security risks occur from three types of actions :
  1. Inadvertent actions
  2. Deliberate actions 3. Inaction

1. Inadvertent actions :

- Inadvertent actions are generated by insiders. These actions are taken without malicious or harmful intention.

2. Deliberate actions :

- Deliberate actions are generated by insiders or outsiders. These actions are taken intentionally and are intended to do harm.
- Following are three categories of motivation for deliberate actions :
  1. Political motivations
  2. Economic motivations
  3. Socio-cultural motivations

Political motivations :

- Examples of political motivations include destroying, disrupting or taking control of targets; spying and making political statements, protests or disciplinary actions.

Economic motivations :

- Examples of Economic motivations include stealing of intellectual property or economically valuable assets like funds, credit card information, blackmailing, fraud, industrial spying and damage.

Socio-cultural motivations :

- Examples of Socio-cultural motivations include attacks with philosophical, theological, political, and even humanitarian goals.
- It also includes fun, curiosity and a desire for publicity or ego satisfaction.

3. Inaction :

- Inactions are generated by insiders. These actions include a failure to act in a given condition because of a lack of appropriate skills, knowledge, guidance or availability of the correct person to take action.

Q. 21 What is software attack ? Explain its types.

Ans. :

Definition :

- The software designed to gain access of computer or installed into the computer without the permission of the user is known as software attack.

Types of Malware (Software attacks) :

- The software attacks are as follows :
  1. Virus
  2. Worm
  3. Trojan horse
  4. Adware
  5. Spyware
  6. Browser hijacking software
  7. Scareware

Virus :

- A virus is a self-replicating program code.
- A virus can damage or harm the host computer by deleting or adding files. It spreads throughout the computer files without user's knowledge.
- During the time of execution, the replicated copy of virus is self inserted into the other computer programs.
- A virus can be spread though email attachment, pen drives, digital images, audio or video clips, etc.
- It can occupy memory space of the computer by replicating the copy of the code. It slows down the performance of the computer or formats the host machine.

Worm :

- Worms are very similar to viruses which can replicate themselves. It is a replicating code that comes via emails which appear legitimate.
- Worms do not need human interference to travel over the entire network and they can spread from the infected machine to the whole network. Worms can spread through a network by using the loopholes in the operating system or through email.
- Due to the replication and spreading, worms consume the network resources such as space and bandwidth and can force the network to choke.

Trojan horse :

- It is a malicious code installed in the host machine by pretending to be useful software. Due to this, the user clicks on the link or download the file that pretends to be a useful file or software from a legal source.
- It damages the host computer by manipulating the data. It also generates a backdoor in the host computer that could be controlled by a remote computer.

Adware :

- Adware is a special type of malware used for forced advertising.
- Adware malware redirects the page to some advertising page or pop-up an additional page that promotes some product or event.

Spyware :

- Spyware is installed in the target computer with or without the user consent.
- It is designed to steal sensitive and confidential data from the target computer.
- Spyware collects the browsing habits of the user and sends it to the remote server.

Browser hijacking software :

- This is a malicious software downloaded along with the free software offered over the Internet and it is installed in the host computer without the knowledge of the user.
- Browser hijacking software modifies the setting of browser and redirect links to other unintentional sites.

Scareware :

- Suddenly a pop-up alert appears on the screen while surfing the Internet and it warns about the presence of dangerous virus, spywares, etc. in the user's computer.
- As a remedy, the message suggests download the full version of the software.
- When the user proceeds to download, a scareware is downloaded into the host computer.
- It holds the host computer until ransome money is paid.
- The scareware can neither be uninstalled from computer nor can it be used till the money is paid.

Q. 22 What is hardware attack ? Explain its types.

Ans. :

Definition :

- The attacks which directly exploit interaction with a system's electronic components are known as hardware attacks.

Hardware attacks :

- The following are the common hardware attacks :
  1. Backdoors 2. Spying
  3. Inducing faults 4. Hardware modification
  5. Fake product assets

Backdoors :

- The backdoors are manufactured for malware or other penetrative purposes.
- They aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
- The creation of backdoor includes the presence of hidden methods for bypassing normal computer authentication systems.

Spying :

- Spying gains access to protected memory without opening other hardware.

Inducing faults :

- If faults includes in ay hardware interrupts the normal behaviour of system.

Hardware modification :

- The modification in hardware tampers invasive operation of hardware or software.

Fake product assets :

- A fake product asset creates extraordinary operations, and those operations gains malicious access to the systems.

Q. 23 Write a note on : Cyber Warfare.

Ans. :

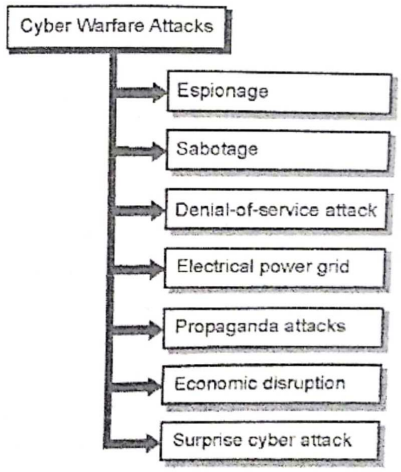
Cyber Warfare :

- Cyber Warfare is a set of actions by a nation or organization to attack on countries or institutions computer network systems with the purpose of disrupting, damaging or destroying infrastructure by viruses or denial-of-service attacks.
- Cyber warfare tries to attack on financial infrastructure, public infrastructure like dams or electrical systems, on safety infrastructure like traffic signals or early warning systems, attacks against military resources or organizations etc.

Q. 24 Write a short note on : Types of cyber warfare attacks.

Ans. :

- Fig. 6.8 shows of the main types of Cyber Warfare Attacks.



(G-2991)**Fig. 6.8 : Types of Cyber Warfare Attacks**

1. **Espionage :**
   - Espionage means spying other countries to steal secrets.
   - Espionage may involve using a botnet or spear-fishing attack in order to gain a foothold in a computer before extracting sensitive information.
2. **Sabotage :**
   - Government organizations should determine sensitive information and the risks if data is compromised.
   - Hostile governments or terrorists can steal data, destroy it, or influence insider threats.
   - Insider threats can be careless employees or government employees with relationship to the attacking country.
3. **Denial-of-Service Attack :**
   - With flooding of fake requests and forcing the website to handle these requests, DoS attacks prevent legal users from accessing a website.
   - This type of attack disturbs critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.
4. **Electrical Power Grid :**
   - Attack on the power grid allows attackers to immobilize critical systems, disturb infrastructure, which results in the physical harm.
   - An attack on the power grid disturbs communications and render services like text messages and broken communications.
5. **Propaganda Attacks :**
   - This attack tries to control the minds and thoughts of people living in or fighting for a target country.
   - Propaganda attack can be used to expose embarrassing truths, spread lies to make people lose trust in their country, or side with their enemies.
6. **Economic Disruption :**
   - Mostly economic systems operate using computers.
   - Attackers target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.
7. **Surprise Cyber attack :**
   - This attack takes place when the enemy is not expecting attack and it weaken their defences.
   - Surprise cyber attack can be used to weaken the enemy in preparation for a physical attack as a form of hybrid warfare.

Q. 25 Write a short note on : Cyber Crime.

Ans. :

Definition :

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Cybercriminals or a hacker commits cybercrime to make money.
- Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are prepared and they use advanced techniques and are highly technically skilled. Others are trainee hackers.
- Cybercrime is an illegal action against any individual using a computer, its systems, and its online or offline applications.
- Various types of Cyber crime attack modes are Hacking, Denial of Service Attack, Software Piracy, Phishing, and Spoofing.

Examples of Cybercrime :

- Following are some most commonly occurring Cybercrimes :
  1. The fraud by manipulating computer network
  2. Unauthorized access to or modification of data or application.
  3. Intellectual property theft which includes software piracy.
  4. Industrial spying and access to or theft of computer materials.
  5. Writing or spreading computer viruses or malware.
  6. Digitally distributing child pornography

Q. 26 State cyber terrorism and explain it with an example.

Ans. :

Definition :

- Cyber terrorism is a deliberate attack against a computer system, computer data, programs and other information with the only aim of violence against secret agents and subnational groups.
- Cyber terrorism is also known as information wars.
- It can be defined as an act of Internet terrorism that includes deliberate and large-scale attacks and disruptions of computer networks using computer viruses, or physical attacks using malware, to attack individuals, governments and organizations.

- The main goal of cyber terrorism is to cause harm and destruction.
- Individuals and groups are misusing the secrecy with the use of the internet.
- They threaten individuals, certain groups, religions, ethnicities or beliefs.

Examples of Cyber Terrorism :

- Following are few examples of cyber terrorism :
  1. Foreign governments can use hackers to spy on U.S. intelligence communications in order to learn about location of our troop or otherwise gain a planned advantage at war.
  2. Domestic terrorists can break into the private servers of a corporation to learn trade secrets, steal banking data or the private data of their employees.
  3. Global terror networks can disturb a major website to generate a public nuisance or inconvenience, or even more seriously, try to stop traffic to a website publishing content with which they disagree.
  4. International terrorists try to access and disable the signal which flies drones or otherwise controls military technology.

Q. 27 State and explain : Cyber espionage.

Ans. :

Definition :

- Cyber espionage or cyber spying is a attack in which an unauthorized user tries to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.
- Cyber espionage is mainly used to collect sensitive or classified information, trade secrets or other types of IP that can be used by the attacker to create a competitive advantage or sold for financial gain.
- In some cases, the breach is simply cause reputational harm to the victim by exposing private information or questionable business practices.
- Cyber espionage attacks are motivated by financial gain; they can also be installed in combination with military operations or as an act of cyber terrorism or cyber warfare.
- Cyber espionage can lead to interruption of public services and infrastructure, as well as loss of life when it is part of a broader military or political campaign.
- The most common targets of cyber espionage contains large corporations, government agencies, academic institutions or other organizations that possess valuable IP and technical data.
- Cyber spies most commonly attempt to access the following assets :
  1. Military intelligence.
  2. Intellectual property such as product formulas or blueprints.
  3. Business goals, strategic and marketing plans.
  4. Research and Development data and activity.
  5. Academic research data.
  6. Political strategies, affiliations and communications.
  7. Salaries, bonus structures and other sensitive information regarding organizational finances and expenditures.
  8. Client or customer lists and payment structures.

Q. 28 State and explain : Cyber security policies.

Ans. :

Cyber security policies :

- Some of the common cyber security policies that organizations follow are as follows :

Virus and Spyware Protection policy :

- This security policy makes sure the detection and removal of viruses by reducing security risk.
- The digital signatures are used to authenticate signals and detect suspicious behavior.

Intrusion Prevention policy :

- Intrusion Prevention policy has an automatic feature to detect network or browser attacks.
- It protects applications from vulnerabilities and uses legal ways for content checking. This contains data packages and malware as well.

Application and Device Control :

- This policy is made for the protection of the system's resources from different parts of the system.
- The device control policy is applicable for Apple and Windows while the application control policy is applicable only for Windows.

Information security policy :

- Information Security Policy is made for employees to keep the company's rules and guidelines in mind and follow them in terms of security.

Business Continuity Plan :

- Business continuity plan uses the recovery plan to restore everything necessary for the company's work.
- It defines how an organization should act during an emergency.

E-Commerce Policy :

- This policy ensures the management and operations of services according to the policy guidelines.

E-Mail Policy :

- This policy regulates the rules for handling emails inside an organization. This can be from sender or receiver.

Firewall Policy :

- The firewall is present in the network of all companies. This policy monitors its traffic.
- It ensures that internet traffic coming is secure and does not cause any threat to the organization.

Information Technology Purchasing Policy :

- This policy is required when the company uses its funds to buy any technical asset or service.
- It has a set of standards, procedures, and restrictions that they need to abide while making a purchase decision. IT department must be in the loop while this process.

Internet policy :

- This policy is contains the regulations about using company's internet. This is for employees, clients, and even other stakeholders.

Password policy :

- Password Policy restricts companies from using easy to guess passwords.
- They should generate strong passwords and change them frequently to avoid security breaches.

Server Security Policy :

- This policy defines internal server base configuration standards and restrictions and this is applicable for servers owned by the company as well as outsourced by them.

Social Media Acceptable Use Policy :

- This policy takes care of things related to social media to maintain security inside the organization.

Website operation policy :

- This policy defines guidelines about information protection, standard confidentiality and ethical transactions on the website.

Wireless connectivity policy :

- This policy defines guidelines that organizations need to follow while using free and unsecured Wi-Fi, to keep the data safe.

□□□