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) In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
(a) 48, 32 (b) 64, 32 (c) 56, 24 (d) 32, 32

(ii) _____ is the term used in computer security to protect the data from being modified by the unauthorized user.
(a) Integrity (b) Authentication
(c) Confidentiality (d) Availability

(iii) Which are the most frequently found letters in the English language?
(a) e,a (b) e,o (c) e,t (d) e,i.

(iv) ..... is an example for public key algorithm.
(a) RSA (b) DES (c) AES (d) None of the above

(v) How many computation rounds does the simplified Advanced Encryption Standard (AES) consists of
(a) 5 (b) 2 (c) 8 (d) 10.

(vi) The AES algorithm has a key length of
(a) 128 Bits (b) 192 Bits (c) 256 Bits (d) All of the above.

(vii) _____ is the term used in computer security that only the authorized users are allowed to access the information.
(a) Integrity (b) Authentication (c) Confidentiality (d) Availability

(viii) Which of the following ciphers is a block cipher?
(a) Caesar cipher (b) Vernam cipher
(c) Playfair cipher (d) None of the above.

(ix) 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) 4 Separate.

(x) CIA stands for

(a) Compressibility, Integrity, Availability

(b) Confidentiality, Integrity, Accountabilty

(c) Confidentiality, Integrity, Availability

(d) None of the above.

Fill in the blanks with the correct word

(xi) The art of breaking ciphers is called _____.

(xii) DDoS stands for _____.

(xiii) The information that gets transformed in encryption is _____.

(xiv) In _____key exchange, the computed shared secret keys are identical.

(xv) _____ is an authentication technique that is used to check the repudiation from the sender side or from the receiver side.

Group - B

2. (a) Explain the OSI security architecture. *[(CO1)(Remember/LOCQ)]*

(b) With the help of a neat diagram explain the overall architecture of DES algorithm. *[(CO2)(Understand/LOCQ)]*

(c) Explain the different transposition techniques used for encryption and decryption. *[(CO2)(Remember/LOCQ))]*

3 + 6 + 3 = 12

3. (a) What is the difference between mono alphabetic and poly alphabetic cipher? *[(CO2)(Analyse/IOCQ)]*

(b) Explain the difference between Passive security attack and active security attack. *[(CO3)(Remember/LOCQ)]*

(c) Explain the attacks that threaten the three elements of the CIA triad. *[(CO3)(Remember/LOCQ)]*

4 + 2 + 6 = 12

Group - C

4. (a) Let q=353 and α =3, X_a=97, X_b=233. Use the Diffie-Hellman Key exchange algorithm to find Y_a, Y_b and, Secret key K. *[(CO6)(Evaluate/HOCQ)]*

(b) Discriminate the Hash function and Message Authentication Code? *[(CO3)(Analyse/IOCQ)]*

8 + 4 = 12

5. (a) 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. 1. Justify your answer elaborately explaining hash function (E stands for encryption function; K stands for key, D stands for decryption function)

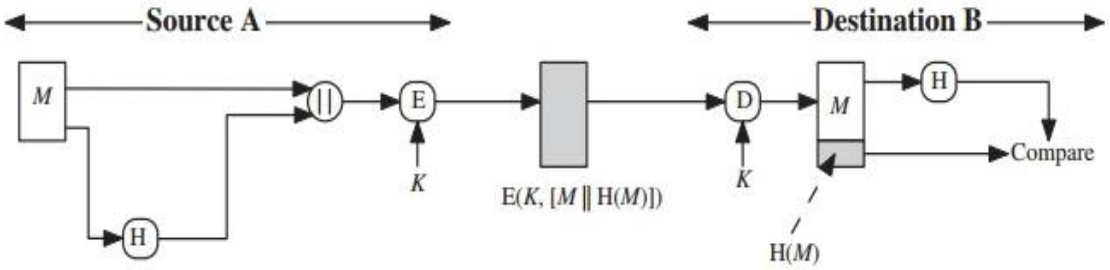

Fig. 1

[(CO3)(Analyze/IOCQ)]

(b) Differentiate between Hash function and Message Authentication Code. *[(CO3)(Analyze/IOCQ)]*

(c) Explain the advantage of ECC over RSA algorithm. *[(CO3)(Remember/LOCQ)]*

6 + 3 + 3 = 12

Group - D

6. (a) Write the methodology involved in computing the keys in Secure Sockets Layer (SSL) protocol. *[(CO3)(Evaluate/HOCQ)]*

(b) Describe how master secret is created from pre-master secret in Transport Layer Security (TLS). *[(CO4)(Remember/LOCQ)]*

8 + 4 = 12

7. (a) Explain the process of creating Dual Signature in Secure Electronic Transaction. *[(CO4)(Understand/LOCQ)]*

(b) Differentiate between statistical anomaly detection and rule-based intrusion detection. *[(CO5)(Analyse/IOCQ)]*

(c) Differentiate between SSL session and SSL connection. *[(CO4)(Analyse/IOCQ)]*

6 + 3 + 3 = 12

Group - E

8. (a) Explain the features of trusted OS. *[(CO6)(Remember/LOCQ)]*

(b) Explain the phases of operation of a virus. *[(CO6)(Understand/LOCQ)]*

(c) Explain the main services of the OS with respect to security. *[(CO6)(Remember/LOCQ)]*

4 + 6 + 2 = 12

9. (a) What is a Firewall? Discuss any three types of Firewall. *[(CO6)(Remember/LOCQ)]*

(b) Discuss Circuit-level gateway. *[(CO4)(Remember/LOCQ)]*

(2 + 6) + 4 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	59.38	23.96	16.66

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.*