COMPUTER NETWORK QUESTION BANK

UNIT I

PART A

1. Define – Data Communication (or) What is meant by data communication?

Data communication is defined as the exchange of data between two devices via some form of transmission medium in whatever form that is agreed upon by the parties creating and using the data.

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

The three criteria necessary for the effective and efficient networks are

a. Performance

b. Reliability

c. Security

3. What are the fundamental characteristics that determine the effectiveness of the data communication system?

The fundamental characteristics that determines the effectiveness of data communication system are

a. Delivery

b. Accuracy

c. Timeliness

d. Jitter

4. What are the advantages of distributed processing?

The advantages of the distributed processing are

a. Security

b. Encapsulation

c. Distributed databases

d. Faster problem solving

e. Security through redundancy

f. Collaborative processing

5. Define – Protocol (M/J – 12 R08)

A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating with each other.

6. For an 'n' device in a network, what is the number of cable links required for a mesh and ring topology?

The link required for the number of cables for a mesh and ring topologies are Mesh topology: n (n-1)/2 (Duplex), n (n-1) (Simplex)

Ring Topology: n

7. What are the five important component of the data communication? (or) Name the various components of data communication system. The five important components of the data communication are

a. Message

b. Sender

c. Receiver

d. Transmission Medium

e. Protocol

8. Name the four topologies used in the network.

The four topologies of a network are

a. Ring

b. Star

c. Mesh

d. Bus

9. Define – Computer network (or) Define – Network

A computer network is group of devices referred to as nodes connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

10. What are the criteria to evaluate the transmission medium? The

criteria used to evaluate transmission medium are

a. Throughput

b. Propagation Speed

c. Propagation Time

d. Wavelength

PARTB

1. Explain in detail, the OSI-ISO reference model of a computer with neat diagram. (16)

2. Explain the TCP/IP reference model with neat sketch. (16) (M-13)

3. Explain the different types of switching networks and list out its advantages and disadvantages. (16)

4. Explain the four basic network topologies and explain with its relevant features. (16) (N-10)

5. Distinguish between point-to-point links and multi-point links with relevant diagram. (16)

6. i) Compare connection oriented service with connection less service. (8)

ii) Compare the performance of TCP/IP (Internet model) with ISO/OSI reference model. (8) (M-11)(M-15)

7. i) Differentiate guided media from unguided media. (8)

ii) How is cable TV used for data transfer? Explain in detail. (8)

UNIT II

PART A

1. Define – Link

Link is a physical medium that transfers data from one device to another

2. List the types of Link. (N/D – 10 R08)(or) What are the two types of line configuration?

The types of link or line configuration are

a. Point to Point

i. Dedicated link between two devices

ii. Capacity reserved for two nodes

b. Multipoint (or) multidrop

i. More than two devices connected

ii. Link and Capacity shared either spatially or temporally

3. Define – Flow control (N/D – 11 R08)

Flow Control refers to a set of procedures which is used to restrict the flow of data that the sender can send before waiting for acknowledgment.

4. Define – Error control (N/D – 10 R08)

Error control in the data link layer refers primarily to methods of error detection and retransmission and is based on automatic repeat request, which is the retransmission of data.

5. What are headers and trailers and how do they get removed?

Each layer in sending machine adds its own information to the message it receives from the layer just above it and passes the whole packages to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6, 5, 4, 3, 2. Trailers are added in the layer 2. At the receiving machine, the headers or trailers attached to the data unit corresponding to the sending layers are removed and appropriate actions are taken at the receiving layers.

6. The transport layer creates a communication between the source and destination. What are the three events involved in the connection?

The three events involved in connection between the source and destination are

a. Connection Establishment

b. Data Transfer

c. Connection Release

7. What are the modes for propagating light along optical channels?

There are two modes for propagating light along optical channels, multimode and single mode.

Multimode: Multiple beams from a light source move through the core in different paths. Single mode: Fiber with extremely small diameter that limits beams to a few angles, resulting in an almost horizontal beam.

8. What is the main function of physical layer? (M/J – 11 R08)

The main functions of physical layer are

a. Physical characteristics of interfaces and media

b. Representation of bits

c. Data rate

d. Synchronization of bits

e. Line configuration

f. Physical topology

g. Transmission mode

9. What is meant by circuit switching? (N/D – 10 R08)

A circuit switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. Circuit switching takes place at the physical layer. In circuit switching, the resources need to be reserved during the setup phase.
The resources remain dedicated for the entire duration of data transfer phase until the teardown phase.

10. What is the role of DSL modem? (M/J – 12 R08)

The role of Digital Subscriber Line (DSL) modem, is to provide high speed access to the Internet over the existing local loops. DSL technology is a set of technologies, each differing in the first letter (ADSL,VDSL, HDSL, and SDSL).

PART B

1. Explain the functioning of Wireless LANs in detail.(16) (N-10)

2. List out the types of Ethernet. Explain in detail standard Ethernet and fast Ethernet in detail. (16)

(N-12)(N-11)

3. Explain the flow and error control mechanisms in data link control. (16) (N-11)

4. i) Explain the stop and wait protocol with a neat diagram. (8) (M-13)

ii) Write short notes on Bluetooth technology. (8) (N-11)

5. i) Compare the dore rakes of standard Ethernet, fast Ethernet, Gigabit Ethernet and Ten-Gigabit Ethernet. (6) (M-13)

ii) Explain piconet and scatter net with diagrams. (10)

(M-13)

6. Explain the architecture and layers of ATM. (16) (N-12)

7. Explain the architecture of a frame relay network with a neat sketch.(16) (M-13)

8. Explain the random access protocols in data link layer.(16) (N-15)

UNIT III

PART A

1. What are the responsibilities of the Data Link Layer?

The responsibilities of data link layer are

a. Framing

b. Physical Addressing

c. Flow Control

d. Error Control

e. Access Control

2. Write short notes on error correction.

Error correction is the mechanism used to correct the error and it can be handled in two ways

a. When an error is discovered, the receiver can have the sender to retransmit the entire data unit.

b. A receiver can use an error correcting code, which automatically corrects certain error.

3. Define – Flow control. (A/M – 11 R08)(N/D – 11 R08)

Flow Control refers to a set of procedures which is used to restrict the flow of data that the sender can send before waiting for acknowledgment.

4. Define Error control. (A/M – 11 R08)

Error control in the data link layer refers primarily to methods of error detection and retransmission and is based on automatic repeat request, which is the retransmission of data.

5. What is a buffer?

Buffer is a device which has a block of memory, reserved for storing incoming data until they are processed.

6. What are the categories of flow control?

The two categories of flow control are

a. Stop and Wait

b. Sliding Window

7. What is the function of stop and wait protocol?

The function of stop and wait protocol is to transmit frame and wait for the acknowledgement before sending the next frame.

8. What is selective reject ARQ?

In selective reject ARQ only specific damaged or lost frame is transmitted. If a frame is corrupted in transit, a NAK (Negative Acknowledgement) is returned and the frame is resent out of sequence.

9. Define Automatic Repeat Request (ARQ).

Error Control in the data link layer is based on the Automatic Repeat Request, which means retransmission of data in three cases.

a. Damaged Frame

b. Lost Frame

c. Lost Acknowledgement

10. What is the function of go-back N ARQ?

The function of go-back-N ARQ is to control the error in the continuous transmission.

PART B

1. Write short notes on the following: (N-12)(N-11)

(i) RARP (8)

(ii) Multicast routing, Multicast routing protocol (8)

2. a) Explain the different classes of IP addressing (12) (M-12)

b) What is the need for an IP address? (4) (M-12)

3. Explain in detail the IPV6 addressing schemes, notation, representation and address space

in detail. (16) (N-10)

4. Explain in detail the ICMP message format and error reporting in detail. (16) (M-13)

5. Define bridge. Explain the features and types of bridges. (16) (N-11)

6. Draw the IPV4 header format and explain the various components and its role in that format. (16)

(M-12)

7. Explain in detail any one routing algorithm. (8) (M-14)

8. Explain in detail the role of ARP .

UNIT IV

PART A

1. What are network support layers and user support layers?

Network Support Layers: The network support layers are Physical, Data Link and Network Layers.These layers deal with the electrical specifications, physical connection, transport timing and reliability.

User Support Layers: The user support layers are Session, Presentation and Application Layers. These allow interoperability among the unrelated software systems.

2. State the goals of Network layer (Or) What are the responsibilities of the network lay (N/D – 10 R08 MCA)

The Network Layer is responsible for the source to destination delivery of packet across multiple network links. The specific responsibilities of network layer includes

a. Logical Addressing

b. Routing

3. Define – ICMP (N/D – 12 R08)

ICMP is a mechanism used by host and gateways to send query and error messages to the source of the datagram.

4. Find the class of each address. (A/M – 11 R08)

00000001 00001011 00001011 11101111

14.23.120.8

00000001 00001011 00001011 11101111 – Class A

14.23.120.8 – Class A

5. What is internetworking? (N/D – 11 R08 EEE)

Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.

6. What is a virtual circuit?

A virtual circuit is defined as a circuit that is made between the sender and the receiver after handshaking. All the packets of the sender and the receiver pair travel in the same path and it is dedicated for the entire session.

7. What is datagram approach?

In datagram approach, each packet is treated independently from all others. Even when a packet represents part of a multipacket transmission, the network treats it as if it exists alone. The individual packets travel different path. Packets in this technology are referred as datagram.

8. What are the two types of implementation formats in virtual circuits?

The two types of implementation formats in virtual circuits are

a. Switched Virtual Circuit

b. Permanent Virtual Circuit

9. What is a router? (Or) What is the function or role of a router? (M/J – 12 R08)

A router is a three layer device that routes packets based on their logical addresses i.e. host to host addressing. A router normally connects LANs and WANs in the internet and has a routing table that is used for making decisions about the route.

The function of a router is to

a. Find a path between nodes in a network

b. Route the packets across the path to their final destination

c. router that connects to the internet uses one private address and one global address.

10. Why is IPV6 preferred than IPV4? (M/J – 12 R08)(M/J – 13 R08)

IPV6 is preferred than IPV4 due to some deficiencies in IPV4 which becomes unsuitable for fast growing internet

The deficiencies in IPv4 are

a. Address depletion is a long term problem in the internet.

b. Lack of accommodation for real-time audio and video transmission.

c. Lack of encryption and authentication of data for some application

PART B

1. Explain the segment formats for TCP and UDP. (16) (N-12)

2. How is connection established and released in TCP? Explain with neat sketch. (8) (M-

13) (M-12)

3. Explain the congestion control mechanism and transmission control protocol with neat sketches. (16)

(N-11) (N-12) (M-12)

4. Explain in detail, the TCP congestion avoidance algorithm. (8) (N-11) (N-11)

5. Explain the default timer mechanism followed in TCP. (8) (M-13)

6. Explain the leaky bucket and token bucket algorithm with flow charts. (8) (N-11)

7. Explain in detail the techniques to improve QOS. (8) (N-11)

8. Explain in detail the user datagram protocol (UDP) in detail. (8)

UNIT V

PART A

1. What is the purpose of Domain Name System? (Or)State the role of DNS. (M/J – 12 R08)

Domain Name System maps a name to an address (IP address) and conversely an address to name.

2. What is cryptanalysis? (M/J – 12 R08)

Cryptanalysis refers to the science and art of breaking ciphers to gain as much information as possible about the original messages.

3. Define – Cryptography (N/D – 11 R08 EEE)

Cryptography refers to the science and art of transforming messages to make them secure and immune to attack.

4. What is PGP? (N/D – 11 R08 EEE)(N/D – 10 R08)

Pretty Good Privacy (PGP) protocol provides security at the application layer. PGP is designed to create authenticated and confidential e-mails.

5. What is HTTP? (N/D – 11 R08 EEE)

Hyper Text Transfer Protocol (HTTP) is a protocol which is used to access data on the World Wide Web (WWW). It functions as a combination of File transfer protocol (FTP) and Simple mail transfer protocol (SMTP).

6. List the multimedia applications. (N/D – 11 R08 EEE)

The multimedia applications are

a. Streaming stored audio/video

b. Streaming live audio/video

c. Real time interactive audio/video

7. What is TELNET? (N/D – 11 R08)

Terminal NETwork (TELNET) is the standard TCP/IP protocol for virtual terminal service as proposed by ISO. TELNET is a general-purpose client/server application program It enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

8. What are the functionalities of TELNET? (N/D – 11 MCA) (Or)Name the function of TELNET.

(N/D – 10 MCA)

TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

9. State the purpose of SNMP. (N/D – 11 R08)

Simple Network Management Protocol (SNMP) is a framework used for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.

10. Why is POP3 or IMAP4 needed for E-mail? (A/M – 11 R08)

POP3 or IMAP4 is a client-server protocol. POP3 or IMAP4 for E-mail is needed by the client to pull messages i.e. retrieve messages from the server. The direction of the bulk data is from the server to the client. The POP3 or IMAP4 are message access agent protocols.

PART B

1. Explain in detail, DNS and its frame format. (8)

(N-11) (N-10) (M-12) (N-12)

2. What is the role of the local name server and the authoritative name server in DNS? What is the

resource record maintained in each of them? (16) (N-10)

3. Explain the SMTP. List out its uses, state strengths and weakness. (8) (N-

10) (N-11)

4. Explain in detail, the HTTP and FTP with neat sketches. (16) (N-

11) (N-12) (N-12)

5. Explain e-mail in detail.(8) (M-12)

6. Explain SNMP in detail.(8) (M-12)

7. Draw the architecture of WWW and explain in detail the various blocks. (16)

UNIT 1 – 2 MARKS

1. Define cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

2. Define cryptanalysis.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code."

3. Define security Attack, mechanism and service

• **Security attack:** Any action that compromises the security of information owned by an organization.
• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

4. Distinguish Threat and Attack

Threat -A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
Attack -An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5. Differentiate active attacks and passive attacks.

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are the release of message contents and traffic analysis.
An active attack attempts to alter system resources or affect their operation. It can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

6. Specify the components of encryption algorithm

- Plaintext
- Encryption algorithm

- Secret key
- Cipher text
- Decryption algorithm

7. Describe security mechanism.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

8. Differentiate block and 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.

9. **What are the essential ingredients of a symmetric cipher?**

• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
• **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.
• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

10. Specify four categories of security threats

- Interruption
- Interception
- Modification
- Fabrication

PART B

1. Tabulate the substitution Techniques in detail. (12)
Definition , example and disadvantages

- Caesar cipher
- monoalphabetic cipher
- playfair cipher
- hill cipher
- polyalphabetic ciphers –vigenere and vernam cipher
- one time pad

2. Describe the Transposition Techniques in detail. (4)

Rail fence

3. (i) List the different types of attacks and explain in detail.(8)

1. A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are

 The release of message contents and

 traffic analysis.

2. **An active attack** attempts to alter system resources or affect their operation. It can be subdivided into four categories:

 masquerade,

 replay,

 modification of messages, and

 denial of service.

4. Describe in detail about the types of cryptanalytic attack. (8)

 Cipher text only

 Known plain text

 Chosen plaintext

 Chosen cipher text

5. (i) Evalute3^21 mod 11 using Fermat's theorem. (6)
(ii) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT. (10)
X=2(mod 3)
X=3(mod 5)
X=2(mod 7)
6 Discuss about the Groups, Rings and Field (8)
7. Solve using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used. (8)

UNIT II PART A

1. 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.

2. What is the difference between diffusion and confusion?

In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext
digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits.
confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm

3. What are the design parameters of a Feistel cipher?

• Block size
• Key size
• Number of rounds
• Subkey generation algorithm
• Round function F
• Fast software encryption/ Decryption

• Ease of analysis

4. Explain the avalanche effect.

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

5. What is the strength of DES?

• The use of 56 bit keys
• The nature of DES algorithm
• Timing attacks

6. Define product cipher

product cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

7. What is substitution and permutation?

Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

8. Give 5 modes of operation in block cipher

• Electronic Codebook(ECB)
• Cipher Block Chaining(CBC)

9. State advantages of counter mode.

*Hardware Efficiency
* Software Efficiency
*Preprocessing
* Random Access
* Provable Security
* Simplicity.

10. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES. In the first instance, plaintext is converted to ciphertext using the encryption algorithm. This ciphertext is then used as input and the algorithm is applied again. This process may be repeated through any number of stages.

PART B

1. Explain in detail about working of DES encryption and decryption

• Definition
• Encryption- Diagram
• Initial Permutation
• Details of Single Round- diagram , S-box
• decryption

2. Explain in detail about working of AES

Definition
Structure – diagram and its explanation (10 pt)
Transformation function

3. Explain in detail about AES key expansion

4. Explain briefly about the block cipher modes of operations ▪ Electronic Codebook(ECB)

▪ Cipher Block Chaining(CBC)

▪ Cipher Feedback(CFB)

▪ Output Feedback(OFB)

▪ Counter(CTR)

4. Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:

a. $p = 3$; $q = 11$, $e = 7$;$M = 5$
b. $p = 5$; $q = 11$, $e = 3$;$M = 9$
c. $p = 7$; $q = 11$, $e = 17$;$M = 8$
d. $p = 11$; $q = 13$, $e = 11$;$M = 7$
e. $p = 17$; $q = 31$, $e = 7$;$M = 2$
5. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$.What is the plaintext M?
6. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.
a. If user A has private key Xa = 5, what is A's public key Ya ?
b. If user B has private key Xb=12, what is B's public key Yb ?
c. What is the shared secret key?
7. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2
a. Show that 2 is a primitive root of 11.
b. If user A has public key Ya = 9, what is A's private key Xa?
c. If user B has public key $Yb = 3$, what is the secret key K shared with A?

UNIT III PART A

1. What is a hash in cryptography?

A **hash function** H accepts a variable-length block of data M as input and produces a fixed-size hash value h= H(M) called as message digest as output. It is the variation on the message authentication code

2. What is the role of a compression function in a hash function?

The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final values of the chaining variable is the hash value usually b>n; hence the term compression

3. What is cryptography hash function?

The kind of hash function needed for security applications is referred to as a cryptographic hash function. A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed

4. What are the applications of cryptographic hash function?

 Message Authentication
 Digital Signatures
 pseudorandom function (PRF) or a pseudorandom number generator (PRNG).

5. What do you meant by MAC?

It involves the use of a secret key to generate a small fixed-size block of data, known as a **cryptographic checksum** or MAC, that is appended to the message. This technique assumes

that two communicating parties, say A and B, share a common secret key .When A has a message to send to B, it calculates the MAC as a function of the message and the key: **MAC = MAC(*K, M*)**

where

M = input message

C = MAC function

K = shared secret key

MAC = message authentication code

6. Differentiate MAC and Hash function?

MAC: In MAC , the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret

7. List any three hash algorithm.

- MD5(message Digest version 5) algorithm
- SHA_1 (Secure Hash algorithm)
- RIPEMD_160 algorithm

8. What is the difference between weak and strong collisions resistance?

Weak collisions resistance: for any given block x, it is computationally infeasible to find y * x with

H(y) = H(x). it is proportional to 2n .

Strong collision resistance: it is computationally infeasible to find any pair (x,y) such that H(x)= H(y). it is proportional to 2n/2

9. Differentiate internal and external error control.

Internal error control:

In internal error control, an error detecting code also known as frame check sequence or checksum.

External error control:

In external error control, error detecting codes are appended after encryption

10. What is the meet in the middle attack?

This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function

PART B

Describe Secure hash Algorithm in detail. (16)

1. Describe the MD5 message digest algorithm with necessary block diagrams. (16)

2. (i)Summarize CMAC algorithm and its usage.(8)
(ii)Describe any one method of efficient implementation of HMAC. (8)

3. Describe digital signature algorithm and show how signing and verification is done using DSS. (16)

4. Explain in detail ElGamal Digital Signature scheme with an example. (16)

5. Explain in detail about different ways of distribution of public keys

6. Consider prime field q=19, it has primitive roots { 2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose XA=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme

UNIT 4- 2
MARKS

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. **What is Kerberos? What are the uses?**
   Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provide a centralized authentication server whose functions is to authenticate servers.
3. **What 4 requirements were defined by Kerberos?**
   - Secure
   - Reliable
   - Transparent
   - Scalable
4. **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 participatingusers in its database.
   - The Kerberos server must share a secret key with each server. Such an environmentis referred to as "Realm".
5. **What is the purpose of X.509 standard?**
   X.509 defines framework for authentication services by the X.500 directory to its users.X.509 defines authentication protocols based on public key certificates.

6. **List the 3 classes of intruder?**
   Classes of Intruders
   - Masquerader
   - Misfeasor
   - Clandestine user
7. **Define virus. Specify the types of viruses?**
   A virus is a program that can infect other program by modifying them the modificationincludes a copy of the virus program, which can then go on to infect other program. Types:
   - Parasitic virus
   - Memory-resident virus
   - Boot sector virus
   - Stealth virus
   - Polymorphic virus
   - Metamorphic virus
8. **What is application level gateway?**
   An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, andthe gateway asks the user for the name of the remote host to be accessed.
9. **List the design goals of firewalls?**
   - All traffic from inside to outside, and vice versa, must pass through thefirewall.
   - Only authorized traffic, as defined by the local security policy, will be allowed to pass

     The firewall itself is immune to penetration.

10. What are the steps involved in SET Transaction?

- The customer opens an account
- The customer receives a certificate
- Merchants have their own certificate
- The customer places an order.
- The merchant is verified.
- The order and payment are sent.
- The merchant requests payment authorization.
- The merchant confirm the order.
- The merchant provides the goods or services.
- The merchant requests payment.

PART-B

11. What is Kerberos? Explain how it provides authenticated service.
12. Explain the format of the X.509 certificate.
13. Explain the technical details of firewall and describe any three types of firewall with neatdiagram.
14. Write short notes on Intrusion Detection.
15. Define virus. Explain in detail.
16. Explain Secure Electronic Transaction with neat diagram.
17. What is a trusted system? **Explain** the basic concept of data access control in trustedsystems. (8)

UNIT V

PART A

1.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.

2.List the limitations of SMTP/RFC 822?

1. SMTP cannot transmit executable files or binary objects.
2. It cannot transmit text data containing national language characters.
3. SMTP servers may reject mail message over certain size.
4. SMTP gateways cause problems while transmitting ASCII and EBCDIC.
5. SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

3.What are the different between SSL version 3 and TLS?

SSL	**TLS**
In SSL , the minor version is zero and major version is 3	In TLS, the major version is 3 and the minor version is 1
SSL use HMAC algorithm, except that the padding bytes concatenation	Make use of the same algorithm
SSL supports 12 various alert codes	It supports all of the alert codes defined in SSL3 with the exception of no-certificate.

4.What are the services provided by PGP services.

• Digital signature
• Message encryption
• Compression
• E-mail compatibility
• Segmentation

5. Explain the reasons for using PGP?

- It is available free worldwide versions that run on a variety of platforms, including DOS/Windows, UNIX, Macintosh and many more
- It is based on algorithms that have survived extensive public review and are considered extremely secure (eg). RSA,DSS
- It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication
- It was not developed by nor and is it controlled by any government or standard organization.

6. 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?

- One time session conventional keys
- Public keys

9. **List out the features of SET.**
    - Confidentiality
    - Integrity of data
    - Cardholder account authentication
    - Merchant authentication
10. **What is security association?**
    A security association (SA) is the establishment of shared security attributes between two network entities to support secure communication.
11. **What does Internet key management in IPSec?**
    Internet key exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.
12. **List out the IKE hybrid protocol dependence.**
    - ISAKMP - Internet Security Association and Key Management Protocols.
    - Oakley
13. **What does IKE hybrid protocol mean?**
    Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the internet protocol security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.

PART B

1. How IPSec ESP does provide transport and Tunnel Mode operation? Explain with a neatsketch. (16)
2. What is the need for security in IP networks? Describe the IPv6 authentication header.(16)
3. What is PGP? Show the message format of PGP(8)
4. Explain the operational description of PGP(10)
5. Describe about the PKI. (8)
6. Identify the fields in ISAKMP and explain it.(8)
7. Evaluate the different protocols of SSL. Explain Handshake protocol in detail.(16)
8. Describe the phases of Internet key exchange in detail. (16)
9. Explain in detail about S/MIME. (8)