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) In secure electronic transaction protocol a customer encrypt's credit card number using
(a) his private key (b) bank's public key
(c) bank's private key (d) merchant's public key.

(ii) The Data Encryption Standard (DES) follows
(a) Hash Algorithm (b) Caesars Cipher
(c) Feistel Cipher Structure (d) SP Networks.

(iii) Which of the following is correct in connection with the password policy?
(a) Usually, password length must be more than 8 characters
(b) Password must contain upper case, lower case, numbers, and special characters
(c) There should be different passwords for different login accounts.
(d) All of the above.

(iv) The art of breaking ciphers is called?
(a) Cryptography (b) Cryptology
(c) Cryptanalysis (d) All of the mentioned.

(v) Data encryption standard is a block cipher and encrypts data in blocks of size of _____ each.
(a) 16 bits (b) 64 bits
(c) 32 bits (d) all of the mentioned above

(vi) The S-DES algorithm has a key length of
(a) 10 bits (b) 8 bits
(c) 64 bits (d) 16 bits.

(vii) Which of the following ciphers uses asymmetric key cryptography?
(a) Rail Fence Cipher (b) Data Encryption Standard (DES)
(c) Diffie Hellman Cipher (d) None of the above.

(viii) The AES algorithm has a key length of
(a) 128 bits (b) 192 bits (c) 256 bits (d) all of the above.

(ix) In RSA algorithm if p=7, q=11, and e=13 then what will be the value of d?
(a) 40 (b) 13 (c) 37 (d) 23

(x) Dividing (11001001) by (100111) gives remainder
(a) 11 (b) 111 (c) 101 (d) 110.

Group - B

2. (a) Explain the DES (Data Encryption Standard) encryption algorithm. [(CO1,CO2)(Remember/LOCQ)]
(b) Illustrate the purpose of the S-boxes in Data Encryption Standard. [(CO1,CO2)(Analyze/IOCQ)]
(c) Explain the encryption process in Affine Cipher Technique. [(CO2)(Evaluate/HOCQ)]
8 + 2+ 2 = 12

3. (a) Evaluate the subkeys for S-DES where, input key is 5AC. 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)]
(b) Illustrate the design principles of block cipher technique. [(CO3)(Understand/LOCQ)]
(c) Differentiate between DES and AES. [(CO2)(Understand/LOCQ)]
6 + 3 + 3 = 12

Group - C

4. (a) Differentiate between Public Key cryptosystem and Private Key cryptosystem. [(CO2,CO3)(Analyze/IOCQ)]
(b) Alice and Bob use the Diffie–Hellman key exchange technique with a common prime number 7 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the public keys of A and B, and also their shared secret key. [(CO3,CO6)(Evaluate/HOCQ)]
(c) Explain the key generation process in Elliptic Curve Cryptography technique. [(CO3)(Analyze/IOCQ)]
4 + 4 + 4 = 12

5. (a) What are the properties a digital signature should have? What requirements should a digital signature scheme satisfy? [(CO3)(Understand/LOCQ)]
(b) Outline the difference between direct and arbitrated digital signature. [(CO3)(Understand/LOCQ)]
(c) Give examples of replay attacks. What is a suppress-replay attack? [(CO3)(Analyze/IOCQ)]
(2 + 2) + 4 + (2 + 2) = 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 secure electronic transaction with neat diagram. [(CO4)(Understand/LOCQ)]
   (b) Explain briefly the different techniques used to eliminate guessable password. [(CO5)(Understand/LOCQ)]
   8 + 4 = 12

Group - E

8. (a) List the capabilities and the limitations of a firewall technique. [(CO5)(Remember/LOCQ)]
   (b) Explain the packet-filtering router type firewall with a block diagram. [(CO5)(Understand/LOCQ)]
   (c) What are the attacks that can be made on packet-filtering routers and what could be the appropriate countermeasures. [(CO5)(Analyse/IOCQ)]
   4 + 4 + 4 = 12

9. (a) Define virus and give a brief overview about the most significant types of viruses. [(CO6)(Remember/LOCQ)]
   (b) Define Distributed Denial of Service Attacks (DDoS). Explain the lines of defence as possible countermeasures to prevent the DDoS. [(CO6)(Understand, Analyse/IOCQ)]
   (2 + 4) + (2 + 4) = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	58.33	29.16	12.50

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.