CRYPTOGRAPHY AND NETWORK SECURITY
(MCA 1232)

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) If ϕ denotes Euler's totient function, then value of ϕ(43) is _____
(a) 24 (b) 37 (c) 42 (d) 1

(ii) DES uses a key generator to generate _____ 48-bit round keys.
(a) sixteen (b) eighteen
(c) twenty-four (d) thirty two

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

(iv) _____ substitution is a process that accepts 48 bits from the XOR operation.
(a) S-box (b) P-box
(c) expansion permutations (d) key transformation

(v) _____ provides privacy, integrity, and authentication in e-mail.
(a) IPSec (b) SSL (c) PGP (d) none of the above

(vi) "An attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges" - what wireless network threat is this?
(a) man in the middle attack (b) identity theft
(c) accidental association (d) network injection

(vii) Digital signature cannot provide _____ for the message.
(a) integrity (b) confidentiality
(c) nonrepudiation (d) authentication

(viii) Which one of the following is not a public key distribution technique?
(a) public-key certificates (b) hashing certificates
(c) publicly available directories (d) public-key authority

(ix) In brute force attack, on an average half of all possible keys must be tried to achieve success.
(a) true (b) false (c) maybe (d) can't be said

(x) What is the maximum length of the message (in bits) that can be taken by SHA-512?
(a) 2^128 (b) 2^256 (c) 2^64 (d) 2^192.

Fill in the blanks with the correct word

(xi) _____ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.

(xii) _____ means that a sender must not be able to deny sending a message that he sent.

(xiii) In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.

(xiv) The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.

(xv) A packet filter firewall filters at the _____.

Group - B

2. (a) Reproduce the difference between active and passive security attacks. *[(CO1)(Remember/LOCQ)]*
(b) State why replay attacks are considered to be fatal. *[(CO1)(Remember/LOCQ)]*
(c) Define the basic security services. *[(CO1)(Remember/LOCQ)]*

5 + 2 + 5 = 12

3. (a) Use Euclidean algorithm to determine gcd (4655, 12075). *[(CO2)(Understand/LOCQ)]*
(b) Prove the following: a ≡ b (mod n) and b ≡ c (mod n) imply a ≡ c (mod n). *[(CO2)(Remember/LOCQ)]*

6 + 6 = 12

Group - C

4. (a) Briefly demonstrate the Hill cipher with an example. *[(CO3)(Analyze/IOCQ)]*
(b) What is triple encryption? Why is the middle portion of 3DES a decryption rather than an encryption? *[(CO3)(Analyze/IOCQ)]*

6 + (3 + 3) = 12

5. (a) Explain how Vernam cipher works by enciphering the following text "V E R N A M C I P H E R" using the: 76 48 16 82 44 3 58 11 60 5 48 88. *[(CO3)(Apply/IOCQ)]*
(b) What is a meet-in-the-middle attack in context of double DES? *[(CO3)(Apply/IOCQ)]*

6 + 6 = 12

Group - D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 3; q = 11, e = 7; M = 5. *[(CO4)(Analyze/IOCQ)]*
   (b) Explain factoring attack and timing attack on RSA. *[(CO4)(Analyze/IOCQ)]*

6 + 6 = 12

7. (a) Examine the working principle of SHA. *[(CO4)(Analyze/IOCQ)]*
   (b) Distinguish between direct and arbitrated digital signature. Examine some threats associated with a direct digital signature scheme. *[(CO4)(Analyze/IOCQ)]*

6 + 6 = 12

Group - E

8. (a) Evaluate the requirements for Kerberos? What entities constitute a full-service Kerberos environment? *[(CO5)(Evaluate/HOCQ)]*
   (b) What is the purpose of the X.509 standard? What are the key elements of an X.509 certificate? *[(CO6)(Create/LOCQ)]*

(3 + 3) + (3 + 3) = 12

9. (a) Assume that passwords are limited to the 95 printable ASCII characters and all passwords are 10 characters in length. How long will it take for a password cracker, with an encryption rate of 6.4 million encryptions per second, to test exhaustively all possible passwords on a UNIX system? *[(CO5)(Evaluate/HOCQ)]*
   (b) Interpret the parking lot attack that can be launched on wireless networks. What security measures can be taken to mitigate this attack? *[(CO6)(Create/HOCQ)]*

6 + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	31.25	50	18.75

Course Outcome (CO):

After the completion of the course students will be able to
CO1. Recall the security goals, threats, vulnerabilities and attacks, types of attacks, security services and mechanisms.
CO2. Apply different mathematical concepts for formulating cryptographic algorithms.
CO3. Identify different symmetric key cryptographic algorithms.
CO4. Examine different asymmetric key cryptographic algorithms and hash functions.
CO5. Evaluate different authentication, e-mail, IP, web and system security applications.
CO6. Appraise wireless network security.

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