	College	ttinad e of Engineering & Technology NCTE-New Dethi and Affiliated to Anna University-Chernal		
	Academi	c Year 2023 - 2024		
Question Bank				
Year/Semester:	Department	:ECE	Unit	: I/II/III/IV/V
II/ IV	Subject Code/Tit	le :EC3401 Network security	Section	: Part A/B/C
Date:27/05/2024	Faculty Name	:P.Nagarani sobana		

<u>UNIT I-</u> NETWORK MODELS AND DATALINK LAYER <u>PART A</u>

1.What are the three criteria necessary for an effective and efficient network?

The most important criteria arc performance, reliability and security. Performance of the network depends on number of users, type of transmission medium, the capabilities of the connected h/w and the efficiency of the s/w. Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. Security issues include protecting data from unauthorized access and viruses

2. Group the OSI layers and its function.

The seven layers of the OSI model belonging to three subgroups. Network support layers: Consisting of Physical, data link and network layers and they deal with the physical aspects of moving data from one device to another. User support layers: Consists of Session. Presentation and application layers and they allow interoperability among unrelated software systems. The transport layer ensures end-to-end reliable data transmission

3. What are the features provided by layering?

It decomposes the problem of building a network into manageable components. Rather than implementing a monolithic piece of software each of this solves one part of the problem.

It provides more modular design. To add some new service, it is enough to modify the functionality at one layer, reusing the functions provided at all the other layers.

4. What are the two interfaces provided by protocols?

1.Service interface-defines the operations that local objects can perform on the protocol.

2. Peer interface-defines the term and meaning of messages exchanged between protocol

peers to implement the communication service.

5.What is LAN?

A LAN is a common name used IO describe a group of devices that share a geographic location. It is limited to single building or campus

6.What is flow Control?

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

7. What is the use of two dimensional parity in error detection?

Two-dimensional parity check increases the likelihood of detecting burst errors. It is used to detect errors occurred in more than one bits.

8.What are the issues in data link layer?

The data link layer has a number of specific functions it can carry out. These functions include, providing a well-defined service interface to the network layer.

Dealing with transmission errors and regulating the flow of data so that slow receivers are not swamped by

fast sent

9. What are the ways to address the framing problem'?

The tracing problem can be addressed by the following protocols:

- Byte-Oriented Protocols(PPP)
- Bit-Oriented Protocols(HDLC)
- Clock-Based Framing(SON

10.What are the responsibilities of' data link layer'?

Specific responsibilities of data link layer include the following.Framing, physical addressing, flow control, error control, access control

11.Mention the types of errors.

There are 2 types of errors. They are single-bit error and burst-bit error.

12.Define the following terms.

Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1. Burst error: Means that 2 or more bits in the data unit have changed from 1 to 0 front 0 t

13.What is redundancy?

It is the error detecting mechanism, which means a shower group of bits or extra bits may be appended at the destination of each unit.

14. What is the purpose of harming code?

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction.

15.What is mean by error control?

Error control is a method that can be used to recover the corrupted data whenever possible. These are two basic types of error control which are backward error control and forward error control.

16.What is OSI?

A standard that specifies a conceptual model called Open systems Interconnection network interface model, which breaks networked communications into seven layers: Application, Presentation, Session, Transport, Network, Data link, Physical.

17.State the major functions performed by the presentation layer of the ISO OSI model.

Presentation layer is concerned with the format of data exchanged between peers, for example, whether an integer is 16, 32, or 64 bits long and whether the most significant bit is transmitted first or last, or how a video stream is formatted

18.State the purpose of layering in networks?

A layer is a collection of related functions that provides services to the layer above it and receives services from the layer below it.

To execute the functions by each layer is independent.

19.What are the two fundamental ways by which network performance is measured?

- 1. Bandwidth
- 2. Latency

20.Define Data Communication.

It is the exchange of data between two devices by transmission medium.

	<u>PART B & C</u>	
1.	Describe in detail about the Data Communication.	(13)
2.	Write short notes on	
	(i) Network Criteria	(3)
	(ii) Physical Structures	(4)
3.	Define the following network topologies with an advantage.	
	(i) Bus topology	(3)
	(ii) Ring topology	(3)
4.	State the following networks in detail.	
	(i) LAN	(3)
	(ii) MAN	(3)
5.	Discuss about the Internet standards and Administration. Summarize the following:	(13)
6.	(i) Principles of Protocol layering.	(7)
7.	Express the various layers and functions of OSI model.	(13)
8.	Examine the Transmission impairment and Data rate limits.	(13)
	(i) Analyze the Services provided by data-link layer.	(7)
9. 10.	(ii) Classify the types of address in link layer Explain the Address Resolution Protocol with an example.	(6) (13)
11.	Generalize the various network topologies and its applications.	(15)
12. 13.	Develop the OSI model and explain its layers with neat sketch. Summarize the following	(15)
10.	(i) Data link laver	(8)
		(0)
	(ii) Link Layer Addressing	(7)

<u>UNIT – II- NETWORK LAYER PROTOCOLS</u> <u>PART A</u>

1. What are the responsibilities of Network Layer?

The Network Layer is responsible for the source-to-destination delivery of packet possibly across multiple networks (links).Logical addressing and routing.

2.What is DHCP?

The Dynamic Host Configuration Protocol has been derived to provide dynamic configuration. DHCP is

also needed when a host moves from network to network or is connected and disconnected from a network.

3.Define ICMP

Internet Control Message Protocol is a collection of error messages that are sent back to the source host

whenever a router or host is unable to process an IP datagram successfully.

4.What is the need of internetwork?

To exchange data between networks, they need to be connected to make internetwork.

5.What do you mean by ARP?

ARP stands for Address resolution protocol. ARP is a dynamic mapping method that finds a physical

address for a given a logical address. i.e. mapping IP address to physical address.

6.What do you mean by RARP?

RARP stands for Reverse Address resolution protocol, maps a MAC address to an IP address.

7.What are the functions of MAC?

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and

error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

8. Define the term medium access control mechanism

The protocol that determines who can transmit on a broadcast channel are called medium access control

(MAC) protocol. The MAC protocols are implemented in the Mac sub-layer which is the lower sub-layer of the data link layer.

9.What is bridge?

Bridge is a hardware networking device used to connect two LANs. A bridge operates at data link layer

of the OSI reference model.

10.What is a repeater?

Repeater is a hardware device used to strengthen signals being transmitted on a network.

11.Define router

A network layer device that connects networks with different physical media and translates between

different network architecture.

12.What is a switch?

A switch is a networking device that manages networked connections between devices on a star networks.

13.What is mean by Ethernet?

Ethernet is a networking technology developed in 1970 which is governed by the IEEE 802.3 specifications.

14.What are the advantages of Ethernet?

1.Inexpensive

2.Easy to install

3.Supports various writing technologies.

15.Identify the class and default subnet mask of the IP address 217.65.10.7.

IP Address 217.65.10.7 belongs to Class C. Its subnet mask is 255.255.255.0.

16.What are the limitations of bridges?

1.Scale

2.Heterogeneity

17.Define Bluetooth.

Bluetooth is a wireless technology standard for exchanging data over short distances (using shortwavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs).

18.What are the 3 levels of hierarchy in IP Addressing?

- 1. Netid
- 2. Subnetid
- 3. Hostid

19.What are the functions of bridge?

- 1. Connecting networks
- 2. Filtering information so that network traffic for one portion of the network does not congest the rest of the network.

20.Define sub- netting

Sub-netting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus control the flow of traffic for security or efficiency reasons.

PART B & C

1.	(i) What is meant by the Distance Vector Routing Algorithm	n? (7)	
2.	(ii) List the limitations of Distance Vector Routing Algorith Define Unicast routing and its Internet structure with neat diag	nm. (6) gram. (13)	
3.	(i) Write note on the Border Gateway Protocol with neat dia	igram. (8)	
4.	(ii) Draw the RGP 4 undate packet format Define multicasting and explain in detail about multicast add	dress. (13)	
5.	Summarize the different Datagram approaches. Also show th DVR. List the limitations of Link State Routing Algorithm.	the advantages of LSR ov (13)	er
6.	Summarize the DVMRP and its algorithm.	(13)	
7.	Explain the Protocol Independent Multicast (PIM) and its varie	ous	
8.	Describe about RIP. Explain in detail about RIP and OSPF v	vith diagrams.	
	List the difference between them.	(13)	
9.	Discuss in detail about the IPv6 Protocol.	(13)	
10.	(i) Examine Distance Vector Multicast Routing protocol.	(8)	
	(ii) Simplify the metrics and their calculation method.	(5)	
11.	(i) Explain the internet multicasting. Explain in detail.	(7)	
12.	(ii) Find the IBy6 header details and evaluin them Analyze the following in IPv6 Addressing.	(6)	
	(i) Autoconfiguration	(6)	

- 13. Interpret the RIP algorithm with a simple example of your choice (13)
- 14. Elaborate in detail about the transition from IPv4 to IPv6. (13)

UNIT- III- TRANSPORT AND APPLICATION LAYERS

1. What are the fields on which the UDP checksum is calculated? Why?

UDP checksum includes a pseudo header, the UDP header and the data coming from the application layer.

2. What are the advantages of using UDP over TCP?

- UDP does not include the overhead needed to detect reliability
- It does not need to maintain the unexpected deception of data flow
- UDP requires less processing at the transmitting and receiving of hosts.
- It is simple to use for a network
- The OS does not need to maintain UDP connection information.

3.What is TCP?

TCP provides a connection oriented, reliable byte stream service. The connection oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

4.Define congestion

When too many packets rushing to a node or a part of network, the network performance degrades. This situation is called as congestion.

5.List the flag used in TCP header.

TCP header contains six flags. They are URG, ACK, PSH, RST, SYN, FIN

6. Give the approaches to improve the QoS.

Fine grained approaches, which provide QoS to individual applications or flows. Integrated services, QoS architecture developed in the IETE and often associated with RSVP.

7.What do you mean by QoS?

Quality of Service is used in some organizations to help provide an optimal end user experience for audio

and video communications. QoS is most commonly used on networks where bandwidth is limited with a large number of network packets competing for a relatively small amount of available and width.

8.What is multiplexing?

The job of gathering data chunks at the sources host from different sockets, encapsulating each data

chunks with header information to create segments, and passing the segments to the network layer is called multiplexing.

9.What is de-multiplexing?

The job of delivering the data in a transport layer segment to the correct socket is called demultiplexing.

10.What is RTT?

RTT is an acronym for Round Trip Time: it is a measure of the time it takes for a packet to travel

from

a computer, across a network to another computer, and back.

11.What is the segment?

Transport layer protocols send data as a sequence of packets. In TCP/IP these packets are called segments.

12.What is a port?

Applications running on different hosts communicate with TCP with the help of a concept called as

ports. A port is a 16 bit unique number allocated to a particular application.

13.List the services of end to end services.

- Guarantee message delivery.
- Delivery messages in the same order they are sent.
- •Deliver at most one copy of each message.
- Support arbitrarily large message.
- Support synchronization.

14.What is congestion?

When load on network is greater than its capacity, there is congestion of data Packets. Congestion

occurs

because routers and switches have queues or buffers.

15.What are the functions of transport layer?

- Breaks messages into packets.
- Connection control.
- Addressing.
- Provide reliability.

16.What are the types of QoS tools?

- Congestion avoidance
- Shaping/policing
- Link efficiency

17.List some ways to deal with congestion

- packet elimination
- Flow control
- Buffer allocation
- Choke packets

18.Define network congestion?

When two or more nodes would simultaneously try to transmit packets to one node there is a high probability that the number of packets would exceed the packet handling capacity of the network and lead to congestion.

19.List the three types of addresses in TCP/IP.

Three types of addresses are used by systems using the TCP/IP protocol: the physical address, the

internetwork address (IP address), and the port address.

20.What is the flow characteristics related to QoS?

The flow characteristics related to QoS are

•Reliability

•Delay

•Jitter, Bandwidth

PART B & C

1.	Write short notes on:	
	(i) Process-to-process communication	(4)
2.	(ii) Addressing Summarize the following:	(5)
	(i) Stop-and-Wait Protocol	(7)
3.	Show the services provided by transport layer protocol.	(13)
4.	Describe the working principle of TCP congestion control.	(13)
5.	Explain the services offered by TCP to the process at the applicatio	n layer. (13)
6.	Analyze the TCP connection with its Three-Way Handshaking.	(13)
_	Examine the State Transition Diagram for TCP.	(13)
⁷ 8.	Manipulate the flow control mechanism for TCP (i) With neat sketches, evaluate the retransmission techniques in	(13) detail. (6)
9. 10.	(ii) Criticize the events and transitions about the TCP state transi Elaborate on TCP connection Management using neat diagrams.	tion diagrams. (7) (13)
11.	Write in detail the principle of establishment of QoS through D	fferentiated services. (13)
12.	Examine the concept of congestion avoidance in TCP.	(13)

UNIT-IV NETWORK SECURITY PART-A

1. Differentiate passive attack from active attack with example.

A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

2. What are the two problems with one-time pad?

It makes the problem of making large quantities of random keys. It also makes the problem of key distribution and protection.

3. Define threat and attack.

Threat: A Potential violation of security which exists when there is circumstance, capacity, action or event that could breach security and cause harm .i.e. A threat is a possible danger that might exploit a vulnerability.

Attack: An assault on system security that derives from an intelligent threat: i.e. an intelligent

act or deliberate attempt to evade security services and violate the security policy of the system.

4. What is cryptanalysis and cryptography?

Cryptanalysis is the study of taking encrypted data, and trying to unencrypted it without use of the key. The other side of cryptography, cryptanalysis is used to break codes by finding weaknesses within it. In addition to being used by hackers with bad intentions, cryptanalysis is also often used by the military. Cryptanalysis is also appropriately used by designers of encryption systems to find, and subsequently correct, any weaknesses that may exist in the system under design. Cryptography the primary goal of cryptography is to conceal data to protect it against unauthorized third-party access by applying encryption. The more theoretical or mathematical effort is required for an unauthorized third party to recover data, the stronger is the encryption.

5. What are the key principles of security?

- Confidentiality
- Integrity
- Availability

6. How does simple columnar transposition work?

Write the message in a rectangle row by row and read message off column by column but permute the order of the columns. The order of the column becomes the key to the algorithm.

7. What are the essential ingredients of a symmetric cipher?

A symmetric cipher encryption has five ingredients. They are:

- Plaintext
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

8. What are the two basic functions used in encryption algorithms?

The two basic functions used in encryption algorithms are

Substitution

Π

Transposition

9. How many keys are required for two people to communicate via a cipher?

If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.

10. What is the difference between a block cipher and a stream cipher?

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

11. What are the two approaches to attacking a cipher?

The two approaches to attack a cipher are:

- Cryptanalysis
- Brute-force attack

12. What is the difference between an unconditionally secure cipher and a Computationally secure cipher?

An unconditionally secure cipher is a scheme such that if the cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plain text, no matter how much cipher text is available.

A computationally secure scheme is such that the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

13. Briefly define the Caesar cipher.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example:

Plain: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

14. Briefly define the monoalphabetic cipher?

A monoalphabetic cipher maps from a plain alphabet to cipher alphabet. Here a single cipher alphabet is used per message.

15. Briefly define the playfair cipher.

The best-known multiple-letter encryption cipher is the playfair, which treats diagrams in the plain text as single units and translates these units into cipher text diagrams.

16. What is a transposition cipher?

Transposition cipher is a cipher, which is achieved by performing some sort of permutation on the plaintext letters.

17. What is Steganography?

Hiding the message into some cover media. It conceals the existence of a message. The process of hiding a message in image.

18. Why is it not practical to use an arbitrary reversible substitution cipher?

An arbitrary reversible cipher for a large block size is not practical, however, from an implementation and performance point of view. Here the mapping itself is the key.

19. What is the difference between diffusion and confusion?

In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation.

In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution.

20. What is the difference between a mono alphabetic cipher and a poly alphabetic cipher?

(NOV/DEC 2012)

- Mono alphabetic cipher: Here a single cipher alphabet is used.
- Poly alphabetic cipher: Here a set of related mono alphabetic substitution rules is used.

21. List the types of cryptanalytic attacks.

- Cipher text only
- **Known plaintext**
- Chosen plaintext
- Chosen cipher text
- Chosen text

22. Explain active and passive attack with example?

Passive attack:

Monitoring the message during transmission Eg: Interception

Active attack:

It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption

23. Define integrity and nonrepudiation?

Integrity:

Service that ensures that only authorized person able to modify the message.

Nonrepudiation:

This service helps to prove that the person who denies the transaction is true or false.

24. List ways in which secret keys can be distributed to two communicating parties.

• A can select a key and physically deliver it to B.

• A third party can select the key and physically deliver it o A and B

• If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key

• If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B

25. What is the difference between Rijndael and AES?

AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.

26. Why is the middle portion of 3DES a decryption rather than an encryption?

Decryption requires that the keys be applied in reverse order:

P=Dk1[Ek1[P]]

This results in a dramatic increase in cryptographic strength. The use of DES results in a mapping that is not equivalent to a single DES encryption.

PART B & C

1. Discuss the classical cryptosystems and its types.

Explain about the single round of DES algorithm. (10)

Describe key discarding process of DES. (6)

2. Explain RSA method in detail. (16)

3. Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain.

4. Explain the ceaser cipher and monoalphabetic cipher.

5. Explain in detail about the Public -key cryptosystems with neat diagrams

6. Discuss in detail about RSA algorithms

7.Write notes on Hash functions

8.Discuss about Secure Hash algorithm in detail

9.Explain about the Digital Signature algorithm in detail

10.List and discuss about the objectives of computer security

11.Discuss about OSI security arechitechture

12.Write note on Encryption process

13.Explain in detail about AES encryption and decryption in detail

14.Explain in security services and security mechnisms.

15.Write a note on AES key expansion.

UNIT V HARDWARE SECURITY

PART – A

1.Define Kerberos.

Kerberos is an authentication service developed as part of project Athena at MIT.The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

2.In the content of Kerberos, what is realm?

A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

The Kerberos server must have user ID and hashed password of all participating users in its database.

The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

3.Assume the client C wants to communicate server S using Kerberos procedure.

How can it be achieved? a) $C \rightarrow AS$: [IDC|| PC || IDV] b) $AS \rightarrow C$: Ticket c) $C \rightarrow V$: [IDC || ADC || IDV] Ticket = EKV [IDC || ADC || IDV]

4. Any three hash algorithm.

• MD5 (Message Digest version 5) algorithm.

• SHA_1 (Secure Hash Algorithm).

• RIPEMD_160 algorithm.

5. Specify the four categories of security threats

- Interruption
- Interception
- Modification
- Fabrication

6. Explain the reasons for using PGP?

a) It is available free worldwide in versions that run on a variety of platforms,

including DOS/windows, UNIX, Macintosh and many more.

b) It is based on algorithms that have survived extensive public review and are considered extremely secure.

E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128,

IDEA, 3DES for conventional encryption, SHA-1for hash coding.

c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.d) It was not developed by nor is it controlled by any governmental or standards organization. 3. Why E-mail compatibility function in PGP needed?

Electronic mail systems only permit the use of blocks consisting of ASCII text.

To accommodate this restriction PGP provides the service converting the row 8- bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

7. Name any cryptographic keys used in PGP?

a) One-time session conventional keys.

b) Public keys.

c) Private keys.

d) Pass phrase based conventional keys.

8. Define key Identifier?

PGP assigns a key ID to each public key that is very high probability unique

with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

9. List the limitations of SMTP?

a) SMTP cannot transmit executable files or binary objects.

b) It cannot transmit text data containing national language

characters. c) SMTP servers may reject mail message over certain size.

d) SMTP gateways cause problems while transmitting ASCII and EBCDIC.

e) SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

10. Define S/MIME? (MAY/JUNE 2012)

Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security.

11. What are the elements of MIME?

- Five new message header fields are defined which may be included in an
 RFC 822 header.
- A number of content formats are defined.
- Transfer encodings are defined that enable the conversion of any content
- format into a form that is protected from alteration by the mail system.

12. What are the headers fields define in MME?

- MIME version.
- Content type.
- Content transfer encoding.
- Content id.
- Content description.

13. What is MIME content type ?

It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are,

- 1. Text type
- 2. Multipart type
- 3. Message type
- 4. Image type
- 5. Video type.
- 6. Audio type.
- 7. Application type

14.What are the key algorithms used in S/MIME?

- Digital signature standards.
- Diffi Hellman.
- RSA algorithm.

15. Give the steps for preparing envelope data MIME?

- Generate Ks.
- Encrypt Ks using recipient's public key.
- RSA algorithm used for encryption.
- Prepare the 'recipient info block'.
- Encrypt the message using Ks.

16. What you mean by versioned certificate?

Mostly used issue X.509 certificate with the product name" versioned

digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

17. What are the function areas of IP security?

- Authentication
- Confidentiality
- Key management.

18. Give the application of IP security? • Provide secure communication across private & public LAN.

- Secure remote access over the Internet.
- Secure communication to other organization.

19. Give the benefits of IP security?

- Provide security when IP security implement in router or firewall.
- IP security is below the transport layer is transparent to the application.
- IP security transparent to end-user.
- IP security can provide security for individual user.

20. What are the protocols used to provide IP security?

- Authentication header (AH) protocol.
- Encapsulating Security Payload(ESP).

21. Specify the IP security services?

- Access control.
- Connectionless interpretty.
- Data origin authentication
- Rejection of replayed packet.
- Confidentiality.
- Limited traffic for Confidentiality.

22. What do you mean by Security Association? Specify the parameters that identifies the Security Association?

• An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on.

• A key concept that appears in both the authentication and confidentiality mechanism for ip is the security association (SA). A security Association is uniquely identified by 3 parameters:

- Security Parameter Index (SPI).
- IP Destination Address.
- Security Protocol Identifier.

23. What does you mean by Reply Attack?

• A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.

• Each time a packet is send the sequence number is incremented .

24. Explain man in the middle attack?

If A and B exchange message, means E intercept the message and receive the B's public key and b's userId, E sends its own message with its own public key and b's userID based on the private key and Y.B compute the secret key and A compute k2 based on private key of A and Y

25. Steps involved in SS L required protocol?

1. SSL record protocol takes application data as input and fragments it.

- 2. Apply lossless Compression algorithm.
- 3. Compute MAC for compressed data.

4. MAC and compression message is encrypted using conventional alg.

PART B & C

1.Discuss in detail about reverse engineering with neat sketches

2.Explain in detail about probing attack with neat sketches

3.Write note on design of security

4.Discuss in detail about the blockchain technology

5.Illustate the taxonomy of Trojan countermeasures

6.Discuss the classification of Trojan based on the payload

7.Write a note on hardware fpga design

8.Describe the major steps of the electronic hardware design and test flow, and discuss the security issues in each stage.

9.Explain the Side channel attacks.

10.Explain the physical channel attack

11.Describe in detail about the block chain technology

12.Describe the different types of security vulnerabilities.

13.Provide a brief description of generic Trojan structure.

14.Describe the classification of Trojans based on activation mechnaisims

15.Provide a brief discussion in Trojan structure.















Faculty Incharge

Head of the Department