**B.TECH/ECE/6$^{TH}$ SEM/ECEN 3234/2025**

# NETWORK SECURITY
## (ECEN 3234)

**Time Allotted : 2½ hrs** **Full Marks : 60**

***Figures out of the right margin indicate full marks.***

***Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.***

***Candidates are required to give answer in their own words as far as practicable.***

## Group – A

1. Answer any twelve: **12 × 1 = 12**

*Choose the correct alternative for the following*

(i) Use Caesar's Cipher to decipher the following: HQFUBSWHG WHAW
(a) ABANDONED LOCK (b) ENCRYPTED TEXT
(c) ABANDONED TEXT (d) ENCRYPTED LOCK

(ii) How many computation rounds does the simplified Advanced Encryption Standard (AES) consist of?
(a) 5 (b) 2
(c) 8 (d) 10

(iii) Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
(a) Hill Cipher (b) Playfair cipher
(c) Both (a) and (b) (d) None of the above

(iv) The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
(a) Authenticated (b) Joined
(c) Submit (d) Separate

(v) Elliptic curve cryptography offers similar security to RSA with
(a) Larger key sizes (b) Smaller key sizes
(c) More complex computations (d) Simpler key generation

(vi) A message authentication code (MAC) provides
(a) Confidentiality (b) Integrity and authentication
(c) Non-repudiation (d) Availability

(vii) Secure Electronic Transaction (SET) protocol was designed for
(a) Secure online credit card transactions (b) Encrypting emails
(c) Securing web browsing (d) Detecting intrusions

(viii) Which of the following statements is true for Digital Envelope?
(a) Digital envelope is created using the public key of the bank with the RSA algorithm
(b) Digital envelope is created using the private key of the bank with the RSA algorithm
(c) Both (a) and (b)
(d) None of the above

(ix) A Trojan horse disguises itself as
(a) A legitimate program (b) A virus
(c) A worm (d) A firewall

(x) ____________ infects the master boot record and it is a challenging and complex task
(a) Boot sector (b) Polymorphic
(c) Multipartite (d) Trojans

*Fill in the blanks with the correct word*

(xi) The process of verifying the identity of a user is called ___________.

(xii) A proxy firewall filters at ________ layer.

(xiii) In RSA, Φ(n) = ______ in terms of p and q.

(xiv) The Advanced Encryption Standard (AES) cipher operates on data blocks of _________ bits.

(xv) _______are individuals who attempt to gain unauthorized access to computer systems.

## Group - B

2. (a) Explain the CIA triad briefly. *[(CO1) (Understand/LOCQ)]*
(b) Evaluate the subkeys for S-DES where the input key is 3AC. The initial permutation order for the 10-bit key is given as 3, 5, 2, 7, 4, 10, 1, 9, 8, 6. The 8-bit selection post the shifting operations is given as 6, 3, 7, 4, 8, 5, 10, 9. *[(CO2 ,CO6) (Evaluate/HOCQ)]*
(c) Differentiate between active and passive attacks in network security. *[(CO1) (Analyze/IOCQ)]*

**4 + 6 + 2 = 12**

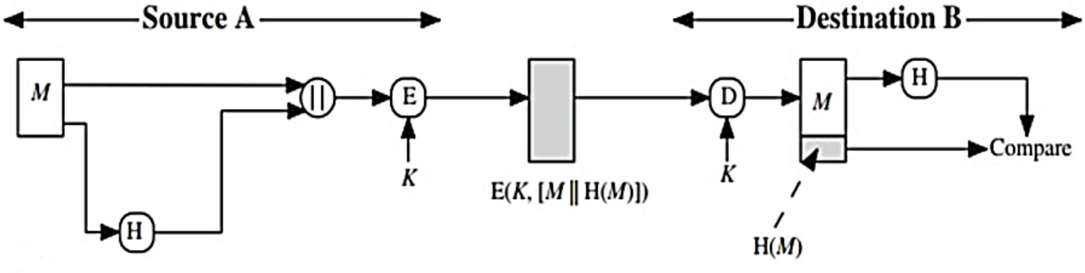
3. (a) Explain a symmetric encryption model with the help of a block diagram. *[(CO2) (Remember/LOCQ)]]*
(b) Differentiate between DES and AES. *[(CO2) (Understand/LOCQ)]*
(c) Explain the process of key generation in DES algorithm. *[(CO2)(Apply/IOCQ)]*

**4 + 4 + 4 = 12**

## Group - C

4. (a) Differentiate between Hash function and Message Authentication Code. *[(CO4) (Analyze/HOCQ)]*
(b) Given below is a way of using hash code (H) with a message (M) while sending a message from user A to user B. Identify the aspects of network security, ensured by the hashing technique used in fig. below. Justify your answer elaborately

explaining hash function (E stands for encryption function; K stands for key, D stands for decryption function)



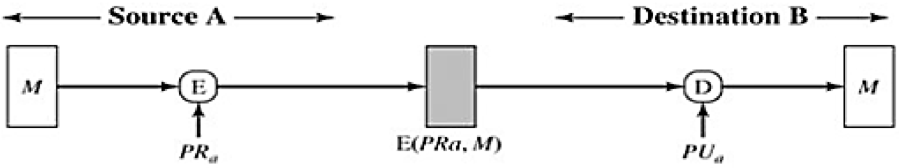
[(CO4) (Analyze/IOCQ)]

(c) Explain the advantage of Elliptic Curve Cryptography over the RSA algorithm. [(CO3)(Remember/LOCQ)]

**3 + 6 + 3 = 12**

5. (a) Explain an asymmetric encryption model with the help of a block diagram. [(CO3)(Understand/LOCQ)]

(b) A message M is getting encrypted from source A using private key of A, *PRa* and decrypted at destination using public key of A, *PUa.* Which aspect of network security is fulfilled in the schematic depicted below?



[(CO4)(Analyse/IOCQ)]

(c) Differentiate between direct digital signature and arbitrated digital signature. [(CO2)(Apply/IOCQ)]

**4 + 5 + 3 = 12**

## Group - D

6. (a) Briefly explain the services provided by the Secure Socket Layer (SSL) Record Protocol. Describe the SSL record protocol format. [(CO4) (Remember/LOCQ)]

(b) Illustrate the difference between an SSL connection and an SSL session. [(CO4) (Remember/LOCQ)]

(c) Compare the Web Security Threats and their Consequences. [(CO4) (Analyze/IOCQ)]

**(2 + 4) + 2 + 4 = 12**

7. (a) Explain the terms PIMD, OIMD, and POMD and their significance in secure electronic transactions. [(CO5) (Remember/LOCQ)]

(b) Briefly describe the sequence of events that are required for Secure Electronic Transaction. [(CO5) (Remember/LOCQ)]

**6 + 6 = 12**

## Group - E

8. (a) List the capabilities and the limitations of a firewall technique. [(CO6) (Remember/LOCQ)]

(b) Explain the packet-filtering router type firewall with a block diagram.
*[(CO6) (Understand/LOCQ)]*

(c) List the attacks that can be made on packet-filtering routers and what could be the appropriate countermeasures. *[(CO6) (Analyse/IOCQ)]*

**4 + 4 + 4 = 12**

9. (a) Define Virus and give a brief overview about the most significant types of viruses.
*[(CO5) (Remember/LOCQ)]*

(b) Define Distributed Denial of Service Attacks (DDoS). Explain the lines of defence as possible countermeasures to prevent the DDoS. *[(CO5) (Understand, Analyse /IOCQ)]*

**(2 + 4) + (2 + 4) = 12**

| Cognition Level | LOCQ | IOCQ | HOCQ |
|---|---|---|---|
| Percentage distribution | 55.21 | 35.42 | 9.37 |