B.TECH/ECE/6TH SEM/ECEN 3234/2022

NETWORK SECURITY
(ECEN 3234)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

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

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) The DES algorithm has a key length of
(a) 128 Bits (b) 32 Bits (c) 64 Bits (d) 16 Bits.

(ii) In brute force attack, on average half of all possible keys must be tried to achieve success.
(a) True (b) False (c) May be (d) Can't say

(iii) Security attacks like masquerading and repudiation are threat to
(a) confidentiality (b) integrity
(c) authenticity (d) none of the above.

(iv) In public key cryptosystem _____ keys are used for encryption and decryption.
(a) same (b) different
(c) encryption keys (d) none of the mentioned

(v) Which are called the block ciphers?
(a) IDEA (b) CAST
(c) Triple-DES (d) All of the mentioned.

(vi) Among the following given options, chose the strongest encryption technique?
(a) DES (Data Encryption Standard) (b) Double DES
(c) Triple DES (d) AES (Advance Encryption Standard).

(vii) Which of the following cannot be chosen as a key in the Caesar cipher?
(a) An integer (b) An alphabet (A-Z or a-z)
(c) A string (d) None of the above.

(viii) Message authentication code is also known as
(a) key code (b) hash code
(c) keyed hash function (d) message key hash function.

(ix) Number of S-boxes used in DES algorithm is
(a) 4 (b) 8 (c) 16 (d) 32.

(x) In the DES algorithm the input key is _____ bit and the keys in every round is _____ bits.
(a) 48, 32 (b) 64, 48 (c) 56, 24 (d) 32, 32

Group- B

2. (a) Describe the model for network security with neat sketch. [(CO1)(Remember/LOCQ)]
(b) Outline any three transposition ciphers with examples. [(CO1)(Analyze/IOCQ)]
(c) Distinguish between stream and block ciphers. [(CO2)(Evaluate/HOCQ)]
4 + 6 + 2 = 12

3. (a) Distinguish between DES and AES. [(CO2)(Analyze/HOCQ)]
(b) Explain the different transposition techniques used for encryption and decryption. [(CO2)(Remember/LOCQ))]
(c) Generate the cipher text for the plain text *hello* with the key value *network* using Playfair cipher. [(CO2)(Evaluate/HOCQ)]
4 + 2 + 6 = 12

Group - C

4. (a) Explain the RSA algorithm for encryption and decryption. [(CO3)(Understand/LOCQ)]
(b) Generate the cipertext for the plaintext *me* using RSA algorithm. Given p = 3, q = 11, e = 7. [(CO3)(Evaluate/HOCQ)]
(c) Alice and Bob use the Diffie–Hellman key exchange technique with a common prime number 11 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the shared secret key. [(CO6)(Evaluate/HOCQ)]
4 + 4 + 4 = 12

5. (a) Explain the key generation process of RSA cryptosystem. Bob chooses p = 17, q = 11, and selects e = 7. Find the value of n, $\phi(n)$, and d. [(CO6)(Evaluate/HOCQ)]
(b) Illustrate the benefits of Digital Signature. [(CO3)(Understand/LOCQ)]
(4 + 4) + 4 = 12

Group - D

6. (a) List and briefly define three classes of intruders. What is the difference between statistical anomaly detection and rule-based intrusion detection? [(CO5)(Analyze/IOCQ)]
(b) Classify the difference between a SSL connection and a SSL session. [(CO5)(Evaluate/HOCQ)]

(c) For what applications is SSH useful? [(CO5)(Analyze/IOCQ)]

(4 + 3) + 3 + 2 = 12

7. (a) Explain secure electronic transaction with neat diagram. [(CO4)(Understand/LOCQ)]

(b) List and briefly explain three classes of intruders. [(CO5)(Understand/LOCQ)]

8 + 4 = 12

Group - E

8. (a) Explain about different types of distributed denial of service attacks. [(CO2)(Remember/LOCQ)]

(b) List four techniques used by firewalls to control access and enforce a security policy. [(CO2)(Understand/LOCQ)]

(c) What is a circuit-level gateway? [(CO4)(Analyse/IOCQ)]

4 + 4 + 4 = 12

9. (a) What information is used by a typical packet-filtering router? [(CO3)(Remember/LOCQ)]

(b) What are some weaknesses of a packet-filtering router? [(CO3)(Analyse/IOCQ)]

(c) Illustrate the role of encryption in the operation of a virus. [(CO5)(Analyse/IOCQ)]

4 + 4 + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	36	28	36

Course Outcome (CO):

After the completion of the course students will be able to

1. Understand various tools and protocols for different levels of security.
2. Compare various Cryptographic Techniques.
3. Describe the principles of public-key cryptosystems, hash functions, and digital signature.
4. Add secure coding in the developed applications.
5. Have enough knowledge about various Intrusion algorithm.
6. Design secure systems and applications.

*LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question