Unit III

3 Adhoc and WSN

3.1 : Infrastructure Network and Infrastructure-less Wireless Networks

Q.1 What is adhoc network ? List characteristic.

Ans. : • A Mobile Ad-hoc Network (MANET) is an autonomous system of nodes connected by wireless links. A MANET does not necessarily need support from any existing network infrastructure like an Internet gateway or other fixed stations. The network's wireless topology may dynamically change in an unpredictable manner since nodes are free to move.

- Information is transmitted in a store-and forward manner using multi hop routing. Each node is equipped with a wireless transmitter and a receiver with an appropriate antenna.
- An ad-hoc network consists of a set of nodes that communicate using a wireless medium over single or multiple hops and do not need any preexisting infrastructure such as access points or base stations.
- Ad-hoc networks can comprise of mobile, static, or both types of nodes. Ad-hoc networks containing mobile nodes are known as mobile ad-hoc networks.
- In ad-hoc networks all nodes of mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network.
- Ad-hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain.
- Ad-hoc networks are wireless, self organizing, systems formed by co-operating nodes within communication range of each other that form

temporary networks. Their topology is dynamic, decentralized ever changing and the nodes may move around arbitrarily.

- An ad-hoc network is a multi-hop wireless network where all nodes co-operatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a Mobile Ad-hoc Network (MANET).

Characteristics

1. Dynamic topologies : Nodes are free to move arbitrarily.
2. Bandwidth constrained, variable capacity link.
3. Power constrained operations : All the nodes in a MANET rely on batteries for their energy.
4. Limited physical security : Mobile wireless networks are generally more prone to physical security threats than fixed, hard-wired networks.

Q.2 Differentiate between infrastructure network and infrastructure-less networks ? What are issues in Adhoc wireless network ? ☞ **[SPPU : May-18, Dec.-19, End Sem, Marks 8]**

Ans. : • In Infrastructure network topology is static and infrastructure less network topology is dynamic.

- No bandwidth problem in infrastructure network but infrastructure less network may face bandwidth constrained.
- Limited physical security in infrastructure less network whereas proper security in infrastructure network.
- In Infrastructure network, planning of network is required before installation of components. In infrastructure less network automatically forms network and easy to change.

Also Refer Q.4

Q.3 Differentiate between infrastructure network and infrastructure-less networks ? What are the MAC layer and routing layer design goals ? ☞ **[SPPU : Dec.-18, End Sem, Marks 8]**

Ans. : Refer Q.2, Q.9 and Q.12

3.2 : Design Issues in Adhoc Wireless Network

Q.4 List the issues in adhoc wireless network.

Ans. : • Following are the main issues which affect design, implementation and performance of Adhoc networks.

1. Medium access scheme
2. Routing
3. Multicasting
4. Transport layer protocol
5. Pricing scheme
6. Security
7. Scalability
8. Quality of service provisioning
9. Address and service discovery
10. Energy management
11. Self organization
12. Deployment

Q.5 Explain medium access scheme for adhoc wireless network.

Ans. : Design goals of a MAC protocol for ad hoc wireless networks are : synchronization, distributed operation, throughput, hidden and exposed terminals, access delay, fairness, real time traffic support, resource reservation, adaptive rate control, use of directional antenna etc.

1. The operation of the protocol should be distributed.
2. The protocol should provide QoS support for real-time traffic.
3. The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.
4. The available bandwidth must be utilized efficiently.
5. The protocol should ensure fair allocation of bandwidth to nodes.
6. Control overhead must be kept as low as possible.
7. The protocol should minimize the effects of hidden and exposed terminal problems.
8. The protocol must be scalable to large networks.
9. It should have power control mechanisms.
10. The protocol should have mechanisms for adaptive data rate control.
11. It should try to use directional antennas.
12. The protocol should provide synchronization among nodes.

Q.6 Explain energy management and quality of service provisioning in adhoc network.

Ans. : Energy management : • Transmission power management : The radio frequency (RF) hardware design should ensure minimum power consumption.

- Battery energy management is aimed at extending the battery life.
- Processor power management : The CPU can be put into different power saving modes.
- Devices power management : Intelligent device management can reduce power consumption of a mobile node.

Quality of Service Provisioning

- QoS parameters based on different applications. QoS-aware routing uses QoS parameters to find a path.
- QoS framework is a complete system that aims at providing the promised services to each users.
- QoS provisioning often requires negotiation between host and network, call admission control, resource reservation, and priority scheduling of packets.
- As different applications have different requirements, the services required by them and the associated QoS parameters differ from application to application.
- Applications such as group communication in a conference hall require that the transmissions among nodes consume as mini-mum energy as possible. Hence battery life is the key QoS parameter here.

Q.7 What are the major challenges for routing protocol and requiremet in adhoc network.

Ans. : • Major challenges for routing protocol :

1. **Mobility :** Node mobility results in path breaks, packet collision, difficulty in resource reservation and transient loop.
2. **Bandwidth constraint :** Channel is shared by all nodes, so bandwidth available per wireless link depends on the number of nodes and traffic they handle.
3. **Error-prone and shared channel :** Bit error rate in wireless channel is very high.

4. **Location-dependent contention :** High contention for the channel results in a high number of collisions and subsequent wastage of bandwidth.

- Major requirements of a routing protocol in adhoc :
  a. Minimum route acquisition delay
  b. Quick route reconfiguration
  c. Loop-free routing
  d. Distributed routing approach
  e. Minimum control overhead
  f. Scalability
  g. Provisioning of QoS
  h. Support for time-sensitive traffic
  i. Security and privacy
- Routing's responsibilities are as follows :
  a. Exchanging the route information
  b. Finding a feasible path
  c. Gathering information about path breaks
  d. Mending the broken paths
  e. Utilizing minimum bandwidth

3.3 : Adhoc Network MAC Layer

Q.8 Describe design goals for adhoc network MAC layer.

Ans. :

1. Protocol operation should be distributed through all the nodes.
2. In real time traffic, the protocol should provide QoS.
3. The average delay for packet transmission should be as small as possible.
4. The bandwidth should be utilized efficiently.
5. Each node must have a fair share of the available bandwidth.
6. Control overhead should be minimized.
7. The hidden and exposed terminal problems should be minimized.
8. The protocol must be scalable to large networks.

9. Power control mechanisms are needed for efficient management of the energy consumption of the nodes.
10. Adaptive data rate control should be provided - a node controls the rate of outgoing traffic in relation also to the network load and to the status of the other nodes.
11. Directional antennas are encouraged, the advantages are reduced interference, increased spectrum reuse, and reduced power consumption.
12. Time synchronization between the nodes should be provided.

Q.9 Explain design issues for adhoc network MAC layer.

Ans. : • **Bandwidth efficiency** is defined at the ratio of the bandwidth used for actual data transmission to the total available bandwidth. The MAC protocol for ad-hoc networks should maximize it.

- **Quality of service** support is essential for time-critical applications. The MAC protocol for ad-hoc networks should consider the constraint of ad-hoc networks.
- **Synchronization** can be achieved by exchange of control packets. Some mechanism has to be found in order to provide synchronization among the nodes. Synchronization is important or regulating the bandwidth reservation.
- **Hidden and exposed terminal problems :** The reason for these two problems is the broadcast nature of the radio channel, namely, all the nodes within a node's transmission range receive its transmission.
- **Hidden terminal problem :** two nodes that are outside each-other's range perform simultaneous transmission to a node that is within the range of each of them, hence, there is a packet collision.
- **Exposed terminal problem :** the node is within the range ofa node that is transmitting, and it cannot transmit to any node.
- **Error-prone shared broadcast channel :** In radio transmission, a node can listen to all traffic within its range. Therefore, when there is communication going on no other node should transmit, otherwise there would be interferences. Access to the physical medium should be granted only if there is no session going on. Nodes will often compete for the channel at the same time; therefore, there is high probability of collisions. The aim of a MAC protocol will be to minimize them, while maintaining fairness.

- **No central coordination :** in adhoc networks, there is no central point of coordination due to the mobility of the nodes. Therefore, the control of the access to the channel must be distributed among them. In order for this to be coordinated, the nodes must exchange information. It is the responsibility of the MAC protocol to make sure this overhead is not a burden for the scarce bandwidth.
- **Mobility of nodes :** The mobility of the nodes is one of its key features. The QoS reservations or the exchanged information might become useless, due to node mobility. The MAC protocol must be such that mobility has as little influence as possible on the performance of the whole network.

Q.10 Explain design issues and design goal in Adhoc network MAC layer. ☞ **[SPPU : Dec.-22, End Sem, Marks 6]**

OR Comment on adhoc network MAC layer with design issues, design goal. ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : Refer Q.8 and Q.9.

3.4 : MACAW Protocol

Q.11 Write short note on MACAW protocol.

☞ **[SPPU : May-18,19, Dec.-19, End Sem, Marks 8]**

Ans. : • A Media Access Protocol for Wireless LANs is based on MACA (Multiple Access Collision Avoidance) Protocol.

- This protocol uses an RTS-CTS-DS-DATA-ACK message exchange and a backoff algorithm. MACAW protocol uses one more control packet RRTS (Request-for-Request-to-Send). This control packet is transmitted by a receiver on behalf of sender to save it from starvation.
- The design of MACAW is based on four observations :
  1. Relevant contention occurs at the receiver; sensing carrier at the sender (as in CSMA) is inappropriate.
  2. Congestion is location dependent.
  3. For fair allocation, collision (congestion) information must be shared among devices.
  4. Information related to contention period must be synchronized among devices to promote fair contention.

- Backoff algorithm : MACAW replaces BEB with MILD (multiplicative increase and linear decrease) to ensure that backoff interval grows a bit slowly and shrinks really slowly (linearly to minimum value). To enable better congestion detection, MACAW shares backoff timers among stations by putting this info in headers.
- Multiple stream model : MACAW uses separate queues for each stream in each node for increased fairness. In addition, each queue runs independent backoff algorithms. However, all stations attempting to communicate with the same receiver should use the same backoff value.
- Fig. Q.11.1 shows the operation of the MACAW protocol.

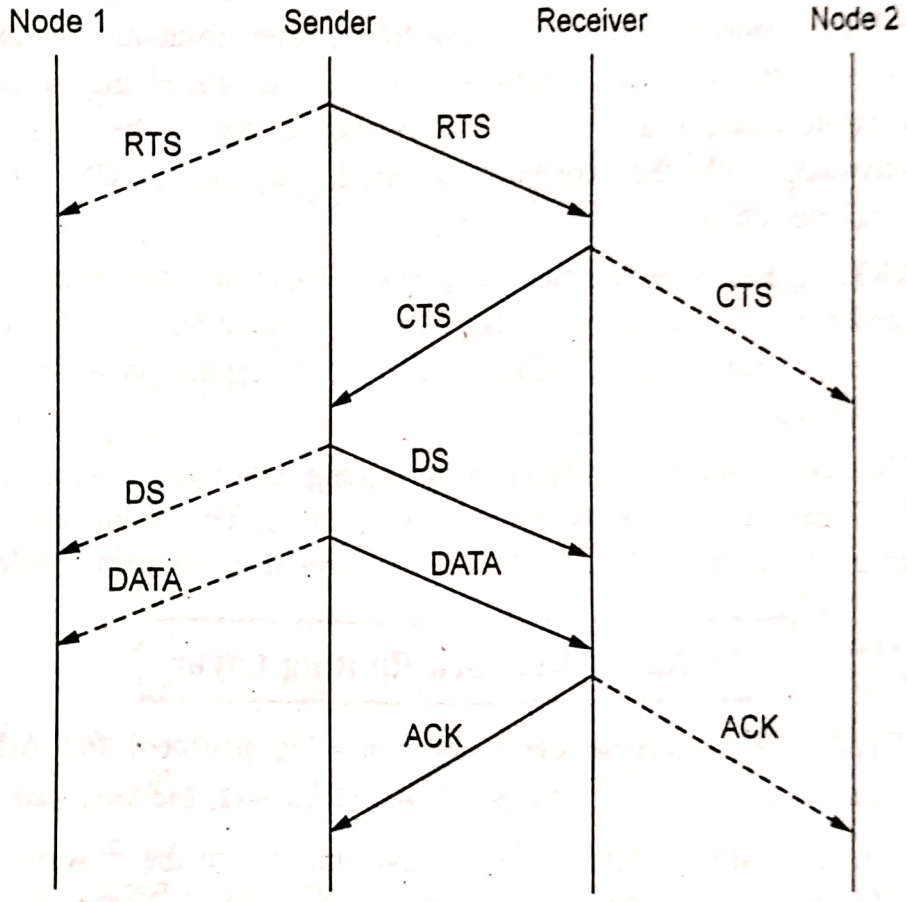


Fig. Q.11.1 Operation of the MACAW protocol

- When RTS transmitted by sender is overhead by node 1, it refrains from transmitting until sender receives the CTS.
- When CTS transmitted by receiver is heard by neighbor node 2, it defers its transmission until data packet is received by receiver.
- On receiving this CTS packet, sender immediately transmits the DS message carrying the expected duration of the data packet transmission.

- On hearing this packet, node 1 back off until the data packet is transmitted. Finally after receiving the data packet, receiver acknowledges the reception by sending sender an ACK packet.
- Basic exchange : MACAW replaces RTS-CTS-DATA to RTS-CTS-DS-DATA-ACK with the following extensions :

1. **ACK :** An extra ACK at the end ensures that errors can be recovered in the link layer, which is much faster than transport layer recovery. If an ACK is lost, next RTS can generate another ACK for the previous transmission.
2. **DS :** This signal ensures a 3-way handshake between sender and receiver (similar to TCP) so that everyone within hearing distance of the two stations know that a data transmission is about to happen. Without the DS packet, stations vying for the shared media cannot compete properly and one is always starved due to the lack of its knowledge of the contention period. In short, DS enables synchronization.
3. **RRTS :** RRTS is basically a proxy RTS, when the actual RTS sender is too far away to fight for the contention slot. However, there is one scenario where even RRTS cannot guarantee fair contention.
4. **Multicast :** Multicast is handled by sending data right away after the RTS packet, without waiting for CTS. It suffers from the same problems as in CSMA, but the authors leave it as an open challenge.

3.5 : Adhoc Network Routing Layer

Q.12 Explain the issues in designing a routing protocol for Adhoc wireless network. ☞ **[SPPU : May-19, June-22, End Sem, Marks 9]**

Ans. : 1. Mobility : Adhoc is highly dynamic due to the movement of nodes. The node movement causes frequent path breaks. The path repair in wired network has slow convergence.

2. **Bandwidth constraint :** Wireless has less bandwidth due to the limited radio band. Wireless has less bandwidth due to the limited radio band. Less data rate are difficult to maintain topology information. Frequent change of topology causes more overhead of topology maintenance. For that purpose, bandwidth optimization and design topology update mechanism with less overhead is required.

3. **Error-prone shared broadcast radio channel :** Wireless links have time varying characteristics in terms of link capacity and link-error probability. So it is necessary to interact with MAC layer to find better-quality link. Hidden terminal problem causes packet collision.
4. **Resource constraints :** Because of limited battery life and limited processing power, necessary to optimally manage these resources.

Q.13 Explain DSDV and AODV protocol in detail.

☞ [SPPU : May-19, Dec.-19, 22, End Sem, Marks 9]

OR Explain the connection establishment and data transfer phase in the following routing protocols with suitable diagram.

i) AODV ii) DSDV ☞ [SPPU : Dec.-18, End Sem, Marks 8]

Ans. : i) AODV :

- Ad-hoc on demand distance vector routing (AODV) is a stateless on-demand routing protocol. Two major functions of AODV protocols are: route discovery and route maintenance. The performance of protocol is improved by keeping the routing information in each node.
- AODV is a distance vector routing protocol, which means routing decisions will be taken depending on the number of hops to destination. A particularity of this network is to support both multicast and unicast routing.

Algorithm

- When a route is needed to some destination, the protocol starts route discovery. Then the source node sends route request message (RREQ) to its neighboring nodes (flooding). And if those nodes do not have any information about the destination node, they will send the message to all its neighboring nodes and so on.
- If any neighbor node has the information about the destination node, the node sends route reply message to the route request message initiator. The path is recorded in the intermediate nodes. This path identifies the route and is called the reverse path.
- Since each node forwards route request message to all of its neighbors, more than one copy of the original route request message can arrive at a node. A unique ID is assigned, when a route request message is created. When a node received, it will check this ID and the address of the initiator and discarded the message if it had already processed that request.

- Node that has information about the path to the destination sends route reply message to the neighbor from which it has received route request message. This neighbor does the same. Due to the reverse path it can be possible. Then the route reply (RREP) message travels back using reverse path. When a route reply message reaches the initiator the route is ready and the initiator can start sending data packets.
- When a node detects the link failure to its next hop, it propagates a link failure notification message, Route-Error (RERR) to each of its active upstream neighbours to inform them to erase that part of the route. These nodes in turn propagate the link failure notification message to their upstream neighbours and so on, until the source node is reached.
- When the source node receives the link failure notification message, it will re-initiate a route discovery for the destination if a route is still needed. A new destination sequence number is used to prevent routing loops formed by the entangling of stale and newly established paths.
- AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information.

Route maintenance

- Another part of this algorithm is the **route maintenance.**
- While a neighbour is no longer available, if it was a hop for a route, this route is not valid anymore.
- AODV uses HELLO packets on a regular basis to check if they are active neighbours. Active neighbours are the ones used during a previous route discovery process. If there is no response to the HELLO packet sent to a node, then, the originator deletes all associated routes in its routing table.
- HELLO packets are similar to ping requests. While transmitting, if a link is broken (a station did not receive acknowledgment from the layer 2), a ROUTE ERROR packet is unicast to all previous forwarders and to the sender of the packet

Illustration

- In the example illustrated in Fig. Q.13.1, node-A needs to send a packet to node-I. A route request () packet will be generated and sent to B and D.
- B and D add A in their routing table, as a reverse route and forward a route request (RREQ) packet to their neighbours.

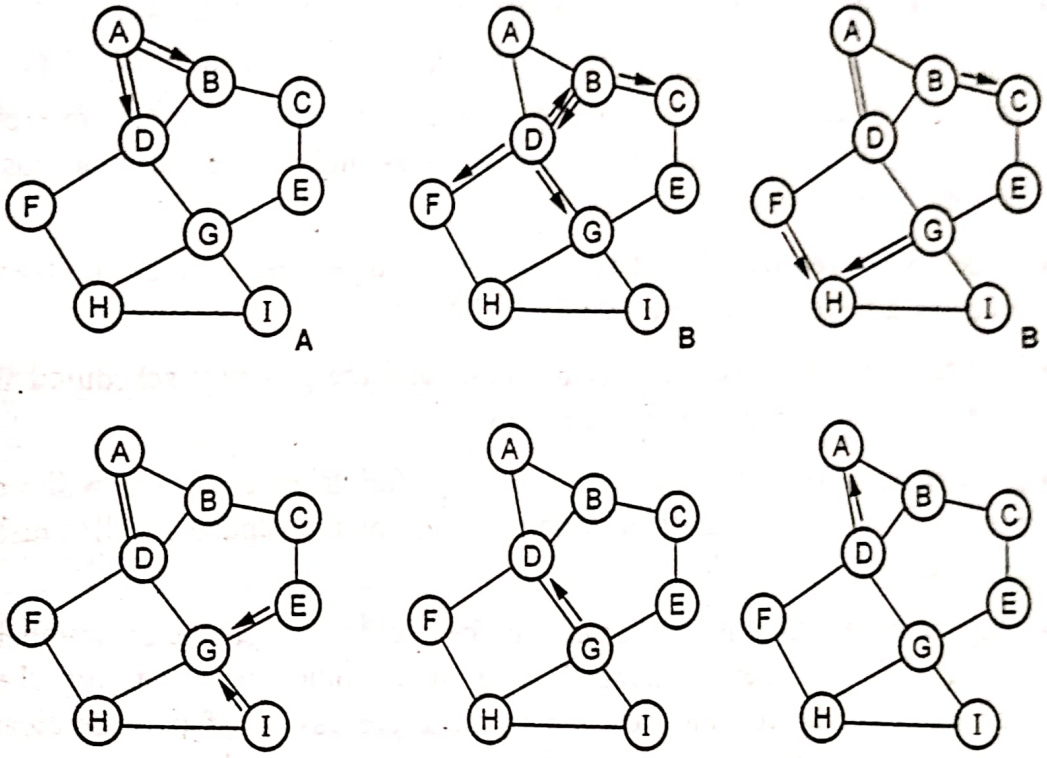


Fig. Q.13.1 AODV protocol

- B and D ignored the packet they exchanged each others (as duplicates). The forwarding process continues while no route is known.
- Once node-I receives the route request (RREQ) from G, it generates then a route reply (RREP) packet and sends it to the node it received from. Duplicate packets continue to be ignored while the route reply (RREP) packet goes on the shortest way to A, using previously established reverse routes.
- The reverse routes created by the other nodes that have not been used for the route reply (RREP) are deleted after a delay. G and D will add the route to I once they receive the route reply (RREP) packet.

ii) DSDV :

- DSDV was one of the first proactive routing protocols available for Ad-hoc networks.

Algorithm

- DSDV is based on the Bellman-Ford algorithm.
- With DSDV, each routing table will contain all available destinations, with the associated next hop, the associated metric (numbers of hops) and a sequence number originated by the destination node.

- Another classification can be done based on the use of temporal information for routing. A third option is to classify such protocols based on the routing topology. Finally, they can be also classified based on the utilization of specific resources.
- Ad-hoc routing protocols can be classified into three major groups based on the routing strategy.
  1. Pro-active or table driven,
  2. Reactive or on-demand,
  3. Hybrid
- In proactive routing protocols routes to a destination are determined when a node joins the networks or changes its location and are maintained by periodic route updates.
- In reactive routing protocols routes are discovered when needed and expire after a certain period.
- Hybrid routing protocols combine the features of both proactive and reactive routing protocols to scale well with network size and node density. Each of these groups can be further divided into two sub-groups based on the routing structure: flat and hierarchical.
- In flat routing protocols nodes are addressed by a flat addressing scheme and each node plays an equal role in routing. On the other hand, different nodes have different routing responsibilities in hierarchical routing protocols. These protocols require a hierarchical addressing system to address the nodes.
- Classification of ad-hoc routing protocols based on routing strategy and network structure.
- Proactive routing protocols require each node to maintain up-to-date routing information to every other node in the network. The various routing protocols in this group differ in how topology changes are detected, how routing information is updated and what sort of routing information is maintained at each node.
- These routing protocols are based on the working principles of two popular routing algorithms used in wired networks. They are known as link-state routing and distance vector routing.
- In the link-state approach, each node maintains at least a partial view of the whole network topology. To achieve this, each node periodically broadcasts link-state information such as link activity and delay of its outgoing links to all other nodes using network-wide flooding.

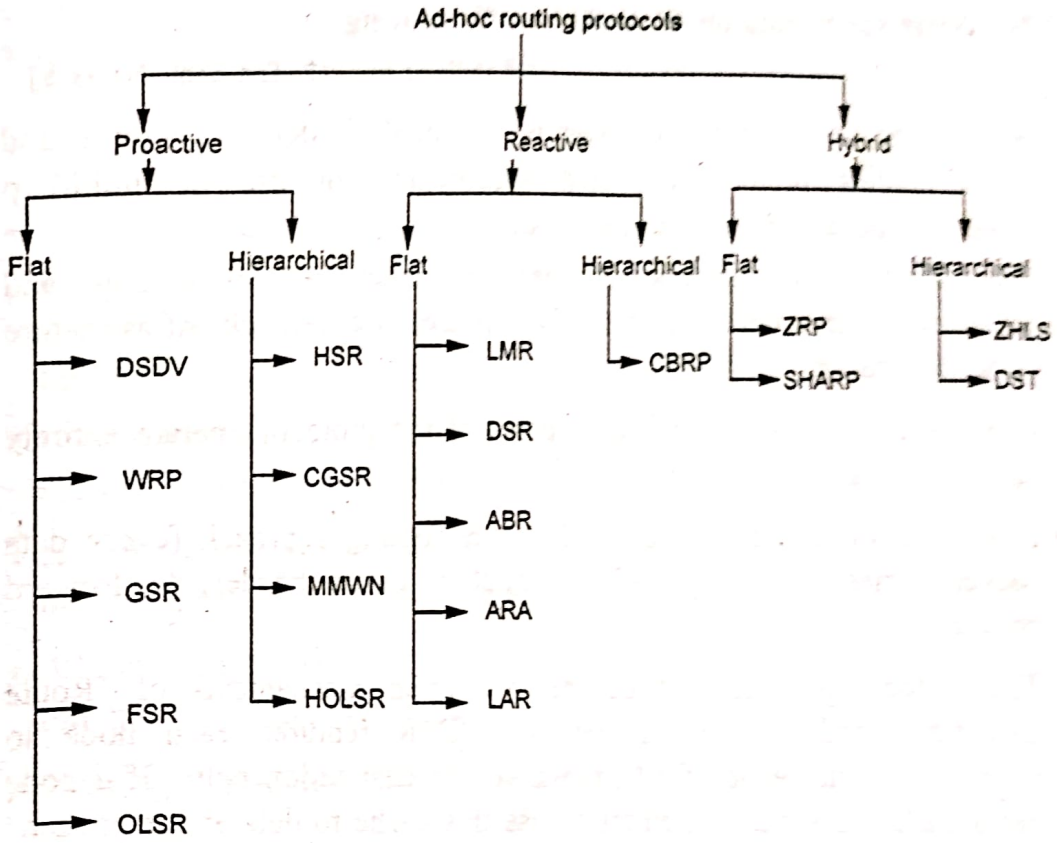


Fig. Q.15.1 Classification of routing protocols

- When a node receives this information, it updates its view of the network topology and applies a shortest-path algorithm to choose the next hop for each destination.
- The welknown routing protocol OSPF is an example of a link-state routing protocol. On the other hand, each node in distance vector routing periodically monitors the cost of its outgoing links and sends its routing table information to all neighbours.
- The cost can be measured in terms of the number of hops or time delay or other metrics. Each entry in the routing table contains at least the ID of a destination, the ID of the next hop neighbour through which the destination can be reached at minimum cost, and the cost to reach the destination.
- Thus, through periodic monitoring of outgoing links, and dissemination of the routing table information, each node maintains an estimate of the shortest distance to every node in the network.
- Distributed Bellman Ford and RIP is classic examples of distance vector routing algorithms.

Q.16 Write short note on dynamic source routing.

☞ [SPPU : Dec.-19, End Sem, Marks 8]

Ans. : • The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.

- DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.
- It is a reactive protocol and all aspects of the protocol operate entirely on-demand basis.
- DSR protocol uses the concept of source routing approach (every data packet carries the whole path information in its header) to forward packets.
- The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance". DSR requires each node to maintain a route cache of all known self to destination pairs. If a node has a packet to send, it attempts to use this cache to deliver the packet.
- In source routing technique the sender of a packet determines the complete sequence of nodes through which, the packets are forwarded. Otherwise, it will initiate a route discovery phase by flooding a Route REQuest (RREQ) message.
- The RREQ message carries the sequence of hops it passed through in the message header. Any nodes that have received the same RREQ message will not broadcast it again.
- Once an RREQ message reaches the destination node, the destination node will reply with a Route REPly (RREP) packet to the source. The RREP packet will carry the path information obtained from the RREQ packet.
- When the RREP packet traverses backward to the source, the source and all traversed nodes will know the route to the destination. Each node uses a route cache to record the complete route to desired destinations.
- The advantage of source routing is: intermediate nodes do not need to maintain up to date routing information in order to route the packets they forward.

- Route failure is detected by the failure of message transmissions. Such a failure will initiate a route error message to the source. When the source and the intermediate nodes receive the error message, they will erase all the paths that use the broken link from their route cache.
- If the destination does not exist in the cache, then a route discovery phase is initiated to discover a route to destination, by sending a route request (RREQ). The RREQ request includes the destination address, source address and a unique identification number.
- If a route is available from the route cache, but is not valid any more, a route maintenance procedure may be initiated.
- A node processes the route request packet only if it has not previously processes the packet and its address is not present in the route cache.
- A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.

Advantages and Disadvantages of DSR

Advantages

1. DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.
2. DSR is simple and loop-free.

Disadvantages

1. The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link.
2. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
3. Considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.
4. The loop free feature may waste bandwidth if every data packet carries the entire path information.

Q.17 Explain characteristics of AODV routing algorithm protocol.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. :

1. AODV support unicast, broadcast and multicast communication.
2. AODV performs on-demand route establishment with small delay.
3. Multicast trees connecting group members maintained for lifetime of multicast group.
4. Link breakages in active routes efficiently repaired.
5. All routes are loop-free through use of sequence numbers.
6. Use of Sequence numbers to track accuracy of information.
7. Only keeps track of next hop for a route instead of the entire route.
8. Use of periodic HELLO messages to track neighbors.

3.6 : Adhoc Transport Layer

Q.18 Explain issues in designing a transport layer protocol for adhoc wireless networks.

Ans. : • **Induced traffic :** Ad hoc wireless networks use multi-hop radio relaying, and a link-level transmission affects neighbor nodes of both sender and receiver of the link. This induced traffic affects throughput of the transport layer protocol.

- **Induced throughput unfairness :** Some MAC protocols, like IEEE 802.11 DCF, may add throughput unfairness to the transport layer. A transport layer protocol needs to take this into account to provide a fair throughput for contesting flows.
- **Separation of congestion control, reliability, and flow control :** The throughput may be improved if the transport controls protocol handles congestion control, reliability and flow control separately. Congestion is usually a local activity that affects only neighboring nodes while reliability and flow control are end-to-end issues. Separation of these should not produce significant control overhead.
- **Misinterpretation of congestion :** Commonly used methods of detecting the congestion by measuring packet loss and retransmission timeout are not suitable for ad hoc wireless networks. Packet loss occurs in wireless networks relatively frequently for several reasons. Bit error rates are much higher than in wired networks and path breaks

occur frequently because nodes are constantly moving and they may fail e.g. after draining a battery. Thus, a better method for detecting congestion must be used.

- **Completely decoupled transport layer :** In wired networks, transport layer is usually almost completely decoupled from lower network layers. In wireless networks, cross-layer interaction would help transport layer protocol to adapt to the changes in the network
- **Power and bandwidth constraints :** Ad hoc wireless networks are constrained by available power and bandwidth. These constraints affect the performance of transport layer protocol.
- **Dynamic topology :** Topology of ad hoc wireless network may change rabidly and this leads to path breaks and partitioning of network. A transport layer protocol should be able to adapt to these changes.

Q.19 List design goals of a transport layer protocol for adhoc wireless networks

Ans. :

1. Per connection throughput should be maximum.
2. It should provide throughput fairness across contending flows.
3. It should incur minimum connection set up and connection maintenance overheads.
4. It should have mechanisms for congestion control and flow control in the network.
5. It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
6. It should be able to adapt to the dynamics of the network such as rapid changes in topology.
7. Bandwidth must be used efficiently.
8. It should be aware of resource constraints such as battery power and buffer sizes and make efficient use of them.
9. It should make use of information from the lower layers for improving network throughput.
10. Cross-layer interaction framework is defined properly.
11. End-to-End Semantics should be maintained.

Q.20 Given classification of transport layer solutions in adhoc wireless network. Explain operation of TCP-F.

☞ **[SPPU : Dec.-18, End Sem, Marks 8]**

Ans. : Fig. Q.20.1 shows a classification tree the transport layer protocols. The solutions for TCP over ad hoc wireless networks can further be classified into split approaches and end-to-end approaches.

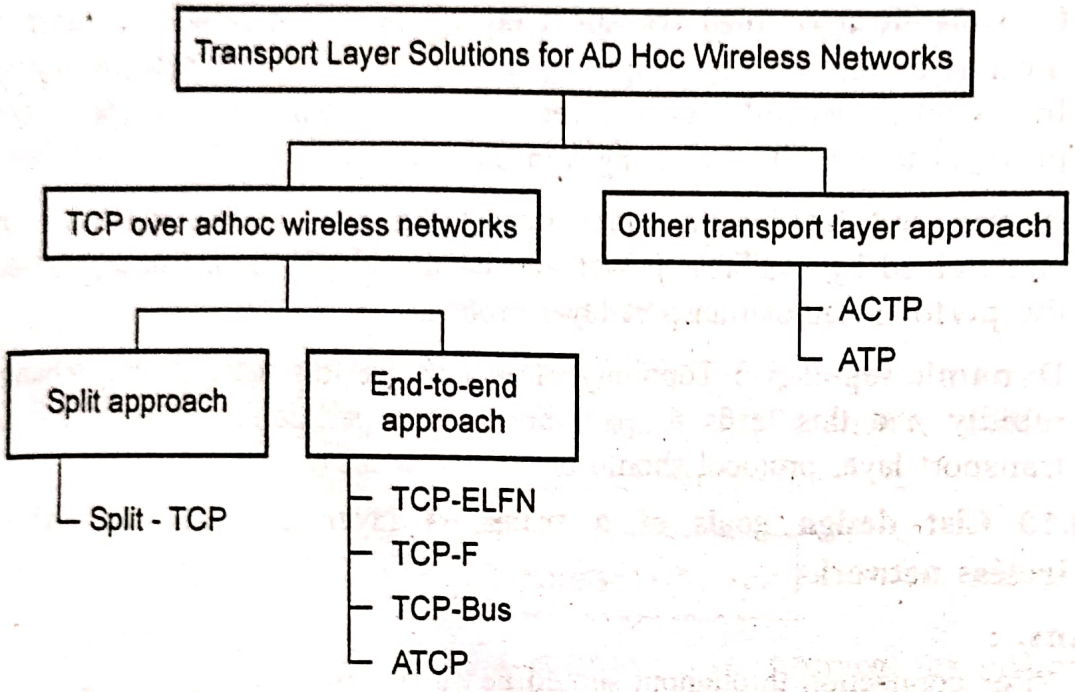


Fig. Q.20.1 Classification of transport layer solutions

Also Refer Q.21

3.7 : TCP Over Adhoc Wireless Network

Q.21 Explain operation of TCP-F. ☞ **[SPPU : May-18, End Sem, Marks 8]**

Ans. : • TCP-F requires the following to enhance performance :

a. Support of reliable data-link layer protocols;

b. Routing support to inform the TCP sender about path breaks;

c. Routing protocol is expected to repair the broken path within a reasonable time.

• The aim of TCP-F is to minimize the throughput degradation resulting from path breaks. Fig. Q.21.1 shows link break in ad-hoc network.

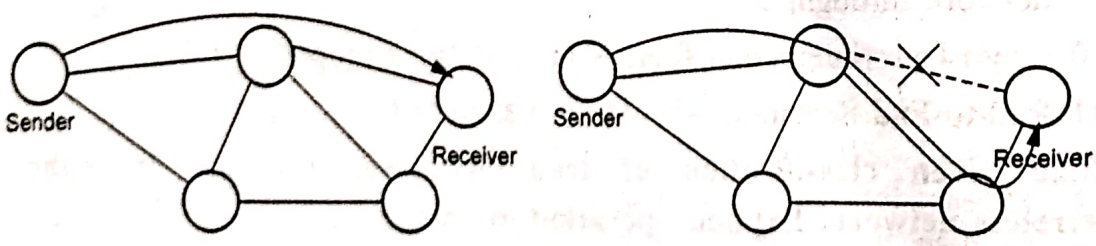


Fig. Q.21.1 Link break in ad-hoc network

- In TCP-F an intermediate node upon detection of the link break, following things occurs :
  a. Obtains information from TCP-F sender's packets routed via this node;
  b. Generates a route failure notification (RFN) packet;
  c. Routes this packet to the TCP-F sender;
  d. Does not forward any packet from this connection;
  e. Updates its routing table;
  f. Stores information about generation of a RFN packet.
- Any intermediate node that forwards the RFN packet :
  a. If this node has an alternative route to destination then discards the RFN packet and uses this path to forward other packets. This allows to reduce an overhead involved in route re-establishment.
  b. If this node does not alternate route to destination then updates its routing table and forwards the RFN packet to the source.
- When TCP-F sender receives the RFN packet it enters the so-called snooze state then stops sending packet to the destination; cancels all the timers; freezes the congestion window and sets up a route failure timer. When failure timer expires TCP-F enters the connected state.
- If the broken links rejoins or intermediate node obtains a new path to destination then route reestablishment notification (RRN) is sent to TCP-F sender.
- Fig. Q.21.2 shows operation of TCP-F.

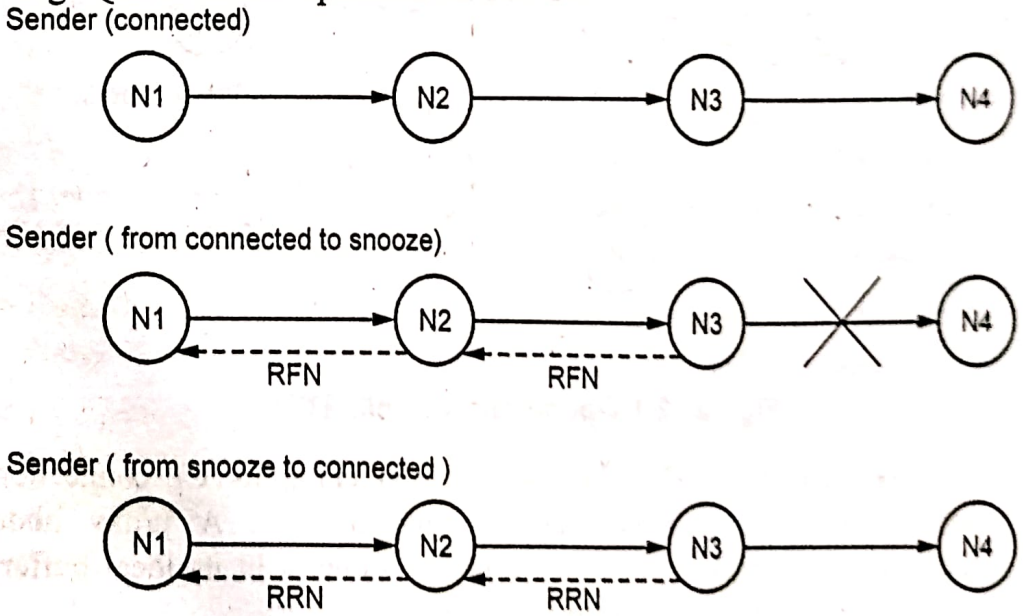


Fig. Q.21.2 Operation of TCP-F

- When the sender receives RRN packet :
  a. Reactivates all timers and congestion window assuming that the network is back;
  b. Starts transmitting data available in the buffer;
  c. Takes care of packets lost due to path break.

Q.22 Explain operations of split TCP. Explain its advantages and disadvantages. ☞ **[SPPU : May-19, End Sem, Marks 8]**

Ans. : • Split-TCP provides a unique solution to channel capture problem by splitting the transport layer objectives into congestion control and end-to-end reliability.

• Fig. Q.22.1 shows operations of split TCP.

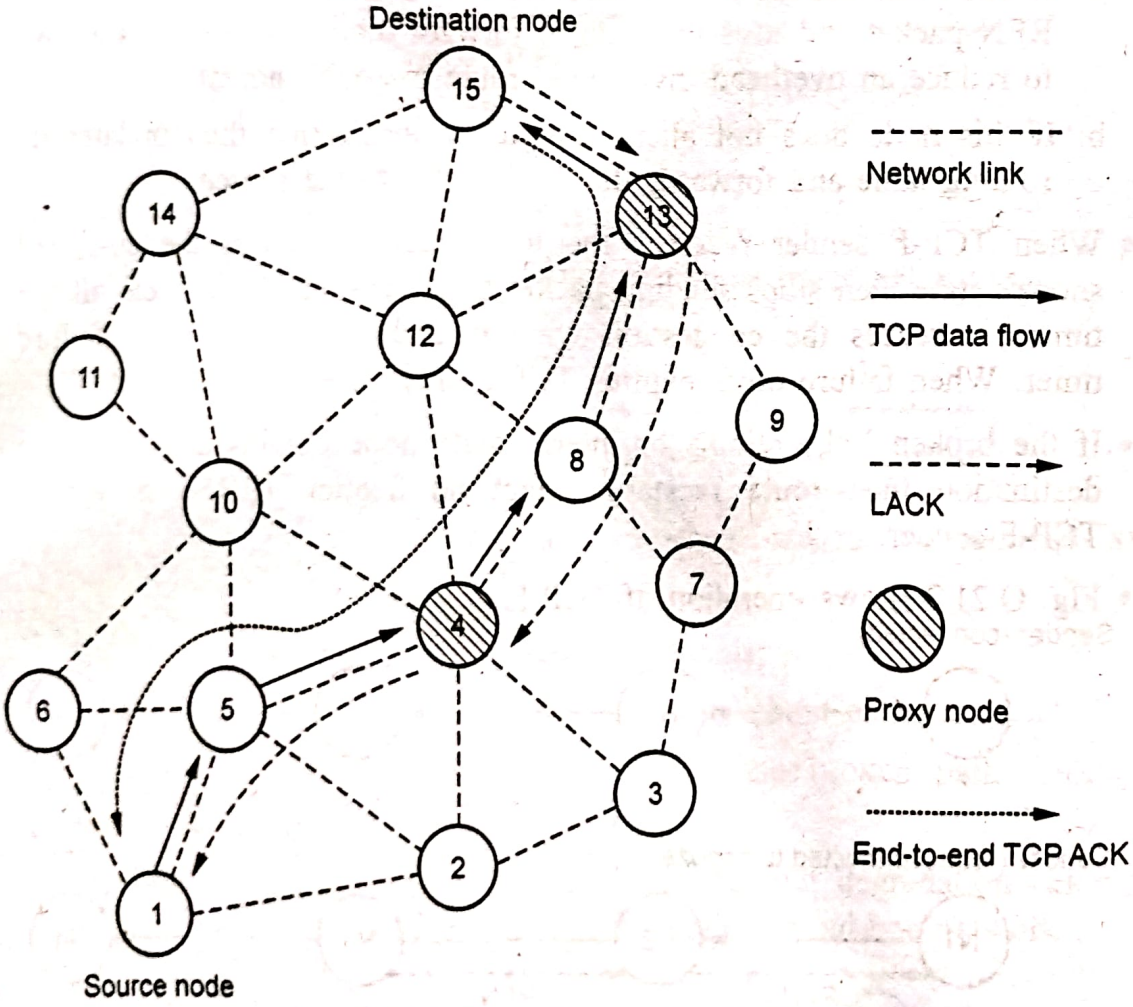


Fig. Q.22.1 Operations of split TCP

- The operation of split-TCP where a three segment split-TCP connection exists between source node and destination node. A proxy node receives the TCP packets, reads its contents, stores it in its local buffer, and sends an acknowledgment to the source.

- This acknowledgment called local acknowledgment (LACK) does not guarantee end-to-end delivery. The responsibility of further delivery of packets is assigned to the proxy node.
- A proxy node clears a buffered packet once it receives LACK from the immediate successor proxy node for that packet.
- Split-TCP maintains the end-to-end acknowledgment mechanism intact, irrespective of the addition of zone-wise LACKs. The source node clears the buffered packets only after receiving the end-to-end acknowledgment for those packets.
- Source Node initiates a TCP session to destination node. Node 4 and node 13 are chosen as proxy nodes. The number of proxy nodes in a TCP session is determined by the length of the path between source and destination nodes.
- Based on a distributed algorithm, the intermediate nodes that receive TCP packets determine whether to act as a proxy node or just as a simple forwarding node.
- In Fig. Q.22.1 the path between node 1 and node 4 is the first zone (segment), the path between nodes 4 and 13 is the second zone (segment), and the last zone is between node 13 and 15.
- The proxy node 4, upon receipt of each TCP packet from source node 1, acknowledges it with a LACK packet, and buffers the received packets. This buffered packet is forwarded to the next proxy node (in this case, node 13) at a transmission rate proportional to the arrival of LACKs from the next proxy node or destination.
- The transmission control window at the TCP sender is also split into two windows, that is, the congestion window and the end-to-end window.
- The congestion window changes according to the rate of arrival of LACKs from the next proxy node and the end-to-end window is updated based on the arrival of end-to-end ACKs.
- Both these windows are updated as per traditional TCP except that the congestion window should stay within the end-to-end window.
- In addition to these transmission windows at the TCP sender, every proxy node maintains a congestion window that governs the segment level transmission rate.

Advantages

1. Improved throughput
2. Improved throughput fairness
3. Lessened impact of mobility

Disadvantages

1. It requires modifications to TCP protocol.
2. The end-to-end connection handling of traditional TCP is violated.
3. The failure of proxy nodes can lead to throughput degradation.

Adhoc TCP :

- Adhoc TCP (ATCP) relies on a network layer feedback to make the TCP sender aware of the status of the network path. ATCP takes advantage of explicit congestion notification (ECN) flags and ICMP destination unreachable (DUR) messages to detect network congestion and path breaks.
- ATCP is not a full replacement to the TCP, instead it operates between the TCP and the network layer. Thus, ATCP is fully compatible with the traditional TCP and the ATCP support is only required for the sender.
- When packet loss is detected or packets arrive out-of-order to the destination, ATCP simply retransmits missing packets without invoking congestion control mechanism. This provides a performance advantage against traditional TCP that invokes congestion control every time the packet loss or out-of-order packets are detected.
- When the ATCP sender receives ECN message, it moves to the congested state where it lets TCP invoke congestion control normally.
- When DUR packets are received, ATCP moves in to disconnect state where it ceases to send packets. After the connection is re-established, ATCP sets the size of the congestion window to one in order to make TCP to determine optimal congestion window size for a new connection.

Advantages

1. Compatible with traditional TCP;
2. Maintains the end-to-end semantics of TCP;

Disadvantages

1. Requires support from routing protocol (route changes, partition detection);
2. Requires changes to interface functions

Q.23 Write short note on TCP-Bus.

Ans. : • Characteristics :

a. Protocol tries to notify the source about the path breaks using the feedback info;

b. This protocol is more dependent on routing protocol compared to TCP-F and TCP-ELFN.

- TCP-BuS was proposed for usage with Associativity-Based Routing (ABR) and uses localized query (LQ) message of ABR; REPLY message of ABR.
- Both these messages are modified to carry TCP connection and segment information. Fig. Q.23.1 shows basic definitions for TCP-BuS protocol.

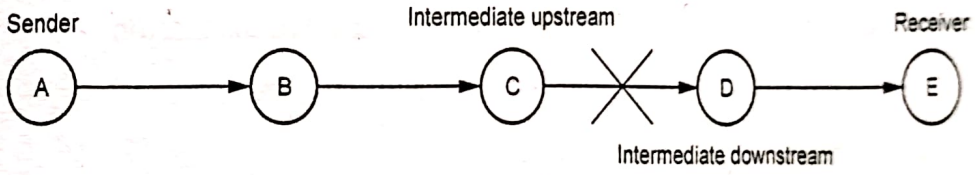


Fig. Q.23.1 : Basic definitions for TCP-BuS protocol

- When a link break is detected, **intermediate downstream node** generates a route notification (RN) message to TCP-BuS receiver. Route notification includes the sequence number of packet belonging to that flow in the head of its queue. All packets belonging to this flow are discarded at all intermediate nodes that forward RN.
- When a link break is detected, **intermediate upstream node :**

a. Generate explicit route disconnection notification (ERDN);

b. When ERDN is received by the sender, it stops sending and freezes timers CW;

c. All packets in transit nodes are buffered, till new partial path is found by source of ERDN;

d. Tries to find a new (partial) route to the TCP-BuS receiver;

e. If it finds, explicit route successful notification packet (ERSN) to the sender is sent.

- Fig. Q.23.2 shows operation of TCP-BuS connection.

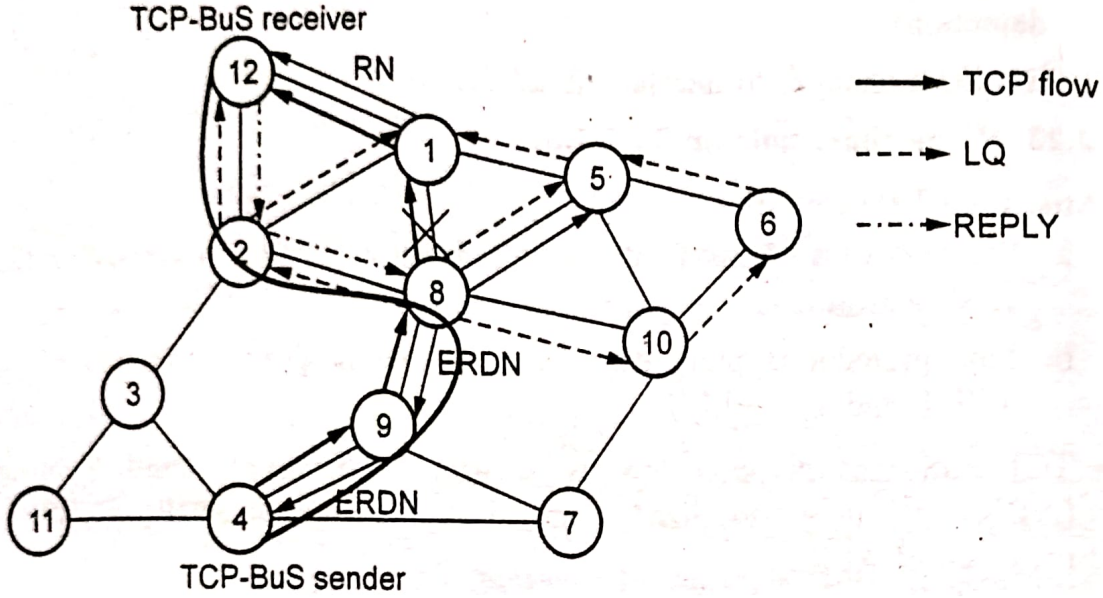


Fig. Q.23.2 : Operation of TCP-BuS connection

Advantages

1. Performance improvement and avoidance of fast retransmission.
2. Use on-demand routing protocol.

Disadvantages

i. Increased dependency on the routing protocol and the buffering at the intermediate nodes.

ii. The failure of intermediate nodes may lead to loss of packets.

iii. The dependency of TCP-BuS on the routing protocol many degrade its performance.

3.8 : Wireless Sensor Network

Q.24 What are the design issues in wireless sensor network ?

☞ **[SPPU : Dec.-18, End Sem, Marks 8]**

Ans. : Design issues in WSN are as follows :

1. **Fault tolerance :** Possibility of node failure and change of topology of network is quite high in case of WSN. Hence the designer of network should make the network robust and reliable even in case of node failures and topology changes.

2. **Scalability :** The design of WSN should support addition of new nodes any time and also the design should support large number of nodes.
3. **Environment :** The design of WSN should be such that WSN should be able to survive regardless of the conditions in which WSN s deployed.
4. **Heterogeneity support :** The protocols designed for WSN should support different kinds of sensor nodes and also be able to support variety of applications.
5. **Autonomous operations :** The WSN should be able to organize , reorganize and operate autonomously because sometimes WSN deployed in places where human habitation is not possible.
6. **Limited memory and processing capability :** The sensor nodes have very limited memory, power and processing capabilities , so all designs of WSN should not be demanding in terms of processing requirements or memory requirements

Q.25 Write a short note on wireless sensor network.

☞ **[SPPU : May-18, End Sem, Marks 4]**

Ans. : • A wireless sensor network is a collection of nodes organized into a co-operative network. Each node consists of processing capability, may contain multiple types of memory, have a RF transceiver and a power source and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad-hoc fashion.

- WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.
- A communication network is composed of nodes, each of which has computing power and can transmit and receive messages over communication links, wireless or cabled.
- The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation and traffic control.

- Possible applications
  1. **Military** : Battlefield surveillance, biological attack detection, targeting.
  2. **Ecological** : Fire detection, flood detection, agricultural uses.
  3. **Health related** : Human physiological data monitoring.
  4. **Miscellaneous** : Car theft detection, inventory control, home applications.
- Sensor network development rely on advances in sensing, communication and computing. To manage scarce WSN resources adequately, routing protocols for WENs need to be energy-aware.
- Data-centric routing and in-network processing are important concepts that are associated intrinsically with sensor networks. The end-to-end routing schemes that have been proposed in the literature for mobile ad-hoc networks are not appropriate WSNs; data-centric technologies are needed that perform in-network aggregation of data to yield energy efficient dissemination.
- A sensor node typically has embedded processing capabilities and onboard storage; the node can have one or more sensors operating in the acoustic, seismic, radio (radar), infrared, optical, magnetic and chemical or biological domains. The node has communication interfaces, typically wireless links, to neighbouring domains. The sensor node also often has location and positioning knowledge that is acquired through a Global Positioning System (GPS) or local positioning algorithm.
- Sensor nodes are scattered in a special domain called a sensor field. Each of the distributed sensor nodes typically has the capability to collect data, analyze them and route them to a designated sink point.

Q.26 Describe each component in sensor node architecture.

☞ **[SPPU : May-18, End Sem, Marks 10]**

Ans. : Some of the **characteristic features of sensor networks** include the following :

- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes are limited in power, computational capacities and memory.

- Sensor nodes may not have global identification because of the large amount of overhead and the large number of sensors.
- Sensor networks require sensing systems that are long-lived and environmentally resilient. Unattended, self-powered low-duty-cycle systems are typical.
- Fig. Q.26.1 shows a typical sensing node. The components of a sensing node include the following :

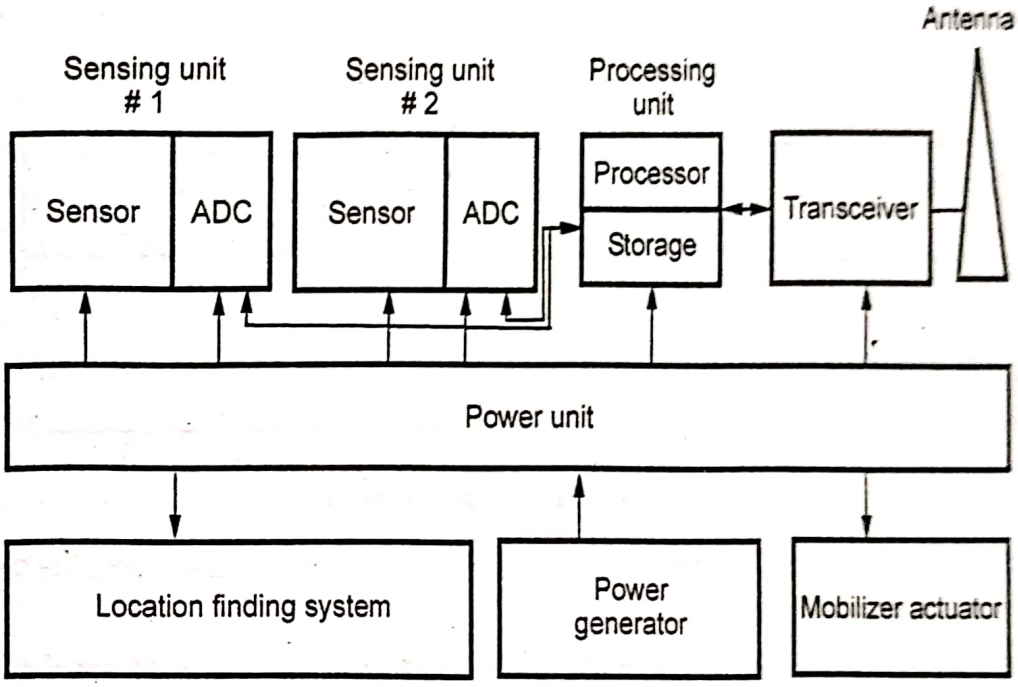


Fig. Q.26.1 Typical sensing node

1. A sensing and actuation unit (single element or array)
2. A processing unit
3. A communication unit
4. A power unit
5. Other application-dependent units.

- Power consumption is often an issue that needs to be taken into account as a design constraint. In most instances, communication circuitry and antennas are the primary elements that draw most of the energy. Sensors are either passive or active devices. Passive sensors in element form include seismic, acoustic, strain, humidity and temperature-measuring devices. Passive sensors in array form include optical, and biochemical measuring devices. Passive sensors tend to be

low-energy devices. Active sensors include radar and sonar; these tend to be high-energy systems. Basic sensor node comprises five main components.

1. Controller
2. Memory
3. Sensors and actuators
4. Communication
5. Power supply.

- Fig. Q.26.2 shows the overview of main sensor node hardware components.

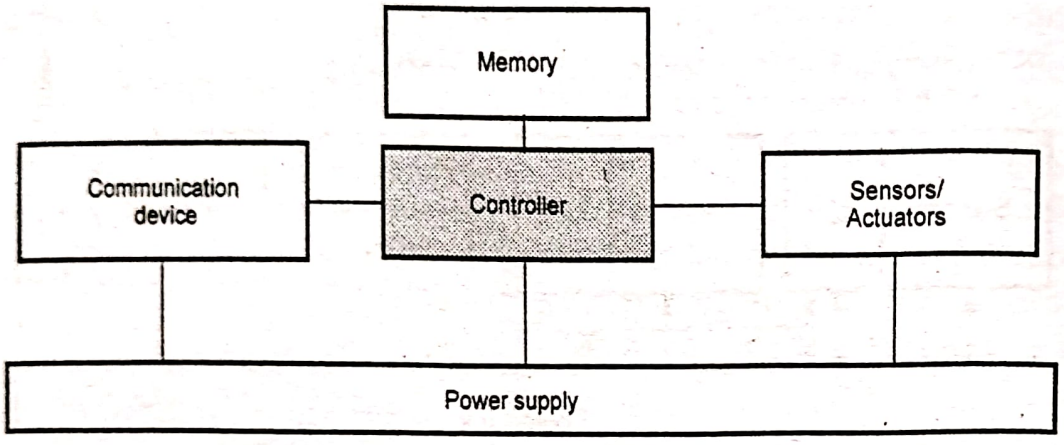


Fig. Q.26.2 Main sensor node

1. **Controller :** A controller to process all the relevant data, capable of executing arbitrary code.
2. **Memory :** Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.
3. **Sensors and actuators :** The actual interface to the physical world, the device that can observe or control physical parameters of the environment.
4. **Communication :** Turning nodes into a network requires a device for sending and receiving information over a wireless channel.
5. **Power supply :** Some forms of batteries are necessary to provide energy.

The energy consumed by an interface depends on its operating mode

1. **Sleep Mode :** An interface can neither transmit nor receive. It is very low energy consumption.
2. **Idle Mode :** An interface can transmit or receive data at any time. it consumes more energy than it does in the sleep state.

3. **Receive Mode and Transmit Mode :** The energy consumption is of the same order of magnitude than idle state. Transmitting requires more energy than receiving, but the difference is generally less than a factor of two.

3.9 : Sensor Network Architecture

Q.27 What are the elements of sensor networks? Differentiate the MAC protocol of WSN from traditional wireless MAC protocol.

☞ [SPPU : Dec.-18,19 End Sem, Marks 8]

Ans. : • Sensor network architectures uses two main concept **source and sink.**

• **Source** provides information to network and **sink** receive information from network. Sink receives the information from source entity. Example of source is sensor node acts as source entity. Examples of sink are sensor network, PDA and entity outside home network. Fig. Q.27.1 shows three types of sink.

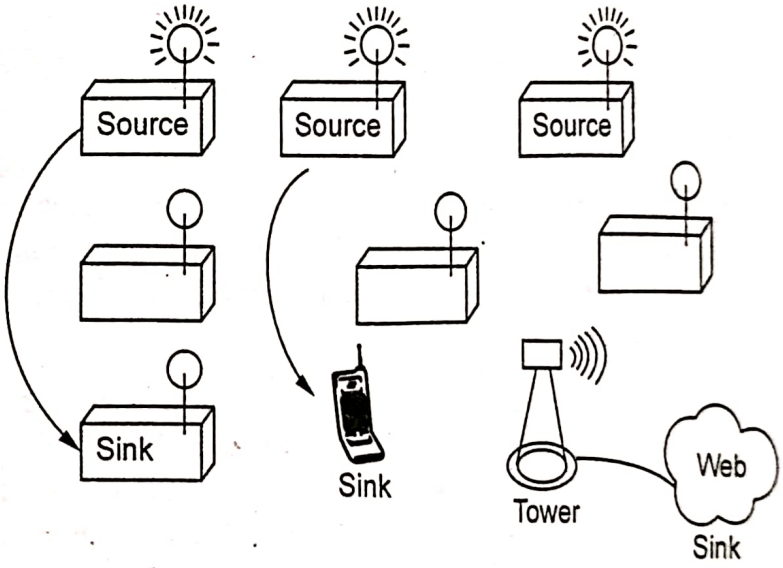


Fig. Q.27.1 Types of sink

• If direct communication is not possible because of distance limit or obstacles, then multihop communication method is used. Multihop communication uses store and forward fashion. Node has to receive a packet properly before it can forward next entity.

• Proper placing of intermediate sensor node is necessary. Fig. Q.27.2 shows multihop communication network.

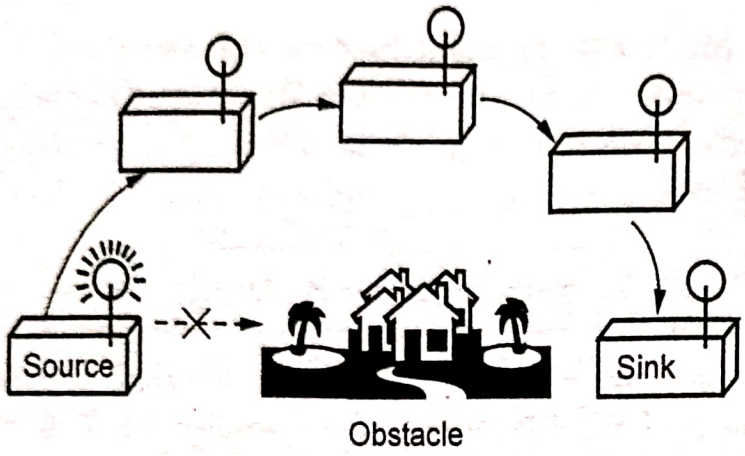


Fig. Q.27.2 Multihop communication

- Traditional transport protocols such as UDP and TCP cannot be directly implemented in sensor networks because if a sensor node is far away from the sink then the flow and congestion control mechanism cannot be applied for those nodes.
- UDP on the other hand has a reputation of not providing reliable data delivery and has no congestion or flow control mechanisms which are needed for sensor networks.
- S-MAC is a Medium-Access Control (MAC) protocol designed for wireless sensor networks.
- A network of these devices will collaborate for a common application such as environmental monitoring. We expect sensor networks to be deployed in an ad hoc fashion, with individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected.
- These characteristics of sensor networks and applications motivate a MAC that is different from traditional wireless MACs such as IEEE 802.11 in almost every way : energy conservation and self-configuration are primary goals, while per-node fairness and latency are less important.
- S-MAC uses three novel techniques to reduce energy consumption and support self-configuration. To reduce energy consumption in listening to an idle channel, nodes periodically sleep. Neighboring nodes form virtual clusters to auto-synchronize on sleep schedules.
- Inspired by PAMAS, S-MAC also sets the radio to sleep during transmissions of other nodes. Unlike PAMAS, it only uses in-channel signaling.

- Finally, S-MAC applies message passing to reduce contention latency for sensor-network applications that require store-and-forward processing as data move through the network.

Q.28 Write a short note on sensor network with classification of protocols used. ☞ [SPPU : Dec.-22, End Sem, Marks 9]

Ans. : Classification of protocols used :

<table>
<tr><td rowspan="20">Sensor Network Protocol</td><td rowspan="2">Architecture</td><td>Layered</td><td>UNPF</td></tr>
<tr><td>Clustered</td><td>LEACH</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="8">Data Handling</td><td rowspan="5">Data Dissemination</td><td>Flooding</td></tr>
<tr><td>SAR</td></tr>
<tr><td>SPIN</td></tr>
<tr><td>SMECN</td></tr>
<tr><td>Gossiping</td></tr>
<tr><td rowspan="3">Data Gathering</td><td>Direct Transmission</td></tr>
<tr><td>Binary Scheme</td></tr>
<tr><td>FEGASIS</td></tr>
<tr><td colspan="2"></td><td rowspan="9"></td></tr>
<tr><td rowspan="3">Medium Access Control</td><td>SMACS</td></tr>
<tr><td>Hybrid FDMA</td></tr>
<tr><td>CSMA</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="2">Location Discovery</td><td>Indoor Localization</td></tr>
<tr><td>Multi-lateration</td></tr>
<tr><td colspan="2"></td></tr>
</table>

	Miscellaneous	Quality of network coverage	Breach Path
			Maximum support path
		Security	LEAP
			INSENS
			SPINS
		Real time communication	SPEED
			RAP
		Other Solutions	Transport Layer
			Synchronizations
			Energy efficient hardware design

Also Refer Q.27

Q.29 Explain different issues and challenges in designing sensor network. ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : Issues and challenges in designing sensor network are as follows :

1. Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.
2. Energy : The operation of sensor nodes is depends on the available energy. Sensors usually rely only on their battery for power, which in many cases cannot be recharged or replaced. Hence, the available energy at the nodes should be considered as a major constraint while designing protocols.
3. Hardware design for sensor nodes should also consider energy efficiency as a primary requirement. The micro-controller, operating system, and application software should be designed to conserve power.
4. Sensor nodes should be able to synchronize with each other in a completely distributed manner.

5. A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up. The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.
6. Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.

Q.30 Compare sensor network with Adhoc wireless network.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. : • Both ad hoc wireless networks and sensor networks consist of wireless nodes communicating with each other, there are certain challenges posed by sensor networks.

- The number of nodes in a sensor network can be several orders of magnitude larger than the number of nodes in an ad hoc network.
- Sensor nodes are more prone to failure and energy drain, and their battery sources are usually not replaceable or rechargeable.
- Sensor nodes may not have unique global identifiers, so unique addressing is not always feasible in sensor networks.
- Sensor networks are data-centric, that is, the queries in sensor networks are addressed to nodes which have data satisfying some conditions. On the other hand, ad hoc networks are address-centric, with queries addressed to particular nodes specified by their unique address.
- Sensor networks require a different mechanism for routing and answering queries. Most routing protocols used in ad hoc networks cannot be directly ported to sensor networks because of limitations in memory, power, and processing capabilities in the sensor nodes and the non-scalable nature of the protocols.
- Sensor networks is data fusion/aggregation, whereby the sensor nodes aggregate the local information before relaying.

3.10 : Cluster Architecture Management

Q.31 Explain with diagram layered architecture & clustered architecture for sensor network. ☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : 1. Layered architecture :

- A layered architecture has a single powerful base station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS.
- Fig. Q.31.1 shows layered architecture.

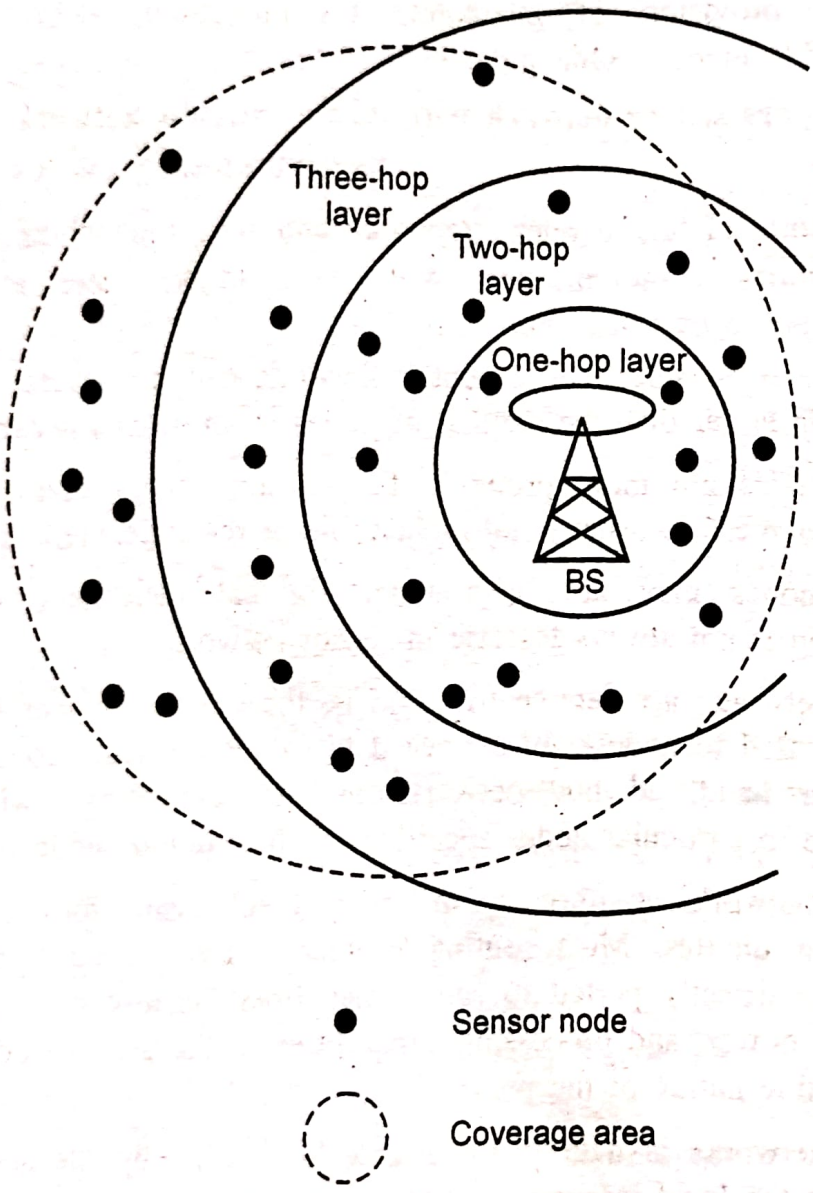


Fig. Q.31.1

- Layered architectures have been used with in-building wireless backbones, and in military sensor-based infrastructure, such as the multi-hop infrastructure network architecture (MINA).
- Unified Network Protocol Framework (UNPF) is a set of protocols for complete implementation of a layered architecture for sensor networks.

- UNPF integrates three operations in its protocol structure : network initialization and maintenance, MAC, and routing protocols.
- Network Initialization and Maintenance Protocol : The network initialization protocol organizes the sensor nodes into different layers, using the broadcast capability of the BS. The BS can reach all nodes in a one-hop communication over a common control channel. The BS broadcasts its identifier using a known CDMA code on the common control channel. All nodes which hear this broadcast then record the BS ID.
- MAC Protocol : Network initialization is carried out on a common control channel. During the data transmission phase, the Distributed TDMA Receiver Oriented Channel (DTROC) assignment MAC protocol is used. Each node is assigned a reception channel by the BS, and channel reuse is such that collisions are avoided.
- Routing Protocol : Downlink from the BS is by direct broadcast on the control channel. The layered architecture enables multi-hop data forwarding from the sensor nodes to the BS.

2. Clustered Architecture :

- A clustered architecture organizes the sensor nodes into clusters, each governed by a clusterhead. The nodes in each cluster are involved in message exchanges with their respective clusterheads, and these heads send messages to a BS, which is usually an access point connected to a wired network.
- Fig. Q.31.2 shows clustered architecture.
- Clustered architecture is specially useful for sensor networks because of its inherent suitability for data fusion. The data gathered by all members of the cluster can be fused at the cluster-head, and only the resulting information needs to be communicated to the BS.
- Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process. This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy (LEACH).

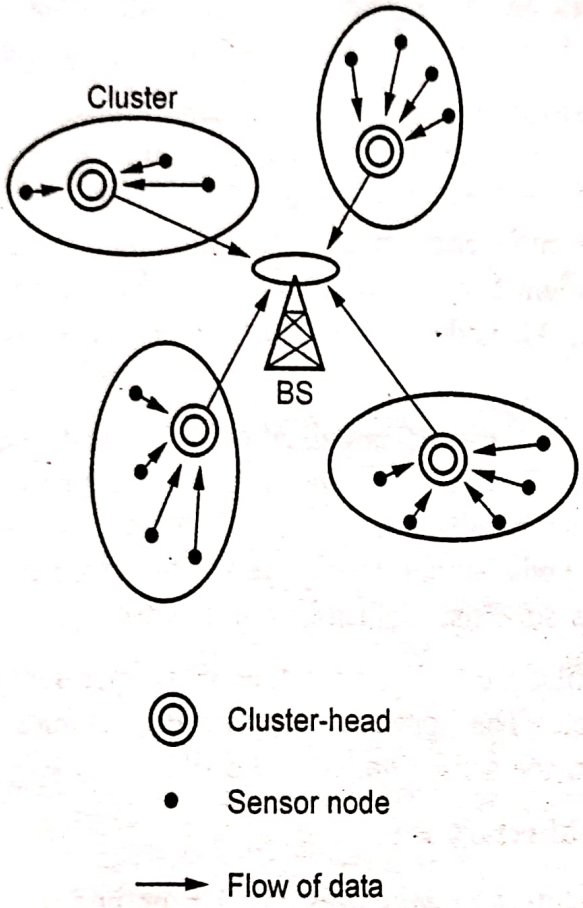


Fig. Q.31.2 clustered architecture

Q.32 Explain with diagram clustered architecture for sensor network.

☞ [SPPU : Dec.-22, End Sem, Marks 6]

Ans. : Refer Q.31

Q.33 Explain in detail LEACH algorithm.

☞ [SPPU : May-18, End Sem, Marks 10]

Ans. : • Low Energy Adaptive Clustering Hierarchy (LEACH) takes a hierarchical approach and organizes nodes into clusters. Within each cluster, nodes take turns to assume the role of a cluster head.

- LEACH uses TDMA to achieve communication between nodes and their cluster head.
- The cluster heads forwards to the base station messages received from its cluster nodes. The cluster head node sets up a TDMA schedule and transmits this schedule to all nodes in its cluster.

- The schedule prevents collisions among data messages. Furthermore, the schedule can be used by the nodes to determine the time slots during which they must be active. This allows each cluster node, except for the head cluster, to turn-off their radio components until its allocated time slots.
- LEACH assumes that cluster nodes start the cluster setup phase at the same time and remain synchronized thereafter one possible mechanism to achieve synchronization is to have the base station send out synchronization pulses to the all the nodes.
- To reduce inter-cluster interference, LEACH uses a transmitter-based code assignment scheme. Communications between a node and its cluster head are achieved using Direct-Sequence Spread Spectrum (DSSS), whereby each cluster is assigned a unique spreading code, which is used by all nodes in the cluster to transmit their data to the cluster head.
- Spreading codes are assigned to cluster heads on a first-in first-served basis, starting with the first cluster head to announce its position, followed by subsequent cluster heads.
- Nodes are also required to adjust their transmit powers to reduce interference with nearby clusters. Upon receiving data packets form its cluster nodes, the cluster head aggregates the data before sending them to the base station.
- The communication between a cluster head and a base station is achieved using fixed spreading code and CSMA.
- Before transmitting data to the base station, the cluster head must sense the channel to ensure that no other cluster head is currently transmitting data using the base station spreading code.
- If the channel is sensed busy, the cluster head delays the data transmission until the channel becomes idle. When this event occurs, the cluster head sends the data using the base station spreading code.
- In general, schedule-based protocols are contention free and as such, they eliminate energy waste caused by collisions. Furthermore, sensor nodes need only turn their radios on during those slots where data are to be transmitted or received.
- In all other slots, the sensor node can turn-off its radio, thereby avoiding overhearting. This results in low-duty-cycle node operations, which may extend the network lifetime significantly.

- Schedule based MAC protocols have several disadvantages, however, which limit their use in WSNs. The use of TDMA requires the organization of nodes into clusters. This hierarchical structure often restricts nodes to communicate only with their cluster head.
- Consequently, peer-to-peer communication cannot be supported directly, unless nodes are required to listen during all times slot. Most of the schedule based schemes depend on distributed, to align slots boundaries.
- Achieving time synchronization among distributed sensor nodes is difficult and costly, especially in energy-constrained wireless networks.
- Schedule-based schemes also require additional mechanisms such as FADMA or CDMA to overcome inter-cluster communications and interference.
- Finally, TDMA-based MAC-layer protocols have limited scalability and are not easily adaptable to node mobility and changes in network traffic and topology.

END...

Unit IV

4 Introduction to Network Security

4.1 : Importance and Need for Security

Q.1 What is importance and need of security ?

☞ [SPPU : Dec.-22, End Sem, Marks 5]

Ans. : • Now a day, protection is easier because many factors working against the potential criminal. Very sophisticated alarm and camera systems silently protect secure places like banks.

- Traditionally information security provided by physical i.e. rugged filing cabinets with locks and administrative mechanisms i.e. personnel screening procedures during hiring process.
- Asset protection systems are designed to recover stolen cash and high value assets, apprehend criminals and deter crime. The system has the capacity to track, protect and manage critical assets in real-time.
- The techniques of criminal investigation have become so effective that a person can be identified by genetic material, voice, retinal pattern, fingerprints etc.
- Use of networks and communications links requires measures to protect data during transmission.
- **Data security** is the science and study of methods of protecting data from unauthorized disclosure and modification.
- Data and information security is about enabling collaboration while managing risk with an approach that balances availability versus the confidentiality of data.
- **Computer security :** Generic name for the collection of tools designed to protect data and to hackers.
- **Network security :** Measures to protect data during their transmission.
- **Internet security :** Measures to protect data during their transmission over a collection of interconnected networks.

Protecting valuables

- Following are certain aspects for the need of security :

1. Increasing threat of attacks.
2. Fast growth of computer networking for information sharing.
3. Availability of number of tools and resources on internet.
4. Lack of specialized resources that may be allotted for securing system.

Q.2 What is business need of network security ? Explain.

Ans. : • Information security performs **four** important organizational functions :

1. Protects the organization's ability to function.
2. Safe operation of organizations applications in IT systems.
3. Protection of organization data.
4. Safeguards the technology assets in use at the organization.

- **Protecting the functionality of an organization :** Information security is implemented in organization by IT department management and general management. In some private organization and government offices, some manager level officers are not interested in implementing security because of complex process.
- **Enabling the safe operation applications :** Some of the resources that important in the organizations. These resources operating system, electronic mail and hardware resources. Organization must provide the security to these resources.
- **Protection of organization data :** Data is important in any organization. The value of data motivates attackers to steal, delete, or corrupt it. An effective information security program directed by management is essential to the protection of the integrity and value of the organization's data.
- **Safeguarding technology assets in organizations :** An organization must add secure infrastructure services matching the size and scope of the enterprise. As the organization's network grows to accommodate changing needs, it may need more robust technology solutions.

4.2 : Network Attacks

Q.3 What is the importance and need for security and explain network attack ? ☞ [SPPU : June-22, End Sem, Marks 8]

Ans. : • In a network attack, attackers are focused on penetrating the corporate network perimeter and gaining access to internal systems. Very often, once inside attackers will combine other types of attacks, for example compromising an endpoint, spreading malware or exploiting a vulnerability in a system within the network.

• Also Refer Q.5.

Q.4 Explain distributed denial of service attacks in details.

☞ [SPPU : June-22, End Sem, Marks 8, Dec.-22, End Sem, Marks 6]

Ans. : • The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.

• The DDoS attack uses multiple computers and Internet connections to flood the targeted resource.

• Fabrication causes Denial Of Service (DOS) attacks. DOS prevents the normal use or management of communications facilities.

• Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

• The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. This kind of an attack is called a **Distributed Denial of Service (DDoS)** attack.

• DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a DoS attack.

• Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

• The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.

• The DDoS attack uses multiple computers and Internet connections to flood the targeted resource.

• DDoS attacks are often global attacks, distributed via botnets.

Q.5 Explain with suitable examples what do you mean by active attacks & passive attacks. ☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : Active attacks :

- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.
- Active attacks can be subdivided into four types :
  1. Masquerade
  2. Replay
  3. Modification of message
  4. Denial of service

1. Masquerade

- It takes place when one entity pretends to be a different entity. Fig. Q.5.1 shows masquerade.

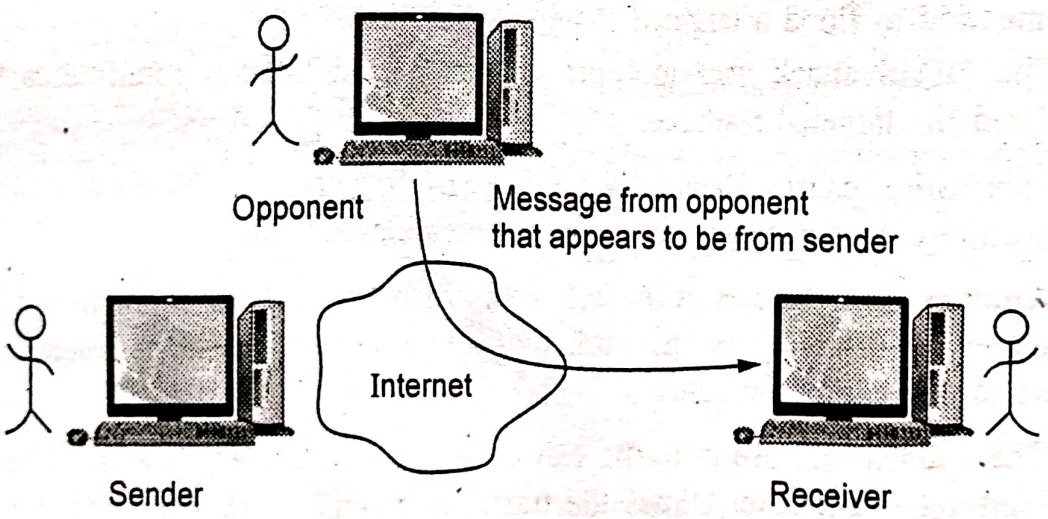


Fig. Q.5.1 Masquerade

- **For example :** Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- **Interruption** attacks are called as masquerade attacks.

2. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Fig. Q.5.2 shows replay attack.

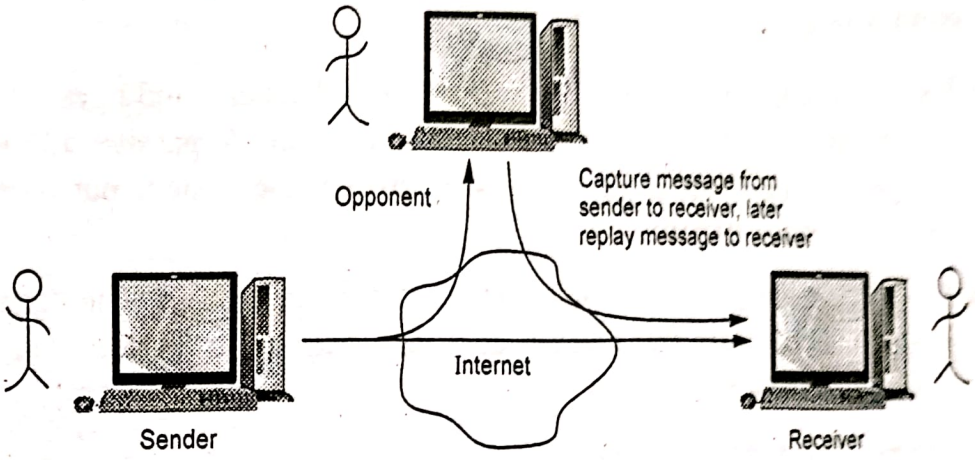


Fig. Q.5.2 Replay

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. Q.5.3 shows the modification of message.
- For example, a message meaning "Allow Rupali Dhotre to read confidential file accounts " is modified to mean "Allow Mahesh Awati to read confidential file accounts".

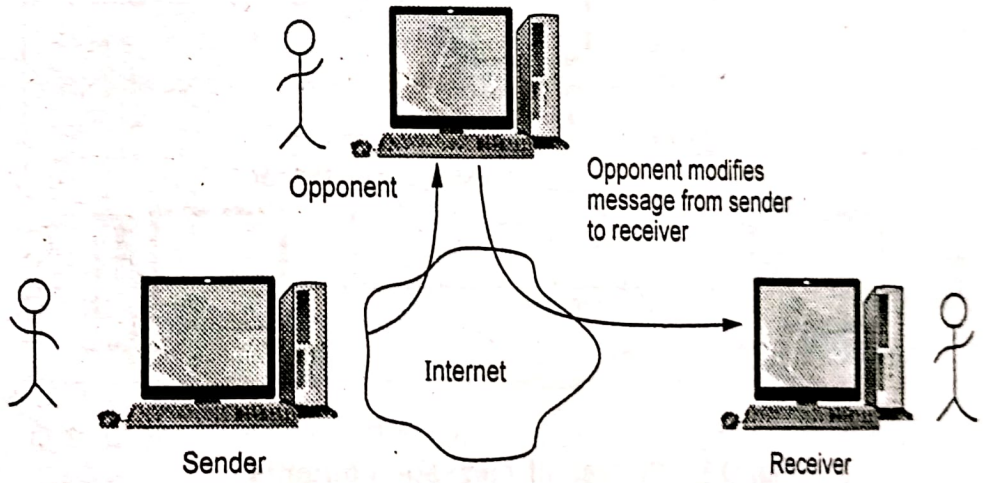


Fig. Q.5.3 Modification of message

4. Denial of service

- Fabrication causes Denial Of Service (DOS) attacks.
- DOS prevents the normal use or management of communications facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Passive Attack :

- Passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- The attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data.
- **Passive attacks** are of two types :
  1. Release of message contents
  2. Traffic analysis
- **Release of message content** is shown in Fig. Q.5.4. A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information we would like to prevent an opponent from learning the content of these transmissions.

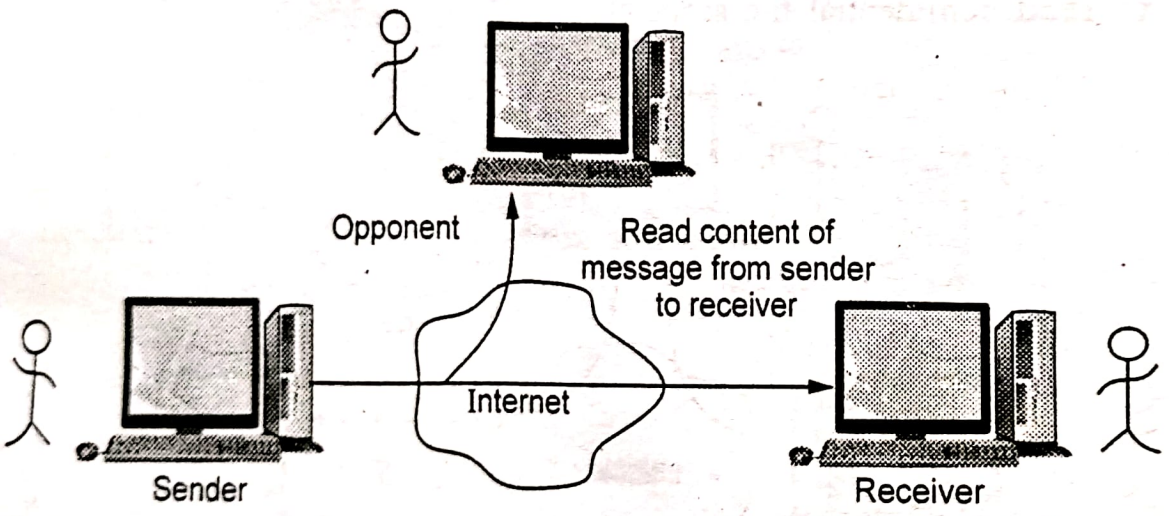


Fig. Q.5.4 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. Q.5.5 shows the traffic analysis.
- Passive attacks are very difficult to detect because they do not involve any alternation of data. It is feasible to prevent the success of attack, usually by means of encryption.

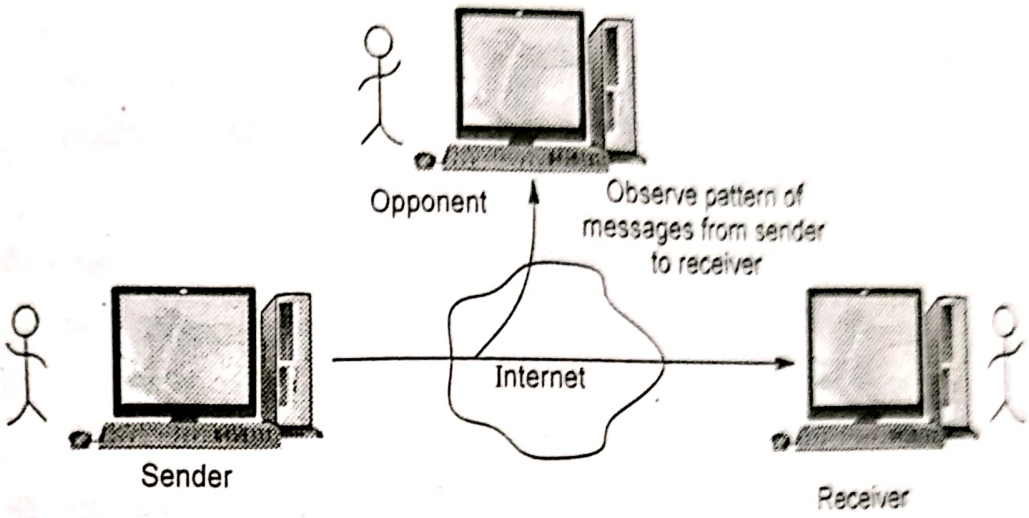


Fig. Q.5.5 Traffic analysis

Q.6 Differentiate between active and passive attack.

Ans. :

Active attack	Passive attack
Active attacks involve some modification of the data stream or the creation of a false stream	Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions
Types : Masquerade, replay, modification of message and denial of service.	Types : Release of message contents and traffic analysis
Easy to detect.	Very difficult to detect.
It is quite difficult to prevent active attacks absolutely.	The emphasis in dealing with passive attacks is on prevention rather than detection.

Q.7 Explain Man in the middle attacks. How to defenses against the attack ?

Ans. : • In cryptography, a **Man-In-The-Middle (MITM) attack** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.

- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.

- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack
  4. Replay attacks
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin.
- Mallory can simply send Alice a public key for which she has the private, matching, key. Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy, and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various

defenses against MITM attacks use authentication techniques that are based on :

1. Public keys
2. Stronger mutual authentication
3. Secret keys (high information entropy secrets)
4. Passwords (low information entropy secrets)
5. Other criteria, such as voice recognition or other biometrics

- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a Certificate Authority, whose public key is distributed through a secure channel.

4.3 : Network Security Threats

Q.8 What is threats and vulnerability ? Explain with example.

Ans. : Threat

- The term "threat" refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat. Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.

Vulnerability

- The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful.
- Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to

provide data used to identify unexpected dangers to security that need to be addressed.

- Such vulnerabilities are not particular to technology - they can also apply to social factors such as individual authentication and authorization policies.
- Testing for vulnerabilities is useful for maintaining ongoing security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise. It is also invaluable for policy and technology development, and as part of a technology selection process; selecting the right technology early on can ensure significant savings in time, money, and other business costs further down the line.
- Understanding the proper use of such terms is important not only to sound like you know what you're talking about, nor even just to facilitate communication. It also helps develop and employ good policies.
- The specificity of technical jargon reflects the way experts have identified clear distinctions between practical realities of their fields of expertise, and can help clarify even for oneself how one should address the challenges that arise.
- Other examples of vulnerability include these :
  1. A weakness in a firewall that lets hackers get into a computer network.
  2. Unlocked doors at businesses.
  3. Lack of security cameras.

Q.9 Write short note on deviations in quality of service.

Ans. : • **Internet service issues :** Most of the organizations uses the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information.

- **Power irregularities :** Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages and power losses. This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.
- Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

- Types of industrial espionage,
  a) Trespassing onto a competitor's property or accessing their files without permission
  b) Posing as a competitor's employee in order to learn company trade secrets or other confidential information
  c) Wiretapping a competitor
  d) Hacking into a competitor's computers
  e) Attacking a competitor's website with malware.

4.4 : Concept of Security Principles

Q.10 Comment on security principles and security services.

☞ [SPPU : Dec.-22, End Sem, Marks 9]

Ans. : • X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

- X.800 divides security services into five different categories.
  1. Authentication
  2. Access control
  3. Data confidentiality
  4. Data integrity
  5. Nonrepudiation

1. Authentication

- Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.
- Two specific authentication services are defined in X.800 :
  a. Peer entity authentication
  b. Data origin authentication
- **Peer entity authentication** used in association with a logical connection to provide confidence in the identity of the entities connected.
- Data origin outhentication enables the recepient to verify that the message have not been tempered in transit (data integrity) and they originally from expected sender (authenticity).

- **Data origin authentication** does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

2. Access control

- It is the ability to limit and control the access to host systems and applications via communications links.
- This service controls who can have access to a resource.

3. Data confidentiality

- Confidentiality is the concealment of information or resources. It is the protection of transmitted data from passive attacks.
- Confidentiality is classified into
  1. **Connection confidentiality :** The protection of all user data on a connection.
  2. **Connectionless confidentiality :** The protection of all user data in a single data block.
  3. **Selective field confidentiality :** The confidentiality of selected fields within the user data on a connection or in a single data block.
  4. **Traffic flow confidentiality :** The protection of the information that might be derived from observation of traffic flows.

4. Data integrity

- Integrity can apply to a stream of messages a single message or selected fields within a message.
- Modification causes loss of message integrity.
- Data integrity can be classified as
  1. Connection integrity with recovery
  2. Connection integrity without recovery
  3. Selective field connection integrity
  4. Connectionless integrity
  5. Selective field connectionless integrity
- Connection integrity with recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence with recovery attempted.

- Connection integrity without recovery provides only detection without recovery.
- Selective field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection.
- Connectionless integrity provides for the integrity of a single connectionless data block and may take the form of detection of data modification.

5. Nonrepudiation

- Nonrepudiation prevents either sender or receiver from denying a transmitted message.
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
- When a message is received, the sender can prove that the alleged receiver in fact received the message.

Q.11 Define confidentiality, integrity and availability.

Ans. :

1. Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones. Sensitive information should be kept secret from individuals who are not authorized to see the information.
2. Integrity ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential communication, but may have the ability to change the information being transmitted.
3. Availability refers, to the availability of information resources. An information system that is not available when we need it is at least as bad as none at all. Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure

4.5 : Stream Ciphers

Q.12 What is stream cipher ? Explain advantages and disadvantages.

Ans. : Stream Cipher

- Stream cipher algorithms are designed to accept a crypto key and a stream of plaintext to produce a stream of ciphertext.
- Fig. Q.12.1 shows the stream cipher.

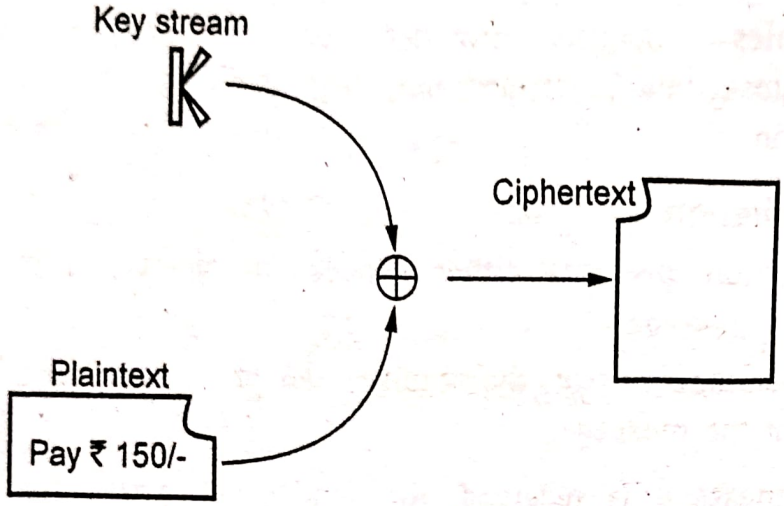


Fig. Q.12.1 Stream cipher

- Stream cipher is similar to a one time pad.
- A stream cipher encrypts smaller block of data, typically bits or bytes.
- A key stream generator outputs a stream of bits $K_1, K_2, K_3 \ldots\ldots K_i$.
- This key stream is XORed with a stream of plaintext bits $P_1, P_2, P_3 \ldots\ldots P_i$ to produce the stream of ciphertext bits.

$$C_i = P_i \oplus K_i$$

- At the description end, the ciphertext bits are XORed with an identical key stream to recover the plaintext bits.

$$P_i = C_i \oplus K_i$$

- The system security depends entirely on the insides of the keystream generator.

Advantages :

1. Speed of transformation
2. Low error propagation.

Disadvantages :

1. Low diffusion
2. Susceptibility to malicious insertation and modifications.

Q.13 Explain difference between stream cipher and block cipher.

Ans. :

Sr. No.	Stream cipher	Block cipher
1.	Stream ciphers operate on smaller units of plaintext.	Block ciphers operate on larger block of data.
2.	Faster than block cipher.	Slower than stream cipher.
3.	Stream cipher processes the input element continuously producing output one element at a time.	Block cipher processes the input one block of element at a time, producing an output block for each input block.
4.	Requires less code.	Requires more code.
5.	Only one time of key use.	Reuse of key is possible.
6.	Ex. - One time pad	Ex. - DES
7.	Application - SSL (secure connections on the web.)	Application - Database, file encryption.
8.	Stream cipher is more suitable for hardware implementation.	Easier to implement in software.

4.6 : Substitution Cipher

Q.14 Explain operation of polyalphabetic cipher.

Ans. : • In polyalphabetic substitution, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one to many.

- An example of polyalphabetic substitution is the **Vigenere cipher.**
- The Vigenere cipher chooses a sequence of keys, represented by a string. The key letters are applied to successive plaintext characters, and when the end of the key is reached, the key start over.
- For example : Let the message be THE BOY HAS THE BAG and let the key be VIG.

Key = VIG VIG VIG VIG VIG

Plaintext = THE BOY HAS THE BAG

Ciphertext = OPKWWECIYOPKWIM

- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.

Q.15 Use polyalphabetic ciphers to encrypt plain text "SHE IS VERY HAPPY AND BEAUTIFUL GIRL" use key 'ANOTHER'

Ans. :

Keyword	anoth	erano	thera	nothe	ranot	heran
Plaintext	sheis	veryh	appya	ndbea	utifu	lgirl
Ciphertext	SUSBZ	ZVRLV	TWTPA	ARULE	LTVTN	SKZRY

Q.16 Explain Monoalphabetic Cipher with example.

Ans. : • Monoalphabetic cipher substitutes one letter of the alphabet with another letter of the alphabet. However, rather than substituting according to a regular pattern, any letter can be substituted for any other letter, as long as each letter has a unique substitute left and vice versa.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	m	n	b	v	c	x	z	a	s	d	f	g	h

Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	j	k	l	p	o	i	u	y	t	r	e	w	q

For example

Plaintext message : hello how are you

Ciphertext message : acggk akr moc wky

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

Homophonic substitution cipher

- It provides multiple substitutes for a single letter. For example, A can be replaced by D, H, P, R; B can be replaced by E, Q, S, T etc.

Q.17 Compare monoalphabetic and polyalphabetic cipher.

Ans. :

Sr. No.	Monoalphabetic cipher	Polyalphabetic cipher
1.	Once a key is chosen, each alphabetic character of a plaintext is mapped onto a **unique** alphabetic character of a ciphertext.	Each alphabetic character of a plaintext can be mapped onto "**m**" alphabetic characters of a ciphertext.
2.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
3.	A stream cipher is a monoalphabetic cipher if the value of *k*i does not depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of *k*i does depend on the position of the plaintext character in the plaintext stream.
4.	Monoalphabetic cipher includes additive, multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor , and Enigma cipher.

4.7 : Transposition Cipher

Q.18 What is transposition cipher? Use transposition cipher to encrypt the plain text "WE ARE THE BEST" use key "HEAVEN".

Ans. : Transposition cipher :

- A transposition cipher rearranges the characters in the plaintext to form the ciphertext. The letters are not changed.
- The rail fence cipher is composed by writing the plaintext in two rows, proceeding down, then across and reading the ciphertext across, then down.
- For example, to enciphere the message "meet me after this party" with a rail fence of depth 2, we write the following :

m e m a t r h s a t
e t e f e t i p r y

- The ciphertext is

  MEMATRHSATETEFETIPRY

- Attacking a transposition cipher requires rearrangement of the letters of the ciphertext.
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.

Plaintext : The book is suitable for self study.

Key : 5 6 4 1 3 2

Key : 5 6 4 1 3 2

Plaintext : t h e b o o
k i s s u i
t a b l e f
o r s e l f
s t u d y

Ciphertext : BSLEDOIFFOUELYESBSUTKTOSHIART.

Key = HEAVEN

KEY	H	E	A	V	E	N
KEY NUMBER	4	2	1	6	3	5
PLAIN TEXT	W	E	A	R	E	T
	H	E	B	E	S	T
Arrange the key number as per ascending order						
KEY	A	E	E	H	N	V
KEY NUMBER	1	2	3	4	5	6

PLAIN TEXT	A	E	E	W	T	R
	B	E	S	H	T	E

Ciphertext = ABEEESWHTTRE

Q.19 Compare substitution and transposition ciphers.

Ans. :

	Substitution ciphers	Transposition ciphers
Definition	Each letter or group of letters of the plaintext are replaced by some other letter of group of letters, to obtain the ciphertext.	Letters of the plaintext are permuted in some form.
Example	Hill cipher, one time pad	Rail fence cipher
Strength	1.Exhaustive search is infeasible. 2.Through to be unbreakable by many back then.	1.Reduce redundancies in plaintext. 2.Transposition cipher can be made more secure by performing more than one stage of transposition.
Drawback	1.Brute force attack is easy	1.The ciphertext has the same letter frequency as the original plaintext. 2.Guessing the number of columns and some probable words in the plaintext holds the key.

4.8 : Block Ciphers Modes

Q.20 Explain different block cipher muscles.

☞ [SPPU : June-22, End Sem, Marks 9]

OR Explain different block cipher modes.

☞ [SPPU : Dec.-22, End Sem, Marks 8]

Ans. : • The modes of operation of block ciphers are configuration methods that allow those ciphers to work with large data streams, without the risk of compromising the provided security.

- There are five types of operations in block cipher modes, ECB (Electronic Code Block) mode, CBC (Cipher Block Chaining) mode, CFB (Cipher Feedback) mode, OFB (Output Feedback) mode and CTR (Counter) mode.
- Where ECB and CBC mode works on block ciphers, and CFB and OFB mode works on block ciphers acting as stream ciphers.
- ECB is used for transmitting a single value in secure manner, CBC is used for encrypting blocks of text authentication, CFB is used for transmitting encrypted stream of data authentication, OFB is used for transmitting encrypted stream of data, CTR is used for transmitting block-oriented applications.
- Modes of operation enable the repeated and secure use of a block cipher under a single key. A block cipher by itself allows encryption only of a single data block of the cipher's block length.
- When targeting a variable-length message, the data must first be partitioned into separate cipher blocks. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme.
- Modes of operation have primarily been defined for encryption and authentication. While modes of operation are commonly associated with symmetric encryption, they may also be applied to public-key encryption primitives such as RSA in principle.

Q.21 Explain Electronic Code block (ECB) mode.

☞ **[SPPU : Dec.-22, End Sem, Marks 6]**

Ans. : • A block of plaintext encrypts into a block of ciphertext. Block size is 64-bits. Each block is encrypted independently.

- Plaintext patterns are not concealed since identical blocks of plaintext give identical blocks of ciphertext. It is not necessary to encrypt the file linearly.
- User can encrypt the 10 blocks in the middle first, then the blocks at the end, and finally the blocks in the beginning. Because of this, encrypted files are accessed randomly like a data base.
- It is very easy to parallelize the process. Pad the last block with some regular pattern i.e. zeros, ones to make it a complete block.

- End of file character is used to denote the final plaintext byte before padding.
- ECB method is ideal for a short amount of data, such as an encryption key.
- Fig. Q.21.1 shows ECB mode.

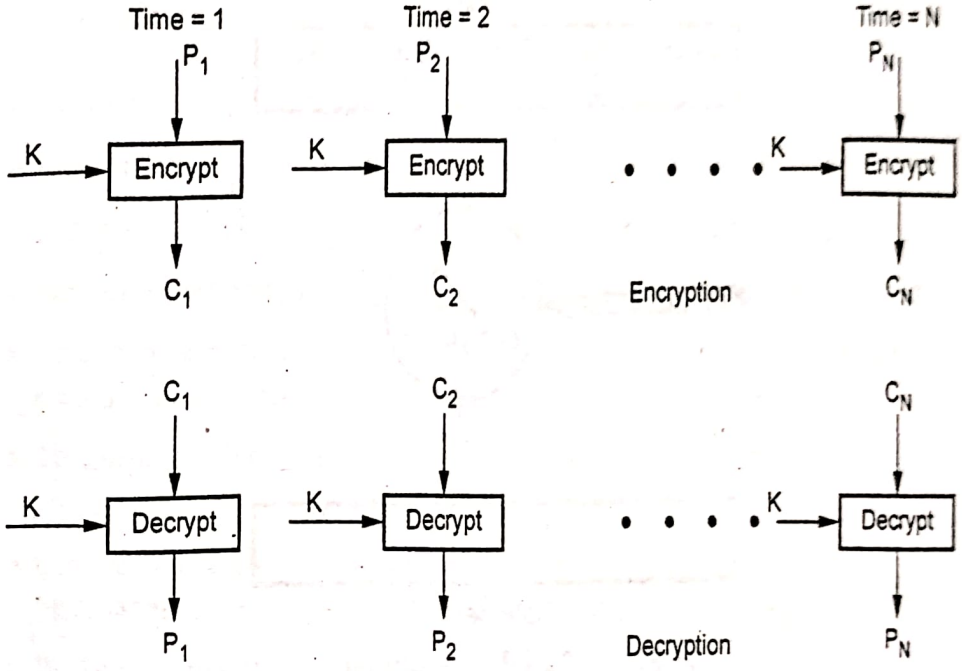


Fig. Q.21.1 ECB mode

- In this mode, the plain text is divided into a block where each block is of 64 bits. Then each block is encrypted separately. The same key is used for the encryption of all blocks. Each block is encrypted using the key and makes the block of ciphertext.
- At the receiver side, the data is divided into a block, each of 64 bits. The same key which is used for encryption is used for decryption. It takes the 64-bit ciphertext and by using the key convert the ciphertext into the plain text.
- For lengthy messages, the ECB mode may not be secure.
- Used in secure transmission of single values i.e. an encryption key.
- ECB has security problems that limit its usability.
- Patterns in the plaintext can yield patterns in the ciphertext.
- It is also easy to modify a ciphertext message by adding, removing or switching encrypted blocks.
- Synchronization error is unrecoverable.

Q.22 What is block cipher ? Explain counter mode of block cipher.

☞ [SPPU : April-17, In Sem, Marks 5]

Ans. : Block Cipher

- A block cipher operates on blocks of data.
- Fig. Q.22.1 shows block cipher method.

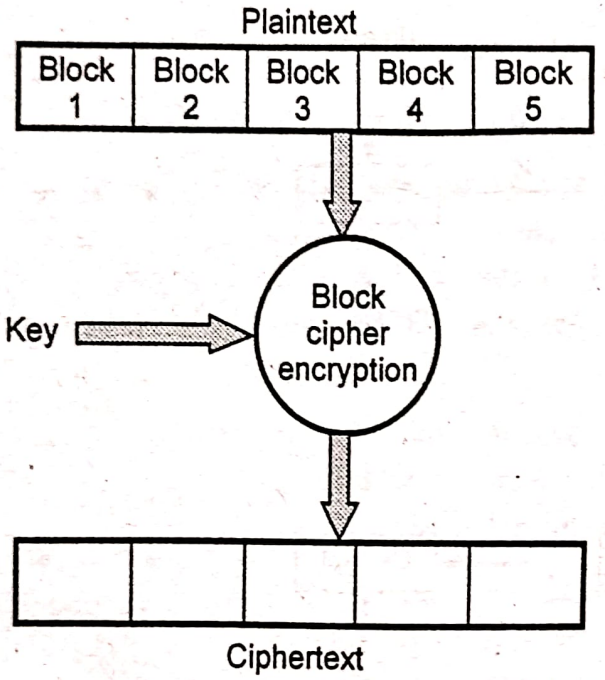


Fig. Q.22.1 Block cipher

- Algorithm breaks the plaintext into blocks and operates on each block independently.
- Usually blocks are 8 or 16 bytes long.
- Security of block ciphers depends on the design of the encryption function.
- Software implementations of block ciphers run faster than software implementation of the stream ciphers.
- Errors in transmitting one block generally do not affect other blocks.
- Each block is enciphered independently, using the same key, identical plaintext blocks produce identical ciphertext blocks.
- Suppose that plaintext is 227 bytes long and the cipher you are using operates on 16-byte blocks.
- Algorithm grabs the first 16-bytes of data, encrypts them using the key table.

- Algorithm produces 16-bytes of ciphertext.
- After first block, algorithm takes next block.
- The key table does not change from block to block.

Plaintext = 227 bytes

$$\text{Block size} = 16 \text{ bytes} = \frac{227}{16} = 14 \text{ blocks plus } 3 \text{ bytes}$$

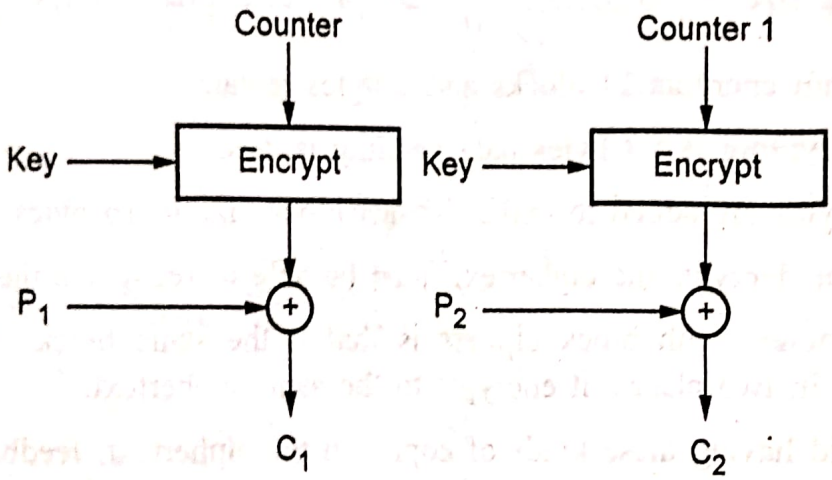
- Algorithm encrypts 14 blocks and 3 bytes remain.
- For encrypting last 3 bytes data padding is used.
- Extra bytes are added to make the last block size to 16 bytes.
- Whoever decrypts the ciphertext must be able to recognize the padding.
- One problem with block ciphers is that if the same block of plaintext appears in two places, it encrypts to the same ciphertext.
- To avoid having these kinds of copies in the ciphertext, feedback modes are used.
- Cipher block chaining does not require the extra information to occupy bit spaces, so every bit in the block is part of the message.
- Before a plaintext block is enciphered, that block is XOR'ed with preceding ciphertext block.
- In addition to the key, this technique requires an initialization vector to XOR the initial plaintext block.
- For decrypting the data, copy a block of ciphertext, decrypt it and XOR the result with the preceding block of ciphertext.
- Taking E_K to be the encipherment algorithm with key K and I to be the initialization vector, the cipher block chaining technique is

$$C_o = E_K(m_o \oplus I)$$
$$C_i = E_K(m_i \oplus C_{i-1}) \quad \text{for i} > 0$$

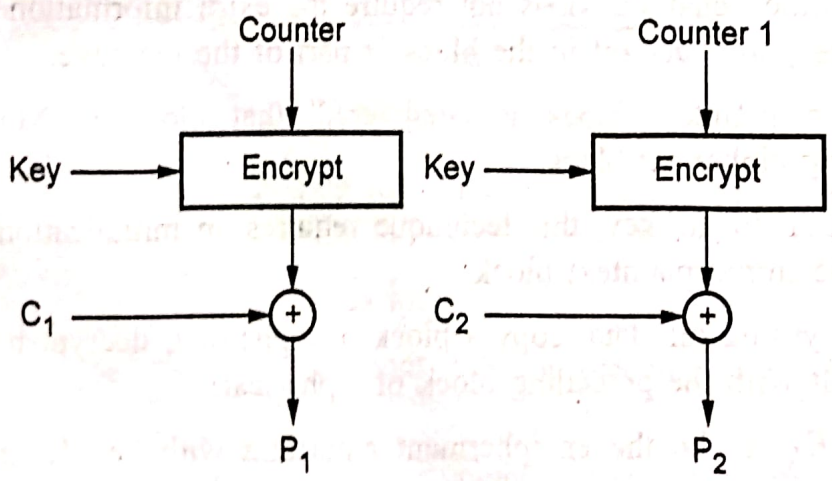
Counter (CTR) Mode of Block Cipher :

- Block ciphers in counter mode use sequence numbers as the input to the algorithm.
- More than one message can be encrypted with the same key, provided that a different initialise vector is used.
- Plaintext is very easy to manipulate, any change in ciphertext directly affects the plaintext.

- Synchronization error is unrecoverable.
- A ciphertext error affects only the corresponding bit of plaintext.
- **Encryption :** The counter is encrypted and then XORed with the plaintext block to produce the ciphertext block.
- Fig. Q.22.2 shows encryption and decryption.



(a) Encryption



(b) Decryption

Fig. Q.22.2 Counter mode

Advantages

1. Simple to implement.
2. It provides confidentiality.
3. Random access of block is possible.
4. Efficiency is same as block cipher.

Q.23 Explain the operation of Cipher Block Chaining (CBC) mode.

☞ [SPPU : May-17, End Sem, April-16, In Sem, Marks 5]

Ans. : Cipher Block Chaining Mode (CBC)

- The plaintext is XORed with the previous ciphertext block before it is encrypted. This mode is iterative mode.
- After a plaintext block is encrypted, the resulting ciphertext is also stored in a feedback register. Before the next plaintext block is encrypted, it is XORed with the feedback register to become the next input to the encrypting routine. The encryption of each block depends on all the previous blocks.
- A ciphertext block is decrypted normally and also saved in a feedback register. After the next block is decrypted, it is XORed with the results of the feedback register. Fig Q.23.1 shows CBC modes of operation.

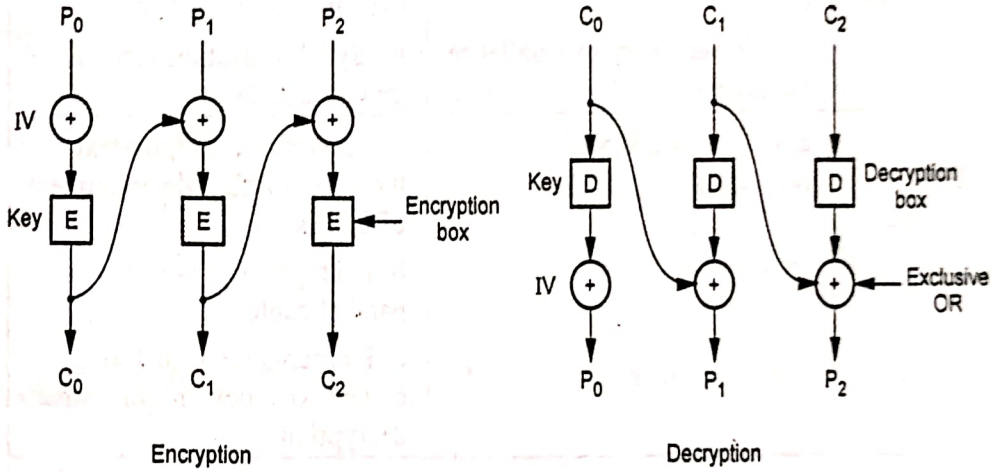


Fig. Q.23.1

- Mathematically it is

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = C_{i-1} \oplus D_k(C_i)$$

- It hides patterns in the plaintext.
- In order to guarantee that there is always some random looking ciphertext to apply to the actual plaintext, the process is started with a block of random bits called the initialization vector (IV).
- When used in networking messages, most CBC implementations add the IV to the beginning of the message in plaintext.
- A single bit error in a plaintext block will affect that ciphertext block and all subsequent ciphertext blocks. CBC mode is self recovering.

- Two blocks are affected by an error, but the system recovers and continues to work correctly for all subsequent blocks. Synchronization error is unrecoverable.
- Encryption is not parallelizable. Decryption is parallelizable and has a random access property.

Q.24 List various modes of operation of block ciphers. Give advantages and disadvantages of each.

Ans. : Various modes of operation of block ciphers are :

1. Electronic Code Book 2. Cipher Block Chaining Mode
3. Cipher Feedback Mode 4. Counter Mode

Modes of operation	Advantages	Disadvanatges
Electronic Code Book	a. ideal for a short amount of data b. It is very easy to parallelize the process	a. ECB has security problems that limit its usability. b. Synchronization error is unrecoverable.
Cipher Block Chaining Mode	a. CBC mode is self recovering.	a. An error in a ciphertext block will affect decipherment of blocks b. Encryption is not parallelizable c. Rearrangement of the ciphertext blocks highly affects decryption.
Cipher Feedback Mode	a. Simplicity b. Need not be used on a byte boundary. c. Input to the block cipher is randomized. d. Ciphert text size is the same size as the plaintext size.	a. Encryption is not parallelizable. b. Plaintext is somewhat difficult to manipulate.
Counter Mode	a. Simple to implement. b. It provides confidentiality. c. Random access of block is possible. d. Efficiency is same as block cipher.	a. Flipping bits in the plaintext is very easy because flipping a ciphertext bit flips the corresponding plaintext bit b. CTR mode has inadequate security when using ciphers with 64-bit blocks

END...

Unit V

5 Cryptographic Algorithm

5.1 : Mathematical Preliminaries : Groups, Rings, Fields, Prime numbers

Q.1 Explain following terms : i) Groups ii) Rings iii) Prime numbers

☞ [SPPU : Dec.-22, End Sem, Marks 9]

Ans. : i) Groups :

- A group G is a nonempty set together with a *binary operation* (*) such that the following three properties are satisfied :
  1. **Associativity :** (a*b)*c = a*(b*c). For all a, b, c ε G.
  2. **Identity :** There is an element e ε G such that a*e = e*a. For all a ε G.
  3. **Inverses :** For each element a ε G, there is an element b ε G such that a*b = b*a = e.
- Order of a Group G is the number of elements it contains (denoted |G|). Order of an element g ε G is the smallest positive integer n such that g^n = e (denoted |g|). Here g^n = g*g*... *g n (times). In a *finite* group, the order of each element of the group divides the order of the group.

ii) Rings :

- A Ring R is a nonempty set with two binary operations, addition (denoted by a + b) and multiplication (denoted ab), such that for all a, b, c ε R :
  1. R is an abelian group under addition.
  2. a(bc) = (ab)c (associativity)
  3. a(b + c) = ab + ac and (b + c)a = bc + ca.
- A Unity in a ring is a nonzero element that is the identity under multiplication.

- A Commutative Ring R is ring such that for all a, b, c, ε R.
  1. a(b + c) = ab + ac = (b + c) a (commutativity)
- A Unit is a nonzero element of a Commutative Ring with Unity that has a multiplicative inverse.
- A Zero-Divisor is a nonzero element a ε R, R is a commutative ring, such that there is a nonzero element b ε R with ab = 0.
- An Integral Domain is a commutative Ring with unity and no zero-divisors.

iii) **Prime Numbers :** Every number can be factorized into its prime numbers. Generally, it's very hard to find the factors of a number. To find all the prime factors of a natural number n, one has to try and divide it by its possible factors up to $\sqrt{2}$. It is very difficult to find the prime factors of a large number. RSA uses prime number.

Q.2 Write short note on finite field.

Ans. : • A field is a set of elements on which two arithmetic operations i.e. addition and multiplication, have been defined and which has the properties of abstract algebra arithmetic, such as closure, associativity, commutativity, distributivity and having both additive and multiplicate inverses.

- A finite field is simply a field with a finite number of elements. It can be shown that the order of a finite field must be a power of a prime p^n, where n is a positive integer.
- Finite field of order p can be defined using arithmetic mod p.
- **Properties**
  1. It can be shown that finite fields have order p^n, where p is a prime.
  2. It can be shown that for each prime p and each positive integer 'n', there is, upto isomorphism, a unique finite field of order p^n.
  3. Let GF (p^n) represent a finite field of order p^n. GF stands for **Galois field.**

Construction of finite fields

- To construct GF (p^n), first find an irreducible polynomial I of degree n, with coefficients in Z_p.

- Let GF $(p^n) = \{a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + ... + a_1 x + a_0 \mid a_i \varepsilon Z_p\}$
- (Note that here addition is done modulo Z_p while multiplication is done modulo I).
- Example GF (16) = GF (2^4) we want polynomial of degree 4 with coefficients in $Z_2 = \{ax_3 + bx_2 + cx + d \mid a, b, c, d, \varepsilon Z_2\}$.
- Here addition is done as in Z_2 [x] , while multiplication is done modulo $x^4 + x + 1$.

Properties of GF (p^n)

- It can be shown that for each positive integer n there exists an irreducible polynomial of degree n over GF(p) for any p.
- It can be shown that for each divisor m of n, GF(p^n) has a unique sub field of order p^m. Moreover, these are the only subfields of GF(p^n).

Primitive Element

- A nonzero element a ε GF(q) is called a **Primitive Element** if $h^1, h^2 ... h^{q-1}$, are precisely all the nonzero elements of GF(q) (i.e. the multiplicative order of a is (q – 1)).
  1. Generator of the multiplicative group of nonzero elements.
  2. Used to simplify multiplication.
- It can be shown that every GF(p^n) contains a primitive element.

5.2 : Symmetric Key Algorithms : DES

Q.3 Write a short notes on : i) Encryption ii) Decryption

☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : i) Encryption : Data encryption is a method of converting data from a readable format (plaintext) into an unreadable, encoded format (ciphertext). Encrypted data can only be read or processed after it has been decrypted, using a decryption key or password. Only the sender and the recipient of the data should have access to the decryption key. Fig. Q.3.1 shows encryption process.

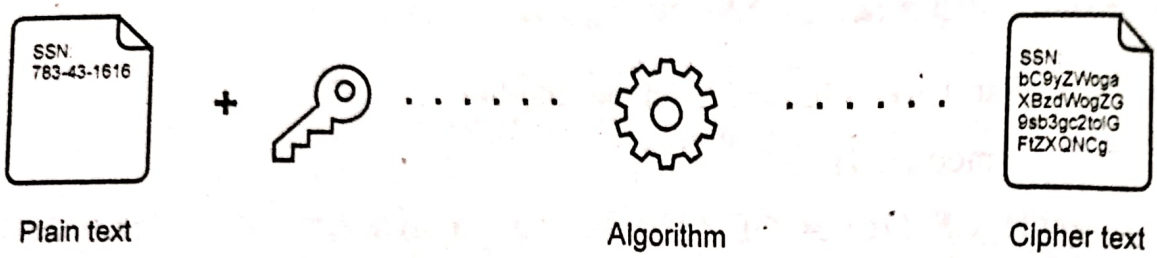


Fig. Q.3.1

- Encryption is a widely used security tool that can prevent the interception of sensitive data, either while stored in files or while in transit across networks.
- There are two types of encryption algorithms: symmetric (also called shared key algorithm) and asymmetric (also known as public key algorithm).

ii) Decryption : Decryption is a process that transforms encrypted information into its original format. Fig. Q.3.2 shows decryption process.

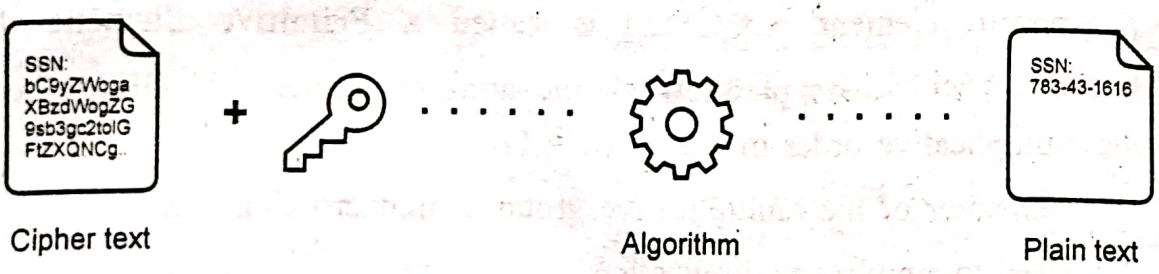


Fig. Q.3.2

Q.4 Explain following terms.

i) Cryptography ii) Symmetric key cryptography

iii) Asymmetric key cryptography ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. :

i) Cryptography : The original intelligible message, referred to as plaintext is converted into random nonsense, referred to as ciphertext. The science and art of manipulating messages to make them secure is called cryptography.

- An original message to be transformed is called the plaintext, and the resulting message after the transformation is called the ciphertext.
- The process of converting the plaintext into ciphertext is called encryption. The reverse process is called decryption. The encryption

process consists of an algorithm and a key. The key controls the algorithm.

- The objective is to design an encryption technique so that it would be very difficult or impossible for an unauthorized party to understand the contents of the ciphertext.

ii) Symmetric key cryptography :

- A symmetric encryption model has five ingredients.
  1. Plaintext
  2. Encryption algorithm
  3. Secret key
  4. Ciphertext
  5. Decryption algorithm
- Fig. Q.4.1 shows the conventional encryption model.

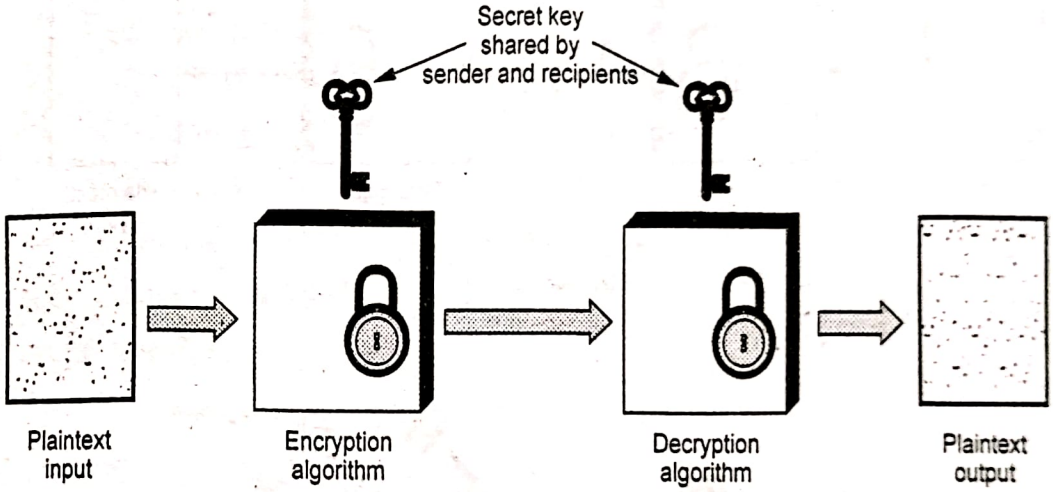
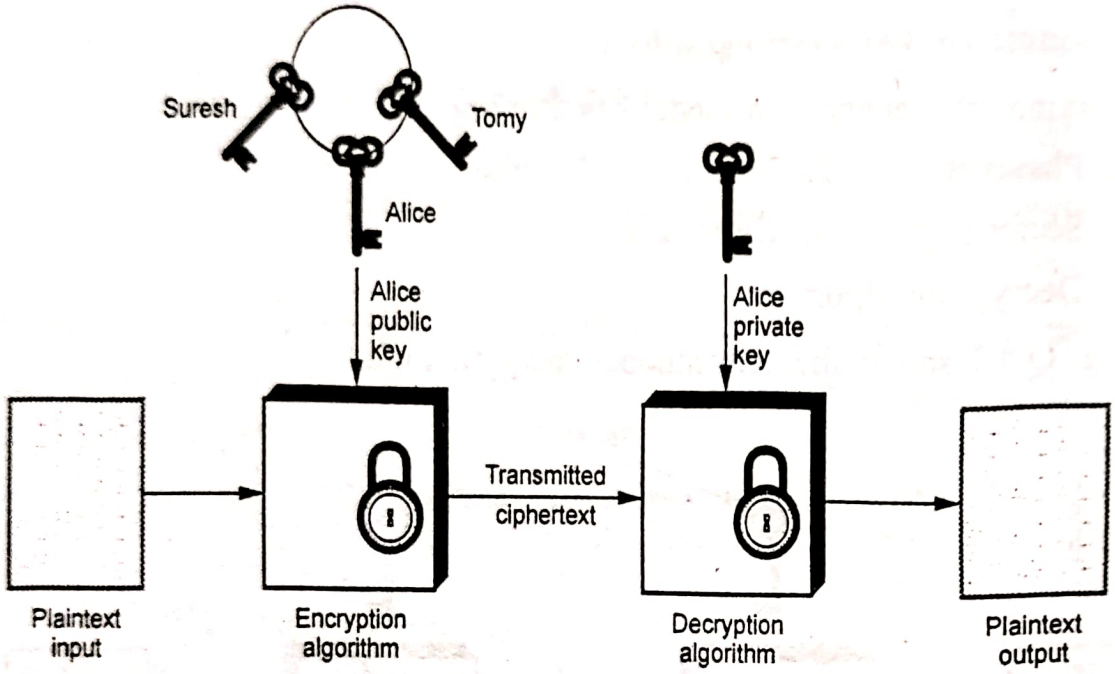


Fig. Q.4.1 Conventional encryption model

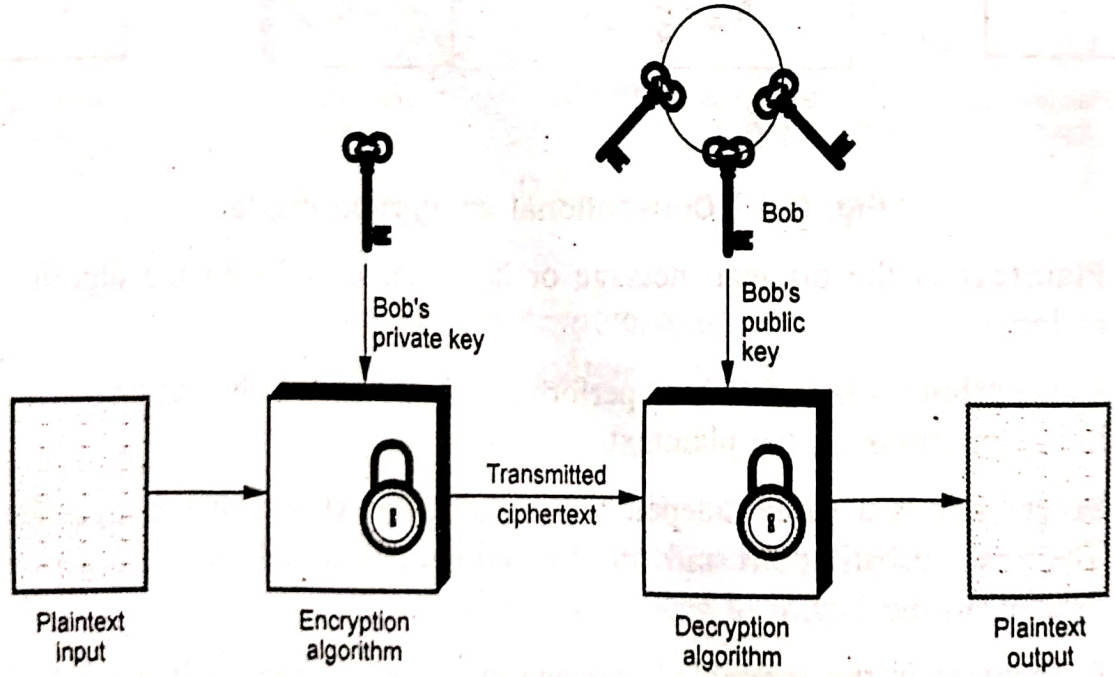
- **Plaintext** is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm** performs various substitutions and transformations on the plaintext.
- **Secret key** is a value independent of the plaintext and of the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext** is the scrambled message produced as output. It depends on the plaintext and the secret key.
- **Decryption algorithm** takes the ciphertext and the secret key and produces the original plaintext.

iii) Asymmetric key cryptography :

A public key encryption scheme has six ingredients. Fig. Q.4.2 shows public key cryptography.



(a) Encryption



(b) Authentication

Fig. Q.4.2 Public key cryptography

1. **Plaintext :** It is input to algorithm and in a readable message or data.
2. **Encryption algorithm :** It performs various transformations on the plaintext.
3. **Public and private keys :** One key is used for encryption and other is used for decryption.
4. **Ciphertext :** This is the scrambled message produced as output. It depends on the plaintext and the key.
5. **Decryption algorithm :** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

- The essential steps are the following :
  1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
  2. Each user places one of the two keys in a public register. This is the public key. The companion key is kept private.
  3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
  4. Alice decrypts the message using her private key.

Q.5 Explain advantages and disadvantages of symmetric key cryptography.

Ans. : Advantages of symmetric-key cryptography

1. High rates of data throughput.
2. Keys for symmetric-key ciphers are relatively short.
3. Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms (i.e. pseudorandom number generators).
4. Symmetric-key ciphers can be composed to produce stronger ciphers.
5. Symmetric-key encryption is perceived to have an extensive history.

Disadvantages of symmetric-key cryptography

1. Key must remain secret at both ends.
2. In large networks, there are many keys pairs to be managed.
3. Sound cryptographic practices dictates that the key be changed frequently.
4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys or the use of third trusted parties.

Q.6 Explain data encryption standards with diagram.

☞ [SPPU : Dec.-22, End Sem, Marks 9]

Ans. : • DES Encryption standard (DES) is **a symmetric key block cipher** published by the National Institute of Standards and Technology (NIST).

- It encrypts data in 64-bit block.
- DES is symmetric key algorithm : The same algorithm and key is used for both encryption and decryption.
- Key size is 56-bit.
- The encryption process is made of two permutations i.e. P-boxes, which is called initial and final permutation.
- DES uses both transposition and substitution and for that reason is sometimes referred to as a **product cipher**. Its input, output and key are each 64-bits long. The sets of 64-bits are referred to as **blocks**.
- The cipher consists of 16 rounds or iterations. Each rounds uses a separate key of 48-bits.
- Fig. Q.26.1 shows DES encryption algorithm. First, the 64-bit plaintext passes through an Initial Permutation (IP) that rearranges the bits to produce the permuted input. (See Fig. Q.26.1 on next page)
- Then there is a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.
- The output of the sixteenth round consists of 64-bits that are a function of the input plaintext and the key.
- The left and right halves of the output are swapped to produce the pre-output. At last, the pre-output is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

Initial permutation

- Table shows the initial permutation and its inverse. The input to a table consist of 64-bits numbered from 1 to 64.
- The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered input bit in the output, which also consists of 64-bits.

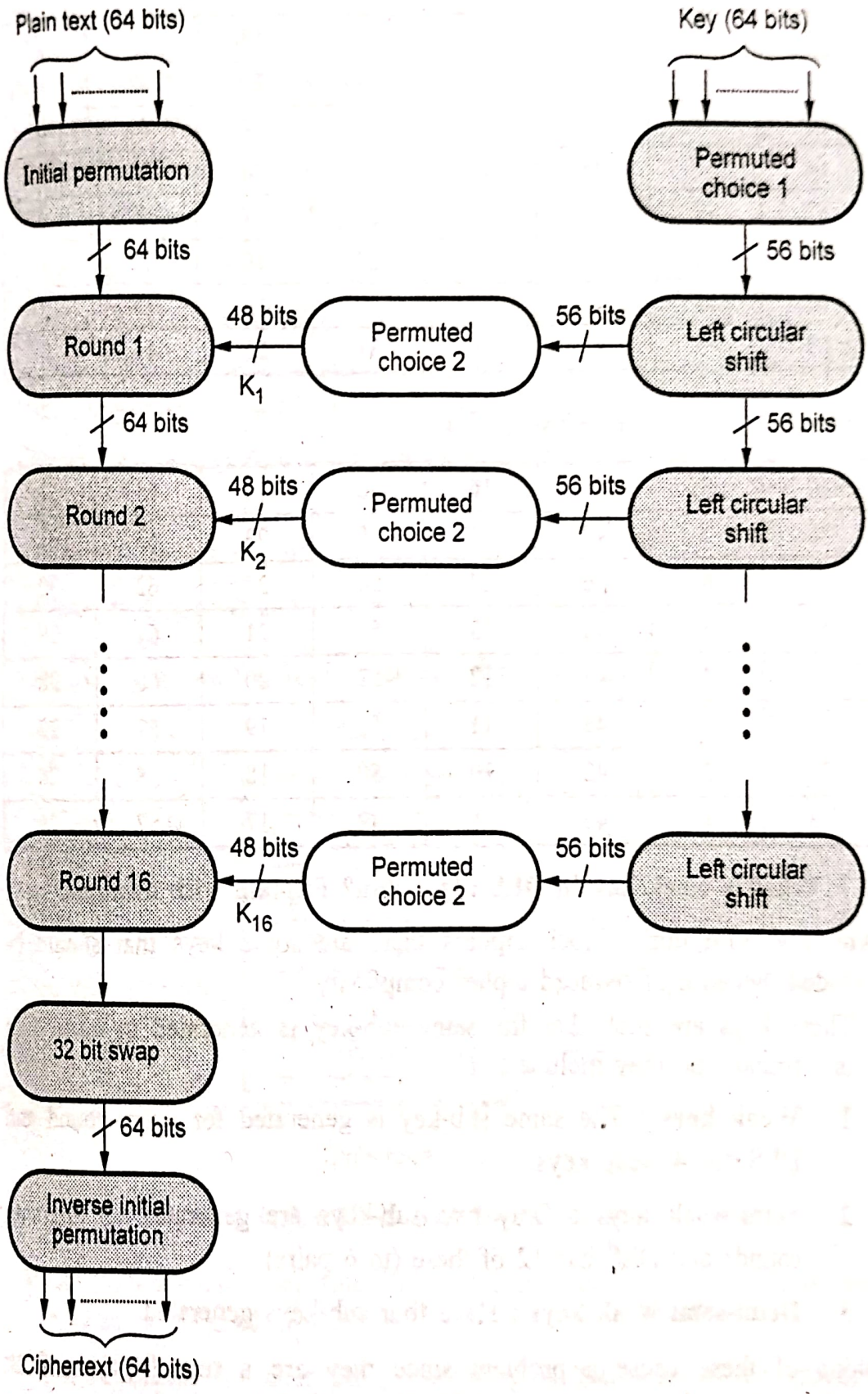


Fig. Q.6.1 DES encryption algorithm

Initial Permutation (IP) table

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	2.1	13	5
63	55	47	39	31	23	15	7

Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Q.7 What is weak key in DES algorithm? Explain with example.

Ans. : • With many block ciphers there are some keys that should be avoided, because of reduced cipher complexity.

- These keys are such that the same sub-key is generated in more than one round, and they include :

1. **Weak keys :** The same sub-key is generated for every round and DES has 4 weak keys.
2. **Semi-weak keys :** Only two sub-keys are generated on alternate rounds and DES has 12 of these (in 6 pairs).
3. **Demi-semi weak keys :** Have four sub-keys generated.

None of these cause a problem since they are a tiny fraction of all available keys however they MUST be avoided by any key generation program.

Q.8 Explain the operation of triple DES algorithm.

Ans. : • Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits.

- The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name triple DES.
- Triple DES uses 2 or 3 keys.
- The data is encrypted with the first key (K_1), decrypted with the second key (K_2), and finally encrypted again with the third key (K_3).
- Triple DES with three keys is used quite extensively in many products including PGP and S/MIME.
- Brute force search impossible on Triple DES.
- Meet-in-middle attacks need 256 Plaintext-Ciphertext pairs per key
- Cipher text is produced as $C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$.
- Fig. Q.8.1 shows the 3DES method with three key.

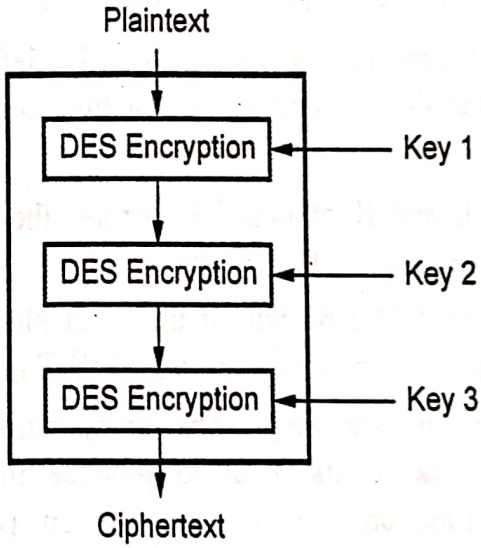


Fig. Q.8.1 3DES with three key method

- Triple DES runs three times slower than standard DES, but is much more secure if used properly.
- The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse.
- Like DES, data is encrypted and decrypted in 64-bit chunks.

- There are some weak keys that one should be aware of : if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES.
- The input key for DES is 64-bits long; the actual key used by DES is only 56-bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56-bits. This means that the effective key strength for Triple DES is actually 168-bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

Q.9 Explain DES encryption and decryption method.

Ans. : DES encryption :

- A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is inverse of the initial permutation IP.
- The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function KS, called the key schedule.
- Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R.

1. **Initial permutation :** The 64-bits of the input block to be enciphered are first subjected to the permutation, called the initial permutation.
2. **Key dependent computation :** The computation which uses the permuted input block as its input to produce the pre-output block consists. Cipher function *f* which operates on two blocks, one of 32-bits and one of 48-bits, and produces a block of 32-bits. Let the 64 bits of the input block in an iteration consist of a 32-bit block L followed by a 32-bit block R. Using the notation defined in the introduction the input block is then LR. Let K be a block of 48 bits chosen from the 64-bit key. Then the output L' R' of an iteration with input LR is defined by :

$$\left.\begin{aligned} L' &= R \\ R' &= L \,(+)\, f(R, K) \end{aligned}\right\} \quad \ldots (Q.9.1)$$

where (+) denotes bit-by-bit addition modulo 2.

As before, let the permuted input block be LR.

Finally, let L_0 and R_0 be respectively L and R and let L_n and R_n be respectively L' and R' of equation (Q.9.1) hence L and R are respectively L_{n-1} and R_{n-1} and K is K_n i.e. when *n* is in the range from 1 to 16,

Then $L_n = R_{n-1}$

$$R_n = L_{n-1} (+) f(R_{n-1}, K_n)T$$

The pre-output block is then $R_{16}L_{16}$.

3. **Key schedule :** Key generation techniques is shown in the Fig. Q.9.1. The input of the first iteration of the calculation is the permuted input block. If L' R' is the output of the 16th iteration then R'L' is the pre-output block. At each iteration a different block K of key bits is

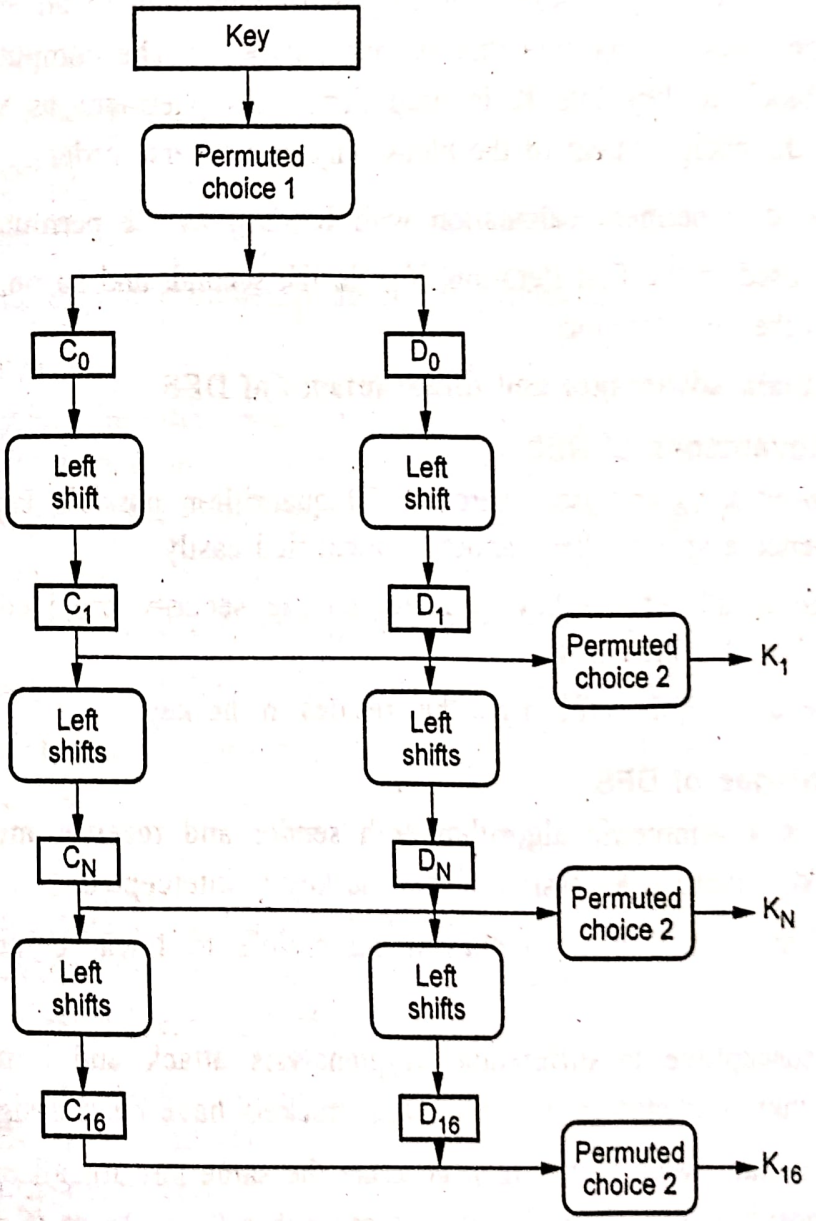


Fig. Q.9.1 Key generation techniques

chosen from the 64-bit key designated by KEY. Let KS be a function which takes a integer n in the range from 1 to 16 and a 64-bit block KEY as input and yields as output a 48-bit block K_n which is a permuted selection of bits from KEY i.e.

$$K_n = KS(n, KEY)$$

with K_n determined by thine bits in 48 distinct bit positions of KEY. KS is called the key schedule.

DES decryption :

- The permutation IP^{-1} applied to the pre-output block is the inverse of the initial permutation IP applied to the input. Consequently, to decipher it is only necessary to apply the very same algorithm to an enciphered message block, taking care that at each iteration of the computation the same block of key bits K is used during decipherment as was used during the encipherment of the block only in a reverse order.
- For the decipherment calculation with $R_{10}L_{10}$ as the permuted input, K_{10} is used in the first iteration, K_{10} in the second, and so on, with K_1 used in the 16^{th} iteration.

Q.10 Explain advantages and disadvantages of DES.

Ans. : Advantages of DES

1. As 56-bit keys are used there are 70 quadrillion possible key values and hence a specific key cannot be identified easily.
2. As the length of the key is increased the security provided by the algorithm also increases.
3. The security of the DES algorithm resides in the key.

Disadvantages of DES

1. As it is a symmetric algorithm both sender and receiver must have same key, there is a possibility that the key is intercepted.
2. The design of S boxes makes it susceptible to linear cryptanalysis attack.
3. It is susceptible to differential cryptanalysis attack and brute force attack taking advantage of which DES crackers have been designed.
4. It has certain weak keys which generate the same key for all cycles of the algorithm like when all key bits are either 0s or 1s or if one half

of the key bits are 0s or 1s. They are 0000000 0000000, 0000000 ffffffff, ffffffff 0000000, ffffffff ffffffff.

5. Some initial keys produce only two subkeys while some produce only four. They are called possible weak keys.

5.3 : Advanced Encryption Standard

Q.11 Explain operation of AES algorithm and state its application.

Ans. : AES :

- Advanced Encryption Standard (AES) is a symmetric key block cipher published by the NIST in December 2001.

Evaluation Criteria for AES

- NIST evaluation criteria for AES are
  1. Security
  2. Cost
  3. Algorithm and implementation characteristics.

1. Security

- This refers to the effort required to cryptanalyse an algorithm. Following parameters are also consider for evaluation.
  a. **Actual security** compared to other submitted algorithms.
  b. **Randomness** : The extent to which the algorithm output is indistinguishable from a random permutation on the input block.
  c. **Soundness** of the mathematical basis for the algorithm's security.
  d. Other security factors raised by the public during the evaluation process.

2. Cost

a. **Licensing requirements** : When the AES is issued, the algorithm specified in the AES shall be available on a worldwide, non-exclusive, royalty free basis.

b. **Computational efficiency** : The evaluation of computational efficiency will be applicable to both hardware and software implementations.

c. **Memory requirements** : The memory requirement for implementing the algorithm in hardware and software will be considered.

3. Algorithm and Implementation Characteristics

This category includes a variety of considerations, including flexibility, suitability for a variety of hardware and software implementations; and simplicity, which will make an analysis of security more straight forward.

The following criteria were used in the final evaluation. :

1. **General security** : NIST relied on the public security analysis conducted by the cryptographic community.
2. **Software implementations** : It includes execution speed, performs across a variety of platforms and variation of speed with key size.
3. Restricted space environments.
4. Hardware implementations.
5. Attacks on implementations.
6. Encryption versus decryptions.
7. Key agility.
8. Other versatility and flexibility.
9. Potential for instruction level parallelism.

Applications of AES :

1. AES can be used anywhere Symmetric Key cryptography is needed.
2. There is no particular list of applications of AES, but many banking systems use AES-128 and AES-256 to secure online banking or internet banking.

Q.12 Compare AES and DES.

Ans. :

Sr. No.	Parameters	AES	DES
1.	Block size	128-bits	64-bits
2.	Key length	128, 192, 256-bits	56-bits (effective length)

3.	Encryption primitives	Substitution, shift, bit mixing	Substitution, Permutation
4.	Cryptographic primitives	Confusion, Diffusion	Confusion, Diffusion
5.	Design rationale	Closed	Open

5.4 : Public Key Encryption and Hash Function : RSA

Q.13 Explain requirement of public key cryptography.

Ans. : Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

Q.14 Explain advantages and disadvantages of public key cryptography.

Ans. : • Advantages of public key algorithm

1. Only the private key must be kept secret.
2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
3. A private/public key pair remains unchanged for considerable long periods of time.
4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

- **Disadvantages of public key algorithm**
  1. Slower throughput rates than the best known symmetric-key schemes.
  2. Large key size.
  3. No asymmetric-key scheme has been proven to be secure.
  4. Lack of extensive history.

Q.15 Explain difference between symmetric and asymmetric key cryptography. ☞ **[SPPU : Dec.-22, End Sem, Marks 9]**

Ans. :

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast	Slower
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Q.16 Explain RSA in details. ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : • Public key cryptography means one key is used for encryption and other key for decryption. The public key is accessed to all participants and private key is generated locally by each participant.

RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n. RSA algorithm is public key encryption type algorithm. In this algorithm, one user uses a public key and other

user uses a secret (private key) key. In the RSA algorithm each station independently and randomly chooses two large primes p and q number and multiplies them to produce n = p x q which is the modulus used in the arithmetic calculations of the algorithm.

Key generation :

1) Pick two large prime numbers p and q, $p \neq q$;
2) Calculate $n = p \times q$;
3) Calculate $\phi(n) = (p - 1)(q - 1)$;
4) Pick e, so that gcd $(e, \phi(n)) = 1, 1 < e < \phi(n)$;
5) Calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e. d is the multiplicative inverse of e in mod $\phi(n)$;
6) Get public key as $K_U = \{e, n\}$;
7) Get private key as $K_R = \{d, n\}$.

Encryption : For plaintext block $P < n$, its ciphertext $C = P^e \bmod n$.

Decryption : For ciphertext block C, its plaintext is $P = C^d \bmod n$.

The modulus n must be selected in such a manner that the following is guaranteed :

$(M^e)^d) \equiv M^{ed} \equiv M \pmod n$

We want this guarantee because $C = M^e \bmod m$ is the encrypted form of the message integer M and decryption is carried out by $C^d \bmod n$.

We also need to ensure that n is not factorizable by one of the modern integer factorization algorithms.

- As we have seen from the RSA design, RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to $\phi(n)$, has exponential inverse in mod n.

- Its exponential inverse d can be calculated as the multiplicative inverse of e in mod $\phi(n)$. The reason is illustrated as follows :

  Based on Euler's theorem, for y which satisfies $y \bmod \phi(n) = 1$, the following equation holds :

  $x^y \bmod n = x \bmod n$

AS $d \cdot e \bmod \phi(n) = 1$, we have that $p^{ed} \equiv P \bmod n$. So the correctness of RSA cryptosystem is shown as follows :

Encyption : $C = P^e \bmod n$;

Decryption : $P = C^d \bmod n = (P^e)^d \bmod n = P^{ed} \bmod n = P \bmod n = P$.

Q.17 For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.

Ans. : $P = 3 \qquad Q = 19$

$N = PQ$

$= 3 \times 19$

$N = 57$

Calculate $\phi(n) = (P - 1)(Q - 1)$

$= (3 - 1)(19 - 1)$

$= 36$

Public key 'e' is calculated by using Euclid algorithm. Using 36, GCD is calculated and 5 and 7 gives GCD = 1

So you can select e = 5 or 7. Here we selected e = 7

So public key (7, 57)

Private key generation (d) :

Determine d such that $ed = 1 \bmod \phi(n)$

$7d = 1 \pmod{36}$

$7 \times 31 = 1 \pmod{36}$

So d = 31

Encryption of message :

Ciphertext (C) $= M^e \bmod n$

$= 6^7 \bmod 57$

$C = 9$

Q.18 Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.

Ans. : RSA algorithm :

$$N = p \times q = 7 \times 11$$

$$= 77$$

$$\text{Calculate } \phi(n) = (p - 1)(q - 1) = (7 - 1)(11 - 1)$$

$$= 6 \times 10$$

$$= 60$$

So, $e = 17$

Determine d such that

$$ed = 1 \bmod \phi(n)$$

$$17d = 1 \bmod 60$$

According to GCD :

$$60 = 17 * 3 + 9$$

$$17 = 9 * 1 + 8$$

$$9 = 8 * 1 + 1$$

$$8 = 1 * 8 + 0$$

Therefore, we have :

$$1 = 9 - 8$$

$$= 9 - (17 - 9)$$

$$= 9 - (17 - (60 - 17 * 3))$$

$$= 60 - 17 * 3 - (17 - 60 + 17 * 3)$$

$$= 60 - 17 * 3 + 60 - 17 * 4$$

$$= 60 * 2 - 17 * 7$$

Hence, we get,

$$d = e^{-1} \bmod f(n)$$

$$= e^{-1} \bmod 60$$

$$= -7 \bmod 60$$

$$= (53 - 60) \bmod 60$$

$$= 53$$

So, the public key is {17, 77} and the private key is {53, 77}

Encryption :

Ciphertext (C) = M^e mod N

= $(8)^{17}$ mod 77

C = 57

5.5 : Digital Signatures

Q.19 What is digital signature ? What are application of digital signature ? ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : • A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key.

- There are three parameters that are public and can be common to a group of users. **Prime number q** is chosen and it is **160-bit**. A **prime number p** is selected with a length between **512** and **1024 bits** such that q divides (p – 1).
- g is chosen to be of the form $h^{(P-1)/q}$ mod p where h is an integer between 1 and (p – 1)
- With these number, user selects a private key and generate a public key. The private key x must be a number from 1 to (q – 1) and should be chosen randomly or pseudorandomly.
- The public key is calculated from the private key as $y = g^x$ mod p.
- To create a signature, a user calculates two quantities, **r and s**, that are functions of

  i) Public key components (p, q, g) ii) User's private key (x)

  iii) Hash code of the message H(M) iv) An additional integer (K)

- **At the receiving end**, verification is performed. The receiver generates a quantity V that is a function of the public key components, the sender's public key and the hash code of the incoming message. If this quantity matches the r components of the signature, then the signature is validated.
- Fig. Q.19.1 shows the functions of signing and verifying.

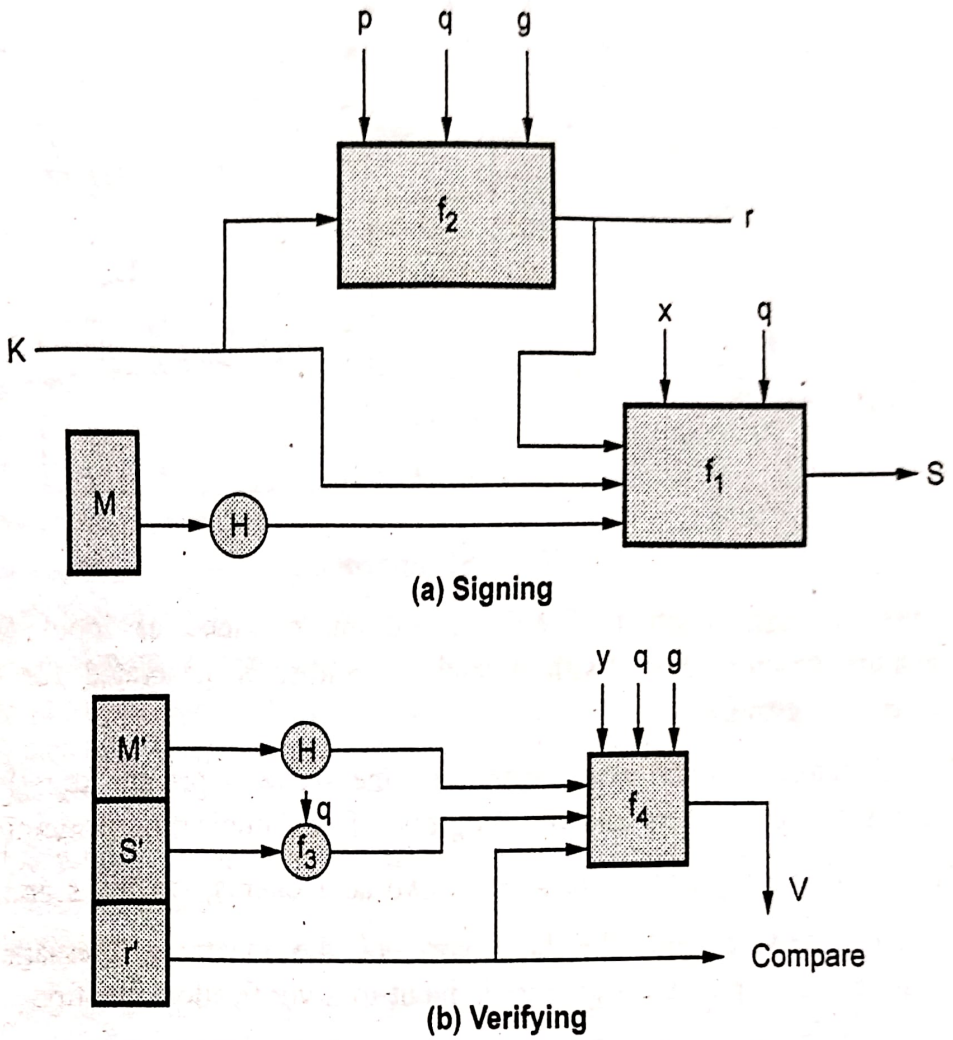


Fig. Q.19.1 Signing and verifying

Application of digital signature :

1. Financial sectors utilize digital signatures for mortgages, insurance documentation, loan processing, paperless banking, as well as contracts.
2. Manufacturing industries utilize digital signatures to help speed up the production processes such as manufacturing enhancements, Quality Assurance (QA), product design, sales and marketing.
3. In cryptocurrencies, security is crucial because hacking has become quite a sore issue in recent years. Fortunately, the cryptocurrency system helps guarantee security by using asymmetric cryptography to prove the legitimate owner of the crypto such as Bitcoin.

Q.20 Explain digital signature standard.

Ans. : • The Digital Signature Standard (DSS) makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, the

Digital Signature Algorithm (DSA). DSS cannot be used for encryption or key exchange. Fig. Q.20.1 shows the DSS approach.

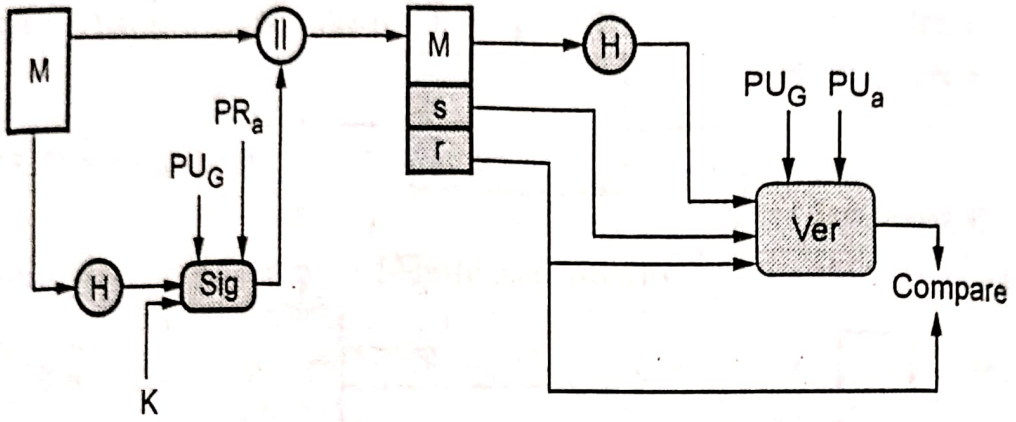


Fig. Q.20.1 DSS approach

- It uses a hash function. The hash code is provided as input to a signature function along with a random number K generated for this particular signature.
- The signature function also depends on the sender's private key (PR_a) and a set of parameters known to a group of communicating principles.
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated. This plus the signature is input to a verification function.
- Fig. Q.20.2 shows the RSA approach. In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted.

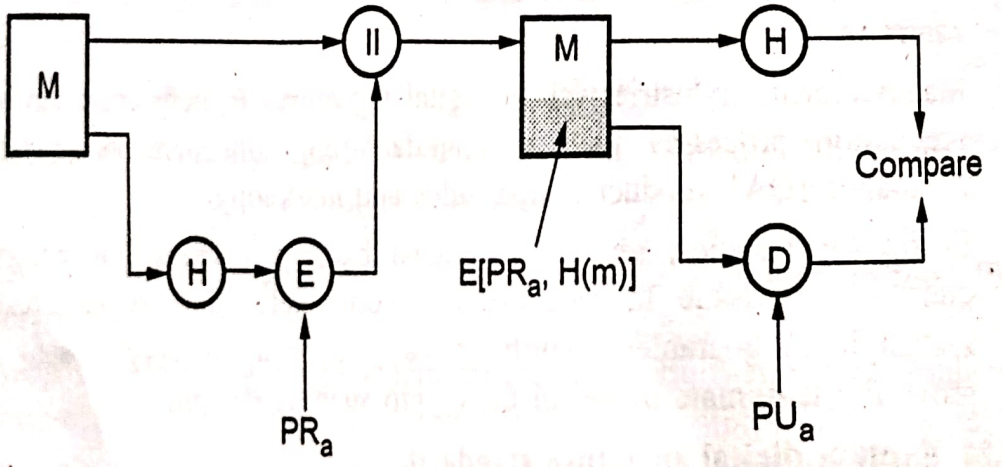


Fig. Q.20.2 RSA approach

- The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid.

5.6 : Digital Certificates

Q.21 Write short note on digital certificate.

Ans. : • A data structure that securely binds an individual or entity to a public key used in cryptographic operations such as digital signatures or asymmetric encryption.

- To obtain digital certificate an organization must apply to a certification authority which is responsible for validating and ensuring the authenticity of requesting organization. The certificate will identify the name of the organization, a serial number, the validity date and the organization's public key where encryption to / from that organization is required.
- In addition, the digital certificate will also contain the digital signature of the certification authority to allow any recipient to confirm the authenticity of the digital certificate.
- A digital certificate is an ID that is carried with a file. To validate a signature, a certifying authority validates information about the software developers and then issues them digital certificates. The digital certificate contains information about the person to whom the certificate was issued, as well as information about the certifying authority that issued it. When a digital certificate is used to sign programs, ActiveX controls, and documents, this ID is stored with the signed item in a secure and verifiable form so that it can be displayed to a user to establish a trust relationship.
- A digital certificate allows unique identification of an entity; it is essentially an electronic ID card, issued by a trusted third party. Digital certificates form part of the ISO authentication framework, also known as the X.509 protocol. This framework provides for authentication across networks.
- A digital certificate serves two purposes : It establishes the owner's identity, and it makes the owner's public key available. A digital certificate is issued by a Certification Authority (CA). It is issued for only a limited time and when its expiry date has passed, it must be replaced.

- A digital certificate consists of :
  1. The public key of the person being certified
  2. The name and address of the person being certified, also known as the Distinguished Name (DN)
  3. The digital signature of the CA.
  4. The issue date
  5. The expiry date
- The Distinguished Name is the name and address of a person or organization. You enter your Distinguished Name as part of requesting a certificate. The digitally-signed certificate includes not only your own Distinguished Name, but the Distinguished Name of the CA, which allows verification of the CA.
- To communicate securely, the receiver in a transmission must trust the CA that issued the certificate that the sender is using. This means that when a sender signs a message, the receiver must have the corresponding CA's signer certificate and public key designated as a trusted root key. For example, your web browser has a default list of signer certificates for trusted CAs. If you want to trust certificates from another CA, you must receive a certificate from that CA and designate it as a trusted root key.
- If you send your digital certificate containing your public key to someone else, what keeps that person from misusing your digital certificate and posing as you? The answer is: your private key.
- A digital certificate alone is not proof of anyone's identity. The digital certificate allows verification only of the owner's identity, by providing the public key needed to check the owner's digital signature. Therefore, the digital certificate owner must protect the private key that belongs with the public key in the digital certificate. If the private key were stolen, anyone could pose as the legitimate owner of the digital certificate.

5.7 : Diffie Hellman Key Exchange

Q.22 Explain Diffie hellman key exchange in detail.

☞ **[SPPU : Dec.-22, End Sem, Marks 9]**

Ans. : • The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

- The protocol has two system parameters p and g. They are both public and may be used by all the users in a system.
- Parameter p is a prime number and parameter g is an integer less than p, with the following property :
  1. For every number n between 1 and p – 1 inclusive.
  2. There is a power k of g such that $n = g^k \bmod p$.
- The protocol depends on the discrete logarithm problem for its security. It assumes that it is computationally infeasible to calculate the shared secret key $k = g^{ab} \bmod p$ given the two public values $g^a \bmod p$ and $g^b \bmod p$ when the prime p is sufficiently large.
- The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.
- Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows :
  1. First, Alice generates a random private value a and Bob generates a random private value b.
  2. Both a and b are drawn from the set of integers. They derive their public values using parameters p and g and their private values.
  3. Alice's public value is $g^a \bmod p$ and Bob's public value is $g^b \bmod p$.
  4. They then exchange their public values.
  5. Finally, Alice computes $g^{ab} = (g^b)^a \bmod p$.
  6. Bob computes $g^{ba} = (g^a)^b \bmod p$.
  7. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

Algorithm :

- Select two numbers (1) prime number q (2) α an integer that is a primitive root of q.
- Suppose the users A and B wish to exchange a key.

1. User A select a random integer $X_A < q$ and computes
   $Y_A = \alpha^{X_A} \bmod q$.
2. User B selects a random integer $X_B < q$ and compute
   $Y_B = \alpha^{X_B} \bmod q$.
3. Both side keeps the X value private and makes the Y value available publicly to the other side.
4. User A computes the key as $K = (Y_B)^{X_B} \bmod q$.
5. User B computes the key as $K = (Y_A)^{X_B} \bmod q$.

- Both side gets same results :

$$K = (Y_B)^{X_A} \bmod q$$
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$
$$= (\alpha^{X_B})^{X_A} \bmod q$$
$$= \alpha^{X_B X_A} \bmod q$$
$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$
$$= (Y_A)^{X_B} \bmod q$$

Example

- Key exchange is based on the use of the prime number and a primitive root of prime number.
- Prime number $q = 353$
  Primitive root $\alpha = 3$
- A and B select secret keys.
  $X_A = 97$ $X_B = 233$
- Calculates the public keys

A computes $Y_A = \alpha^{X_A} \bmod q$
$= (3)^{97} \bmod 353$
$= (1.9080 \times 10^{97}) \bmod 353 = 40$

B computes $Y_B = \alpha^{X_B} \bmod q$
$= (3)^{233} \bmod 353$
$= (1.4765 \times 10^{111}) \bmod 353 = 248$

- After they exchange public keys, each can compute the common *secret key*.

A computes $K = (Y_B)^{X_A} \bmod q = (248)^{97} \bmod 353$

$= (1.8273 \times 10^{232}) \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353$

$= (1.9053 \times 10^{373}) \bmod 353 = 160$

Q.23 Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root $\alpha = 2$.

i) If user A has the public key $Y_A = 9$; what is A's private key X_A ?

ii) If user A has a public key $Y_A = 3$; what is the shared secret key X_A ?

Ans. : i) $q = 11$, $\alpha = 2$, $Y_A = 9$, $X_A = ?$

$2 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

Since $2^e \bmod 11$ for $0 < i < 11$ contains all numbers from 1 to 11 – 1, the size of this set is equal to $\phi(q)$, the order of q.

From the above values $2^6 \bmod 11 = 9$ therefore $X_A = 6$

ii) From the above values

$\alpha^{X_A} \bmod 11 = Y_A$

$2^{X_A} \bmod 11 = 3$

$2^{X_8} \bmod 11 = 3$

$\therefore \quad X_A = 8$

5.8 : Hash Function

Q.24 What is hash function ? How hash is generated ? Explain.

Ans. : • A hash function takes an input m, and computes a fixed size string known as a hash. Unlike a MAC, a hash code does not use a key but is a function only of the input message.

- **Definition :** A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values.
- The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or simply digests.
- A hash function maps a variable-length input into a fixed-length output. This hash function output can be treated as a fingerprint of the input data. A very simple example of hash function is modulo operation. Hash functions have been used in many fields of computer science such as hash table in data structure, checksum algorithms for error detection, digital signature in information security etc.
- The most common cryptographic uses of hash functions are with digital signatures and for data integrity.
- When hash functions are used to detect whether the message input has been altered, they are called Modification Detection Codes (MDC).
- There is another category of hash functions that involve a secret key and provide data origin authentication, as well as data integrity; these are called Message Authentication Codes (MACs).
- A hash value h is generated by a function H of the form.

$$h = H(M)$$

where M = Variable - Length message

$H(M)$ = Fixed - Length hash value.

- Hash code is also referred to as a message digest or hash value. A change to any bit or bits in the message results in a change to the hash code.
- Fig. Q.24.1 (a) shows the basic uses of hash function.

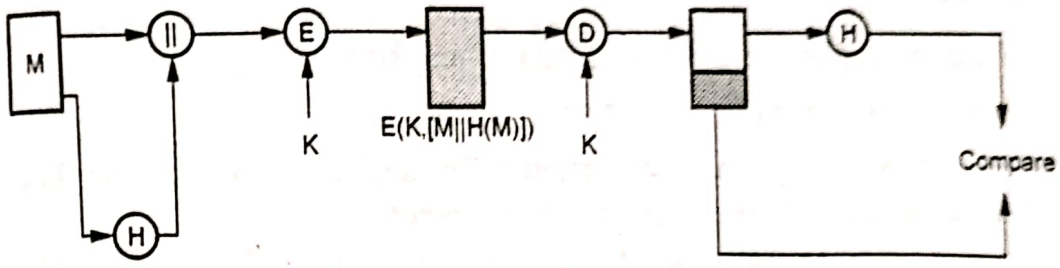


Fig. Q.24.1 (a) Encrypt message plus hash code

1. **Encrypt message plus hash code.**
   - Provide confidentiality : Only A and B share K.
   - Provides authentication : H(M) is cryptographically protected.
2. **Encrypt hash code - shared secret key**
   - Only the hash code is encrypted, using symmetric encryption.
   - Reduces the processing burden for those applications that do not require confidentiality.

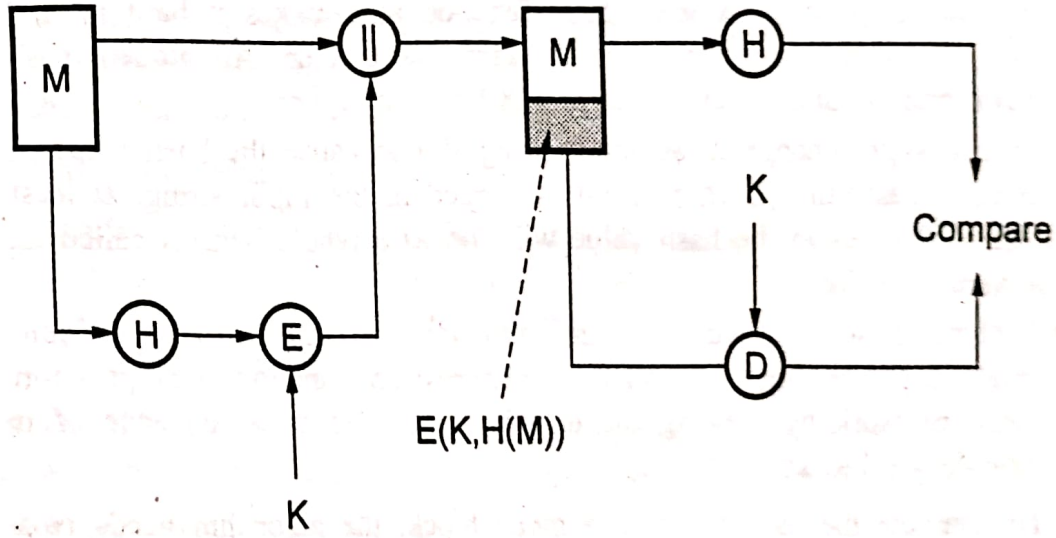


Fig. Q.24.1 (b) Encrypt hash code - shared secret key

Q.25 What are requirement of hash function ?

Ans. : The purpose of a hash function is to produce a fingerprint of a file, message or other block of data.

Properties

1. H can be applied to a block of data of any size.
2. H produces a fixed length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that
   H(x) = h. This is called one-way property.
5. For any given block x, it is computationally infeasible to find $y \neq x$ such that H(y) = H(x). This is called as **weak collision** resistance.
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is called as **strong collision** resistance.

Q.26 Write short note on one way hash function.

Ans. : • A one-way hash function is also known as a message digest, fingerprint or compression function. It is a mathematical function and takes a variable-length input string and converts it into a fixed-length binary sequence.

- One-way hash function is designed in such a way that it is hard to reverse the process. A good hash function also makes it hard to find two strings that would produce the same hash value. All modern hash algorithms produce hash values of 128 bits and higher.
- Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an **avalanche effect**.
- A common way for one-way hash functions to deal with the variable length input problem is called a compression function. Compression functions work by viewing the data being hashed as a sequence of n fixed-length blocks.
- To compute the hash value of a given block, the algorithm needs two things : The data in the block and an input seed.
- The input seed is set to some constant value, c, and the algorithm computes the hash value h_1 of the first block. Next, the hash value of the first block, h_1 is used as the seed for the second block.
- The function proceeds to compute the hash value of the second block based on the data in the second block and the hash value of the first

block, h_1. So, the hash value for block n is related to the data in block n and the hash value h_{n-1} (for $n > 1$). The hash value of the entire input stream is the hash value of the last block.

5.9 : The PKIX Model

Q.27 Explain various public key distribution approaches.

Ans. : Different methods have been proposed for the distribution of public keys. These are

1. Public announcement 2. Publicly available directory
3. Public key authority 4. Public key certificates

- **Public announcement :** In public key algorithm, any participant can send his or her public key to any other participant or broadcast the key to the community at large.
- Because of the growing popularity of PGP, which makes use of RSA, many PGP users have adopted the practice of appending their public key to messages that they send to public forums, such as USENET new groups and Internet mailing lists.
- **Public available directory :** Greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization.
- **Public key authority :** User uses third party for key distribution.
- **Public key certificates :** Certificates can be used by participants to exchange keys without contacting a public key authority. Certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party.
- The third party is a certificate authority, such as government agency or a financial institution, that is trusted by the user community.
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate.

Q.28 What is PKI ? List benefits and limitation of PKI.

Ans. : • Public Key Infrastructure (PKI) is a well-known technology that can be used to establish identities, encrypt information and digitally sign documents.

- PKI identifies and manages relationships of parties in an electronic exchange, serving a wide array of security needs including access control, confidentiality, integrity, authentication and non-repudiation.
- PKI also uses unique Digital Certificates (DC) to secure eCommerce, email, data exchange and Virtual Private Networks (VPN) and intranets and is also used to verify the identity and privileges of each user.
- The Certificate Authority (CA) provides a full life-cycle management of public keys and certificates, including issuance, authentication, storage, retrieval, backup, recovery, updating and revocation to the PKI.
- All users of PKI must have a registered identity, which is stored in a digital certificate issued by a CA.
- Remote users and sites using public private keys and public key certificates can authenticate each other with a high degree of confidence.
- Authentication is dependent on three conditions :
  1. It must be established that each party have a private key that has not been stolen or copied from the owner.
  2. The certificate must be issued to the owner in accord with the stated policy of the certificate issuer.
  3. The policies of the certificate issuer must be satisfactory to the parties so as to verify identity.

Benefits of PKI

1. **Confidential communication :** Only intended recipients can read files.
2. **Data integrity :** Guarantees files are unaltered during transmission.
3. **Authentication :** Ensures that parties involved are who they claim to be.
4. **Non-repudiation :** Prevents individuals from denying.

Limitation of PKI

The problems encountered deploying a PKI can be categorized as follows :

1. Public key infrastructure is new
2. Lack of standards
3. Shortage of trained personnel
4. Public key infrastructure is mostly about policies.

END...

Unit VI

6 Introduction to Cyber Security

6.1 : Introduction to Cyber Security

Q.1 What is cyberspace ?

Ans. : • Cyberspace : The impression of space and community formed by computers, computer networks, and their users; the virtual "world" that Internet users inhabit when they are online.

- The cyber space includes computer systems, computer networks and Internet. LAN and WAN is also part of cyber space. Cybercrime incorporates anything from downloading illegal music files to stealing millions of rupees from online bank accounts.

Q.2 Give real life example of cyber attacks.

Ans. :

1. Cyber-attack will get in control of a food manufacturer factory altering the levels of additives in order to poison the consumers. The food may be delivered to a big number of countries and internationally, thus causing global problems.
2. A cyber-attack will get in control of an air traffic control system of an international airport. The system may be either brought down or provide altered information to airplanes, which may result in possible crash and loss of lives. The intrusion may also be extended to altering the data the pilots are getting from in-cockpit sensors, which may cause their severe confusion.
3. The cyber-attack will bring down stock exchanges and get in control of thousands of bank accounts for the purpose of undermining the confidence in the financial system. Failure of the economic system follows as people are trying to run the banks in order to save their money.

Q.3 What is cyberactivity ? Give example.

Ans. : • Cyberactivists are individuals who perform cyber attacks for pleasure, philosophical, political, or other nonmonetary reasons.

- Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist" such as a member of the cyber-group Anonymous who undertakes an attack for political reasons.
- The activities of these groups can range from nuisance-related denial of service attacks and website defacement to disrupting government and private corporation business processes.

Q.4 Define information security.

Ans. : Information security is refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection. It is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information

6.2 : Attack Vector

Q.5 What is attack vector ? Explain what are the different attack launched with attack vector.

Ans. : • An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.

- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

1. **Code tampering :** This type of attacks are conducted from outside of a client's, by probing open ports and trying to force the code behind those ports to do unwanted actions, allowing hackers either remote execution, illegal upload with further execution, or system crash.
2. **Brute force :** An attacker uses techniques that are trying multiple combinations of passwords and keys trying to pick correct combination.
3. **Denial attack :** When an attacker creates either a large number of requests or specifically crafted requests or both at the same time to cause a client's system to stop responding.

4. **Floods :** An attacker creates large amount of traffic, produced by hacker's controlled infected machines - "bots or zombies" to simply overflow capacities of the client networks or their ISPs.
5. **Browser scripting attacks :** During this attack, a hacker is convincing a user to go to a malicious website. Such website has a java or other scripting code that cause client's browser to perform unwanted actions, infect the computer, download unwanted software, etc.
6. **Email attacks :** During this attack, a hacker tricks a user to open an attachment that has a code that causes the opening program such as MS Office, Adobe PDF viewer, etc. to perform unwanted actions, such as infect the computer, download unwanted software etc.

6.3 : Malware

Q.6 Write short note on Malware. ☞ **[SPPU : June-22, End Sem, Marks 3]**

Ans. : The generic term for threats is malicious software or malware. **Malware** is software designed to cause damage to or use up the resources of a target computer.

Malicious Programs

- Fig. Q.6.1 provides an overall taxonomy of malicious software. These threat can be divided into two categories those that need a host program and those that are independent. Which requires host programs are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.

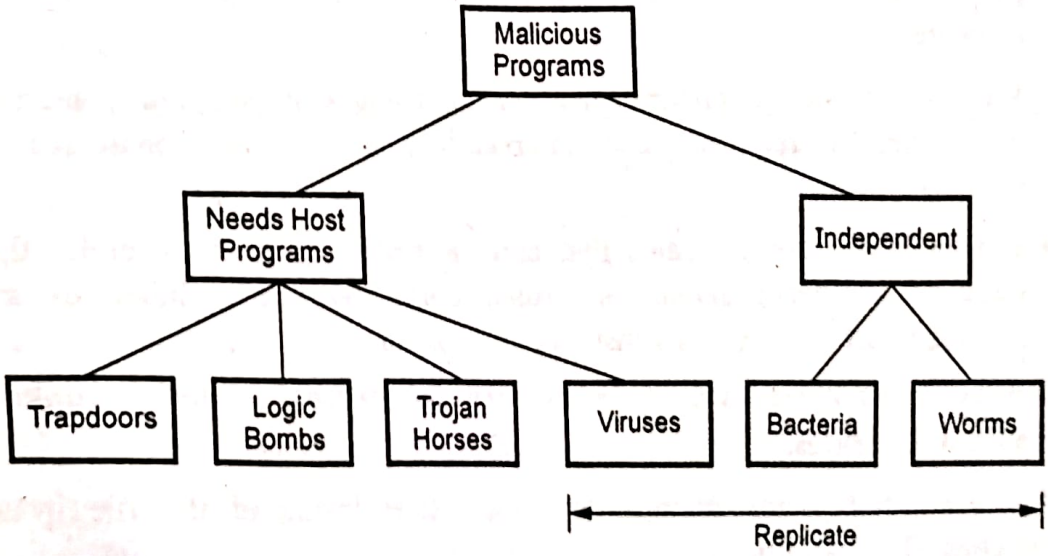


Fig. Q.6.1 Taxonomy of malicious programs

- Second category i.e. independent programs are self contained programs that can be scheduled and run by the operating system.

Q.7 What is virus ? List its components.

Ans. : • A computer virus is a small program that can copy itself to infect computers. Self-replicating programs that spread by infecting other programs or data files. A Virus is a malicious program that spreads using a propagation technique that generally requires user intervention, and always possesses a malicious intent.

- A computer virus requires some sort of user action to abet their propagation. A virus program infects other programs by modifying them.
- A major **component of virus** is an infection code, payload and trigger.
  1. Infection code : This is the part that locates an infectable object.
  2. Payload : Any operation that any other program can do but is usually something meant to be possibly destructive.
  3. Trigger : Whatever sets it off, time-of-day, program execution by user.

Q.8 Explain how is a virus different from a Trojan horse ?

Ans. : Virus : Computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another.

- **Trojan horse** is a program that conceals its purpose, it claims to do one thing but really does another. Trojan horses are also often used to gain access to a computer system to run monitoring or shadowing software.
- **Virus** is a malicious program that spreads using a propagation technique that generally requires user intervention, and always possesses a malicious intent.
- **Trojan** horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program.

Q.9 State the reason why a cavity virus is difficult to detect unlike traditional viruses.

Ans. : • Cavity virus attempts to install itself inside of the file it is infecting. This is difficult.

- Most viruses take the easy way out when infecting files; they simply attach themselves to the end of the file and then change the start of the program so that it first points to the virus and then to the actual program code.
- Many viruses that do this also implement some stealth techniques so you don't see the increase in file length when the virus is active in memory.
- A cavity virus, on the other hand, attempts to be clever. Some program files, for a variety of reasons, have empty space inside of them. This empty space can be used to house virus code.
- A cavity virus attempts to install itself in this empty space while not damaging the actual program itself.
- An advantage of this is that the virus then does not increase the length of the program and can avoid the need for some stealth techniques. The Lehigh virus was an early example of a cavity virus.
- Because of the difficulty of writing this type of virus and the limited number of possible hosts, cavity viruses are rare.

Q.10 What are the phases of viruses ?

Ans. : • During its lifecycle, virus goes through following phases :

1. Dormant phase
2. Propagation phase
3. Triggering phase
4. Execution phase

- **Dormant phase :** The virus is idle. It is activated by some event.
- **Propagation phase :** During this phase, the virus is replicating itself, infecting new files on new systems. Virus will typically not propagate to another infected program.
- **Triggering phase :** The virus is activated to perform the function for which it was intended. It is caused by a variety of system events.
- **Execution phase :** In this phase, the virus performs the malicious action that it was designed to perform, called payload. This action could include something seemingly innocent, like displaying a silly picture on a computer's screen, or something quite malicious, such as deleting all essential files on the hard drive.

Q.11 Explain virus countermeasures.

Ans. : • Prevention is best solution for virus. A countermeasure is an action, process, device, or system that can prevent, or mitigate the effects of, threats to a computer, server or network.

- Antivirus software mainly prevents and removes computer viruses, including worms and trojan horses. Such programs may also detect and remove adware, spyware, and other forms of malware.

1. **Prevention :** Do not allow a virus to get into the system.
2. **Detection :** Once infection has occurred, determine that it has occurred and locate the virus;
3. **Identification :** Once a virus is detected, identify it;
4. **Removal :** Once the specific virus has been identified, remove all traces of the virus and restores the infected programs to their original states.

Q.12 What is worm ? Explain classification of worm.

Ans. : • A worm is a sophisticated piece of replicating code that uses its own program coding to spread, with minimal user intervention. A worm usually exists as a standalone program that executes itself automatically on a remote machine, without any user interaction. Worms are network viruses, primarily replicating on networks.

- Worm infects the environment rather than specific objects. Unlike a virus, does not require a host to propagate.
- The Morris worm or Internet worm was one of the first computer worms distributed via the Internet. Morris worm uses topological techniques. Topological worm searches for local information to find new victims by trying to discover the local communication topology.
- Passive worm does not seek out victim machines. Instead, it either waits for potential victims to contact the worm or rely on user behavior to discover new targets.

Worm Classification

- Worms can be classified according to the following categories :

1. **Stealth worms** do not spread in a very rapid fashion but instead they spread in a slow. This worm is very hard to detect.
2. **Polymorph worms** can change themselves during propagation in order to make signature-based detection more complicated.
3. **File worms** are a modified form of viruses, but unlike viruses they do not connect their presence with any executable file. When they multiply, they simply copy their code to some other disk or directory hoping that these new copies will someday be executed by the user.

4. **Multi-vector worms** use different propagation methods in order to make more hosts vulnerable for attack and effectively propagate behind firewalls.
5. **Email worms** email themselves to other email addresses and make the user execute email attachments with malicious code or use bugs in the email programs to get attachments executed automatically.

Q.13 Explain difference between worm and virus.

Ans. :

Worm	Virus
A worm has ability to self-propagate, and may or may not have malicious intent computer worm is a program that self-propagates across a network exploiting security or policy flaws.	A Virus is a malicious program that spreads using a propagation technique that generally requires user intervention, and always possess a malicious intent.
Worms do not need hosts.	Virus needs hosts.
Worm can spread quicker than virus.	Virus can spread slower than worm.
Example : Self modified virus, stealth virus.	Example : Multi-vector worm, Email worm.

Q.14 What is trojan horse ? What is objective of trojan horse? Explain its types.

Ans. : • Trojan horse is malicious code hidden in an apparently useful host program. When the host program is executed, trojan does something harmful or unwanted.

- Trojan horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program. The Trojan horse could create a backdoor or replace a valid program during installation.

Objectives of trojan horse programs

1. It creates a backdoor and allows remote access to control your computer.
2. Keystrokes are recorded to steal password and bank account information.
3. Destroy or delete data.

4. Uploading or downloading files.
5. Your activity is monitored by camera and send to remote location.

Types of trojan horses

1. Remote access trojans
2. Data sending trojans
3. Destructive trojans
4. Proxy trojans
5. FTP trojans
6. Security software disabler trojans
7. Denial-of-service attack trojans

6.4 : Phishing

Q.15 Write short note on phishing. ☞ **[SPPU : June-22, End Sem, Marks 3]**

Ans. : • Phishing attacks usually will involve an email that appears to be from a company with which user do business prompting user to take action and log in to account with the link provided in the email.

- The Web site user visit is not the real site but a cleverly designed imposter site that may seem real to you, so user will enter your username and password, which is then captured by the attacker.
- **Phishing :** Attempting to criminally acquire sensitive information, such as usernames and passwords, by masquerading as trustworthy entities
- Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies. The purpose of a phishing message is to acquire sensitive information about a user. For doing so the message needs to deceive the intended recipient.

Q.16 How to avoid being a phishing victim ?

Ans. :

1. Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name. Never respond to requests for personal information via email. When in doubt, call the institution that claims

to have sent you the email.
For example, "Dear Sir or Madam" rather than "Dear Dr. Palve".

2. If you suspect the message might not be authentic, don't use the links within the email to get to a web page. Retype the address in a new window.
3. Never fill out forms in email messages that ask for confidential information.
4. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser.
   - Check the beginning of the Web address in your browsers address bar.
   - It should be 'https://' rather than just 'http://'
   - Look for the locked padlock icon on your URL bar.
5. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate and if anything is suspicious, contact your bank and all card issuers immediately.
6. Ensure that your browser and OS software is up-to-date and that latest security patches are applied. Keep antivirus definitions updated.
7. Verify the real address of a website. Phishers also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters.

Q.17 Explain buffer overflow with example.

Ans. : • The main cause for the problem of buffer overflow vulnerabilities is the fact that in many languages, such as C, bounds are not checked when arrays are accessed.

- Buffer is a contiguous block of computer memory that holds multiple instances of the same type. Overflow means to fill more than full. Buffer Overflow happens when a program attempts to write data outside of the memory allocated for that data.
- In buffer overflow attacks, the extra data may contain codes des... to trigger specific actions, in effect sending new instructio... attacked computer that could, for example, damage the ... change data, or disclose confidential information.
- Fig. Q.17.1 shows buffer overflow attack.

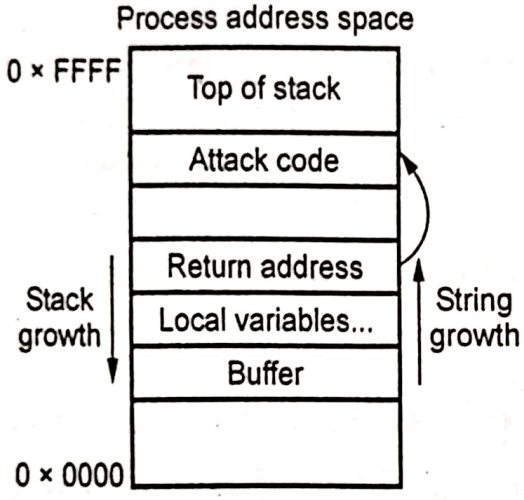


Fig. Q.17.1 buffer overflows attack

- The stack is a section of memory used for temporary storage of information. In a stack-based buffer overflow attack, the attacker adds more data than expected to the stack, overwriting data.
- For example, "Let's say that a program is executing and reaches the stage where it expects to use a postal coder or zip code, which it gets from a web-based form that customers filled out."
- The longest postal code is fewer than twelve characters, but on the web form, the attacker typed in the letter "A" 256 times, followed by some other commands.
- The data overflows the buffer allotted for the zip code and the attacker's commands fall into the stack. After a function is called, the address of the instruction following the function call is pushed onto the stack to be saved so that the function knows where to return control when it is finished.
- A buffer overflow allows the attacker to change the return address of a function to a point in memory where they have already inserted executable code. Then control can be transferred to the malicious attack code contained with the buffer, called the payload.
- The payload is normally a command to allow remote access or some other command that would get the attacker closer to having control of the system.
- C language example :

```
#define BUFSIZE 128
int main (int argc, char **argv)
```

```
{
  char buf[BUFSIZE];
  strcpy(buf, argv[1]);
}
```

- The buffer size is fixed, but there is no guarantee the string in argv[1] will not exceed this size and cause an overflow.

Q.18 Explain types of buffer overflows.

Ans. : Buffer overflows are of two types :

1. Stack based buffer overflows

- A stack is contiguous block of memory which is used by functions, two instructions are used to put or remove data from stack, "PUSH" puts data on stack, & "POP" removes data from stack. The stack works on Last in First out "LIFO" basis.
- Stack based buffer overflows affects any function that copies input to memory without doing bounds checking. For example: Strcpy(), memcpy(), gets() etc.
- A buffer overflow occurs when a function copies data into a buffer without doing bounds checking. So if the source data size is larger than the destination buffer size this data will overflow the buffer towards higher memory address and probably overwrite previous data on stack.

2. Heap-based buffer overflows

- A heap overflow is a form of buffer overflow; it happens when a chunk of memory is allocated to the heap and data is written to this memory without any bound checking being done on the data.
- This is can lead to overwriting some critical data structures in the heap such as the heap headers, or any heap-based data such as dynamic object pointers, which in turn can lead to overwriting the virtual function table.
- Function longjump( ) in C allows the programmer to explicitly jump back to functions, not going through the chain of return addresses.
- Function setjmp() uses environment data to store the point where longjmp() should return. If we can overwrite it to point to the attack code, longjmp() jumps to that.

6.5 : MIM Attack

Q.19 What is a man-in-the-middle attack (MIM) ? Explain in detail.

☞ [SPPU : Dec.-22, End Sem, Marks 9]

OR Write short note on MITA attack.

☞ [SPPU : June-22, End Sem, Marks 3]

Ans. : • In cryptography, a **Man-In-The-Middle attack (MITM)** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.

- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.
- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack.
  4. Replay attacks.
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a Man-In-The-Middle attack can begin.

- Mallory can simply send Alice a public key for which she has the private, matching, key Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various defenses against MITM attacks use authentication techniques that are based on :
  1. Public keys
  2. Stronger mutual authentication
  3. Secret keys (high information entropy secrets)
  4. Passwords (low information entropy secrets)
  5. Other criteria, such as voice recognition or other biometrics
- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a certificate authority, whose public key is distributed through a secure channel.

6.6 : SQL Injection

Q.20 Explain the term phishing and SQL Injection with suitable example. ☞ [SPPU : Dec.-22, End Sem, Marks 8]

Ans. : • SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

- SQL injection attacks are also known as SQL insertion attacks. SQL Injection is one of the most common application layer attack techniques used today.
- SQL injection refers to a class of code-injection attacks in which data provided by the user is included in an SQL query in such a way that part of the user's input is treated as SQL code. An attacker can submit SQL commands directly to the database.
- SQL injection attacks can lead to privilege bypass and/or escalation, disclosure of confidential information and corruption of database information, among other effects.
- SQL Injection Example : An example SQL injection attack starts with code utilizing an SQL statement, such as :
  $db_statement = "SELECT COUNT(1) FROM `users` WHERE `username` = '$username' AND `password` ='$password'";
- In an SQL injection attack against code such as this, the attacker supplies input, such as the following, to the application:
  $username = "badUser";
  $password = "' OR '1'='1";
- Using this example, the SQL statement executed becomes the following :
  SELECT COUNT (1) FROM `users` WHERE `username`='badUser' AND `password`='' OR '1'='1';
- In the above example, this results in returning a count of all rows in the "users" table, regardless of the user name or password supplied, since the conditional '1'='1' always returns as true. If the query shown in this example is used for authentication purposes, the example SQL injection attack has just bypassed the authentication process for the application in question.
- This form of SQL injection occurs when user input is not filtered for escape characters and is then passed into an SQL statement. These results in the potential manipulation of the statements performed on the database by the end user of the application.
- In web application, the values received from a Web form, cookie, input parameter, etc., are not typically validated before passing them to SQL queries to a database server. Then dynamically built SQL statements.
- A attacker can control the input that is sent to an SQL query and manipulate that input. Attacker may be able to execute the code on the

back-end database. Fig. Q.20.1 shows three tier application with SQL commands.

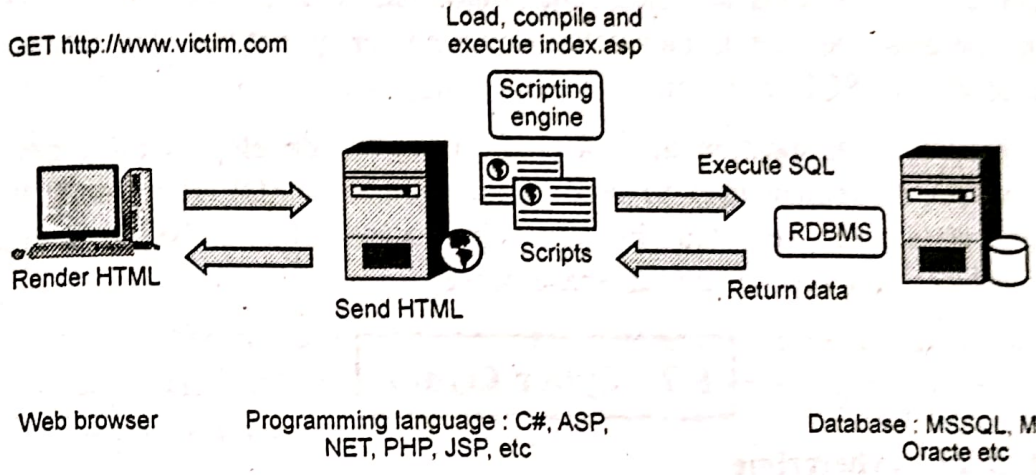


Fig. Q.20.1

- Using SQL injections, attackers can add new data to the database; modify data currently in the database and sometime gain access to other user's system capabilities by obtaining their password.

Prevention from SQL Injection Attack

1. Check syntax of input for validity.
2. Specify the length limits for input string.
3. Scan query string for undesirable word combinations that indicate SQL statements.
4. Limit database permissions.

Q.21 What is blind SQL injection ?

Ans. : • Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. Time delays are a type of blind SQL injection that cause the SQL engine to execute a long running query or a time delay statement depending on the logic injected.

- Blind SQL injection is used when there is no output and no error from the web application. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
- Blind SQL injection is identical to normal SQL injection except that when an attacker attempts to exploit an application rather than getting a useful error message they get a generic page specified by the developer instead.

- Web applications commonly use SQL queries with client-supplied input in the WHERE clause to retrieve data from a database. By adding additional conditions to the SQL statement and evaluating the web application's output, you can determine whether or not the application is vulnerable to SQL injection.
- To secure an application against SQL injection, developers must never allow client-supplied data to modify the syntax of SQL statements. All SQL statements required by the application should be in stored procedures and kept on the database server.

6.7 : Cyber Crime

Q.22 Define cybercrime.

Ans. : Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Internet connected activities are as vulnerable to crime.

Q.23 List the elements of cybercrime.

Ans. :

1. **Location/Place :** Where offender is in relation to crime.
2. **Victim :** Target of offense - government, corporation, organization, individual.
3. **Offender :** Who the offender is in terms of demographics, motivation, level of sophistication.
4. **Action :** What is necessary to eliminate threat.

Q.24 Explain the types of cyber-crimes.

☞ **[SPPU : June-22, End Sem, Marks 8]**

Ans. : There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking :** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.

4. **Identity theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of cyber crime :

a. Online banking fraud
b. Fake antivirus
c. `Stranded traveler' scams
d. `Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals
g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud.

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important cybercrimes known today.
- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest cybercrimes known till date.

Q.25 What is Botnet ? Where it is used ?

Ans. : • A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.

- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. Q.25.1 shows botnet.

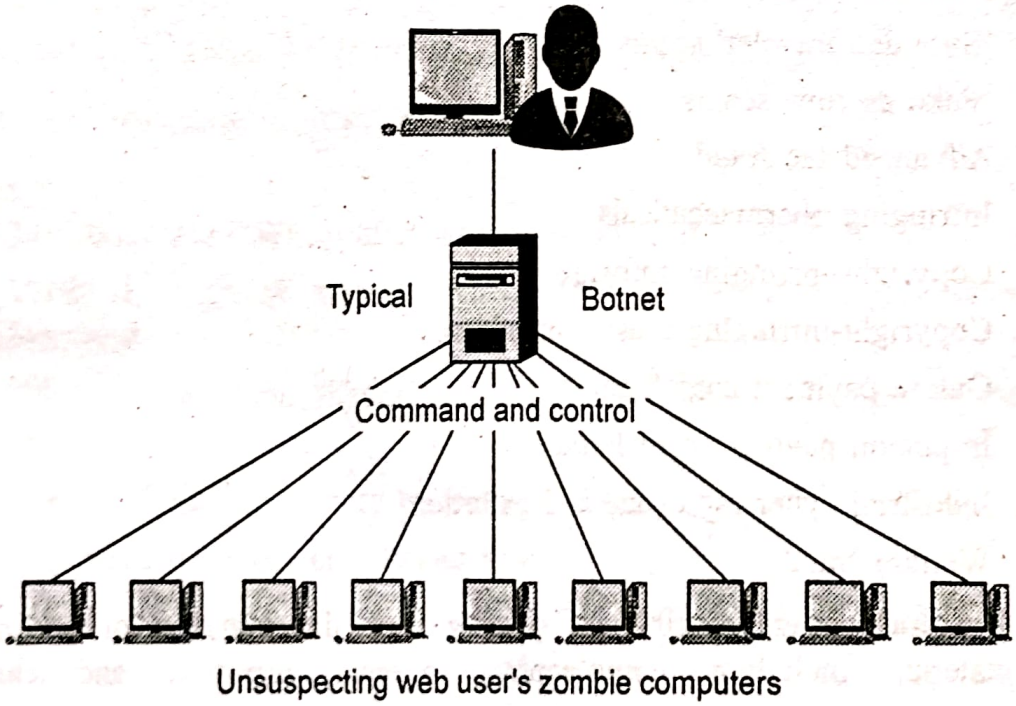


Fig. Q.25.1 Botnet

- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of

several users' computers, take control of each computer, and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage.

- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation.
- At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.
- Botnets can be used to:
  1. Send out spam emails
  2. Launch a Distributed Denial of Service Attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware
  5. Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

Q.26 Write short note on Zombie.

Ans. : • Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.

- Zombie network refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.
- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.

4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.

- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

Q.27 How and why do cyber criminals use botnets ?

Ans. : • The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.

- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create Denial-of-Service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.
- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.8 : Cyber Stalking

Q.28 Explain the term cyber stalking and cyber espionage with suitable example. ☞ **[SPPU : Dec.-22, End Sem, Marks 8]**

Ans. : Cyber stalking :

- Cyberstalking is stalking that takes place using electronic devices or the internet. It is the technological harassment directed towards a specific individual.
- There are several forms of cyberstalking that can take place including :
  1. Placing orders for delivery in someone else's name
  2. Gathering personal information on the victim
  3. Spreading false rumors

4. Encouraging others to join in the harassment
5. Threatening harm through email
6. Creating fear and paranoia for someone else
7. Hacking into online accounts

Cyber espionage :

- Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
- Cyber espionage does not have to be sophisticated, but it can involve complex tactics and long, patient breaches of a target's network. Common methods of cyber espionage include advanced persistent threats (APT), social engineering, malware attacks, and spear phishing. The cyber espionage threat landscape is constantly evolving as attacks become more sophisticated.
- Tips to prevent cyber espionage attacks :
  1. Patch software promptly, particularly internet-facing systems.
  2. Use multi-factor authentication that includes factors that cannot be brute-forced or phished, such as harware keys.
  3. Segment networks to make lateral movement by attackers more difficult.
  4. Monitor unexpected, suspicious behavior and take a proactive approach to detection. This includes threat hunting and threat intelligence found in cyber security solutions and services, such as MDR (managed detection and response) and SIEM (security information and event management).
  5. Review your organization's data policy and restrict who has access to sensitive data by practicing the principle of least privilege.

Q.29 Explain the term cyber stalking. How to identity and detect cyber stalking. ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : Following are the some of the methods for investigating the cyber stalking :

1. Take interview of victim person
2. Take interview of other persons
3. Check risk assessment

4. Find out any other additional digital evidence
5. Purpose of the crime or characteristics
6. Motivation
7. Repeat the steps until.

- **Take interview of victim person :** Victim has to submit the proof about cyber stalking. The investigator has to check proof before taking any action. Collect the initial information from victim and develop victimology.
- After gathering all information, investigation will move forward. The whole story needs to be heard from the perspective of the complainant's history with the suspect in order to properly.
- **Take interview of other persons :** If suppose other persons involved in this case, investigator will take interview of all that peoples. It will help to understand the case.
- **Check risk assessment :** Check the relationship between victim and an offender.
- **Find out any other additional digital evidence :** What is known about the victim and cyber stalker to perform a thorough search of the Internet ? Aim of this stage is to collect detail information about victim, cyber stalker and crime.
- **Purpose of the crime or characteristics :** Find out the depth of crime scenes. Find the location where the cyber stalker and victim meet. There is any physical location and over the internet they meet without knowing to each other.
- **Motivation :** Determine personal interest of cyber stalker.
- Repeat the steps until you reach to the cyber stalker.

Also Refer Q.28.

Q.30 What is Cyberstalking ?

Ans. : • Cyberstalking is stalking that takes place using electronic devices or the internet. It is the technological harassment directed towards a specific individual.

- There are several forms of cyberstalking that can take place including :
  1. Placing orders for delivery in someone else's name
  2. Gathering personal information on the victim

3. Spreading false rumors
4. Encouraging others to join in the harassment
5. Threatening harm through email
6. Creating fear and paranoia for someone else
7. Hacking into online accounts

Q.31 What is cyberbulling ? explain its types.

Ans. : • Bullying is defined as making fun of, putting down, or threatening (physically, verbally or both) another person. Often there is an imbalance of power. Bullying is done on purpose and is often repeated.

• Types of cyberbulling are as follows :

1. **Flaming' :** Online fights using electronic messages with angry and vulgar language
2. **"Harassment" :** Repeatedly sending offensive, rude, and insulting messages
3. **"Cyber stalking" :** Repeatedly sending messages that include threats of harm or are highly intimidating. Engaging in other on-line activities that make a person afraid for his or her own safety
4. **"Denigration" :** 'Dissing' someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships

Q.32 Explain types of cyber stalking.

Ans. : Three of the most common types of cyber stalking are : online abuse, trolling and sexting.

1. **Online abuse :** Actions that use information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm another person. Victims are often known personally by the perpetrator.
2. **Trolling :** Trolling is deliberately sowing hatred, bigotry, racism, misogyny, or just simple bickering between others. Trolls are users who thrive in any environment where they are allowed to make public comments, like blog sites, news sites, discussion forums, game chat and starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community.
3. **Sexting :** Sexting is the use of a mobile phone or other similar electronic device to distribute pictures or video of sexually explicit images. Often carried out by ex-partners who still have access to

sexually explicit images to humiliate and embarrass their victim. Cyber stalkers target their victims through social media platforms, chat rooms, message boards, discussion forums and e-mail.

6.9 : Cyber Terrorism

Q.33 What is cyber terrorism ? Write in detail example of cyber terrorism. ☞ [SPPU : Dec.-22, End Sem, Marks 8]

Ans. : Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

What is terrorism ?

- Most governments in the world cannot agree on one single definition for terrorism. The ambiguity in the definition brings indistinctness in action; as the old maxim goes "one man's terrorist is another man's freedom fighter".
- The US FBI defines terrorism as "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
- The US department of state defines terrorism as "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents".
- It is interesting to note that some definitions of terrorism also include targets to computer systems and its services.
- The traditional terrorism and cyber terrorism share the same attributes. One approach of understanding cyber terrorism is by breaking it down to its fundamental elements. The above definitions suggest that there are at least five elements which must be satisfied to construe **cyber terrorism :**

1. Politically motivated attacks that lead to death or bodily injury;
2. Cause fear and/or physical harm through attack techniques
3. Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations;

4. Attacks that disrupt non-essential services are not considered as terrorism; and.
5. Attacks that are not primarily focused on monetary gain.

- At the moment, there has been no known publicly reported incident of actual cyber terrorism. Most reported cases are related to cyber threats and the use of the Internet as a tool by terrorists.

Internet as an ideal tool for terrorists

- Several works on cyber terrorism and the Internet have been conducted by researchers including experiments on cyber terrorism activities on major websites and blogs such as YouTube and Second Life.
- The researchers also studied popular hosting service providers such as blogspot.com and wordpress.com. Their findings indicate that :
  1. There have been several cases reported in the media where the Internet has helped terrorists in their activities.
  2. The virtual world is indeed used to promote terrorism activities. Some of the videos published on the Net are related to explosives, attacks, bombing and hostage-taking.
  3. Some terrorist groups use the Internet for the purpose of inter-group communication and inter-networked grouping.
  4. The Internet is used to release manifestos and propaganda statements.
  5. Aside from generating propaganda, the Net is also used to coordinate missions or call meetings and to recruit new members.

Cyber Terrorism in India

- Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.
- Cyber terrorism is an attractive option for modern terrorists for several reasons,
  1. It is cheaper than traditional terrorist methods.
  2. Terrorism is more anonymous than traditional terrorist methods.
  3. The variety and number of targets are enormous.

4. Terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
5. Terrorism has the potential to affect directly a larger number of people.

6.10 : Cybercrime Against Property

Q.34 Explain cybercrime against property.

Ans. : • Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

- Property crime is a category of crime that includes, among other crimes, burglary, larceny, theft, motor vehicle theft, arson, shoplifting, and vandalism. Property crime involves the taking of property, and does not involve force or threat of force against a victim.
- Intellectual property crimes : Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- The property transaction scams come against a backdrop of instances of con artists pretending to be solicitors, using either fake names or stealing the identities of genuine firms.
- THEFT : A person commits an offense if he unlawfully appropriates property with intent to deprive the owner of property.
- Cybercrime is nothing but where the computer used as an object or subject of crime. Cybercrime is an evil having its origin in the growing dependence on computers in modern life.
- In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers. Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs.
- Whoever intentionally causes damage to any physical property of another without the person's consent is guilty of a Class A misdemeanor.

- Whoever intentionally causes damage to, intentionally marks, draws or writes with ink or another substance on or intentionally etches into any physical property of another , with-out the person' s consent and with knowledge of the character of the property , is guilty of a Class I felony if the property consists of one or more of the following :

1. Any synagogue or other building, structure or place primarily used for religious worship or another religious purpose.
2. Any cemetery, mortuary or other facility used for burial or memorializing the dead.

6.11 : Cybersquatting

Q.35 Write short note on cybersquatting.

Ans. : • Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.

- Internet Corporation for Assigned Names and Numbers (ICANN) coordinates assignment of domain names by various entities, which generally allocate domain names on a first-come, first-served basis for a modest fee.
- A cybersquatter takes advantage of the domain registration companies' 'first come, first served' policy by submitting a large list of very popular words and names all at once.
- While the domain registration company is in the process of entering these names, the cybersquatter uses profits from individual domain resales to finance the required registration fees.
- A cybersquatter can literally sit on a popular domain name for years, causing grief to the actual celebrity or company it represents.
- As the internet started becoming popular, internet users knew businesses would need a website. Some users started buying domains to create sites that looked like they were from reputable companies.

  Example : A cybersquatter could buy Heinz.com if the company hadn't created a website yet, looking to sell the domain to Heinz at a later date for profit, or use the domain name to attract traffic and generate money through advertising.

- If a business has a good reputation but no website, the company either pays the owner of the domain name to transfer the domain or contacts a trademark attorney to start a lawsuit.
- The second way is time - and cost - intensive, so trying to buy the domain directly from the cybersquatter is usually the preferred method.
- Today, opportunities for cybersquatters aren't as common since most businesses make the purchasing of their domain a high priority, especially if they have a strong trademark.

6.12 : Cyber Security Policy

Q.36 Elaborate different cyber security policies in detail and explain different challenges in internet governance.

☞ **[SPPU : June-22, End Sem, Marks 8]**

Ans. : • The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.

- While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished.
- The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000.
- The Act also enables e-governance applications for the electronic delivery of services to the public, business and government.
- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.
- Challenges in internet governance are as follows :

1. The growing significance of the internet makes the interfaces between technological and social impacts increasingly important. Because far more people are online, and far more is done online,

the digital environment is much more influential and the opportunities and risks are greater.

2. The commercialisation of the internet and the emergence of dominant companies with a high degree of market power mean that many decisions concerning the internet's development and impact are now made by them.
3. The proliferation of international policymaking spaces has made participation in governance more difficult, particularly for smaller countries and stakeholders with limited resources.

END...