CRYPTOGRAPHY AND NETWORK SECURITY
(MCA1232)

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) Which of the following is a mechanism used to achieve data integrity in a secure communication channel?
(a) Encryption (b) Hashing
(c) Access Control (d) Digital Signatures

(ii) Which of the following best defines the discrete logarithm problem?
(a) Given $a^x \equiv b \pmod p$, find x
(b) Given two numbers a and b, find the greatest common divisor gcd(a,b)
(c) Given a number a, find its modular inverse
(d) Given a prime p, find the multiplicative inverse of p

(iii) If Ø denotes Euler's totient function, then value of Ø(37) is
(a) 24 (b) 37 (c) 36 (d) 1

(iv) What is the primary vulnerability in symmetric key encryption?
(a) It relies on large prime numbers
(b) The key used for encryption must be kept secret, and if the key is compromised, the entire system is at risk
(c) It uses complex algorithms that are computationally expensive
(d) The encryption process is very slow

(v) Which of the following is true about the RC4 stream cipher?
(a) RC4 uses a fixed-size key and a fixed-size block for encryption
(b) RC4 is a symmetric stream cipher that operates on variable-length keys
(c) RC4 is based on asymmetric encryption
(d) RC4 is faster than AES and is widely used for secure email encryption

(vi) The security of the Diffie-Hellman Key Exchange relies on which of the following mathematical problems?
(a) Integer factorization problem (b) Discrete logarithm problem
(c) Elliptic curve point multiplication problem (d) RSA factorization problem

(vii) In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
(a) p and q should be divisible by Φ(n) (b) p and q should be co-prime
(c) p and q should be prime (d) p/q should give no remainder

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

(ix) _____ uses the idea of certificate trust levels.
(a) X.509 (b) PGP
(c) KDC (d) none

(x) _____ provide security at the transport layer.
(a) SSL (b) TLS
(c) either (a) or (b) (d) both (a) and (b)

Fill in the blanks with the correct word

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

(xii) DES consists of _____ rounds to perform the substitution and transposition techniques

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

(xiv) A packet filter firewall filters at the _____

(xv) In email security, _____ is a standard that provides encryption and digital signatures for email messages, using a combination of public key cryptography and certificates.

Group - B

2. (a) Use Fermat's Little Theorem to compute $7^{13} \pmod{11}$. *[(CO2)(Apply/IOCQ)]*
(b) Explain the core security goals in information security. How do they help in protecting systems and data from unauthorized access? *[(CO1)(Remember/LOCQ)]*

6 + 6 = 12

3. (a) Solve the system of congruences using the Chinese Remainder Theorem: $x \equiv 4 \pmod{5}$, $x \equiv 3 \pmod{7}$. *[(CO2)(Apply/IOCQ)]*
(b) Explain the difference between a 'Phishing' attack and a 'Man-in-the-Middle' (MitM) attack. Provide an example of each. *[(CO1)(Understand/LOCQ)]*

6 + 6 = 12

Group - C

4. (a) What is the difference between diffusion and confusion? Explain with suitable example. *[(CO3)(Understand/LOCQ)]*
(b) Describe the key schedule process in DES. How is the 56-bit key used to generate

the 16 subkeys required for each round of the DES encryption process? Provide an example illustrating this process. *[(CO4)(Evaluate/HOCQ)]*

5 + 7 = 12

5. (a) Given the plaintext message "ATTACKATDAWN" and the key 'SECRET', perform the encryption process using the Vigenère cipher. Show the step-by-step calculation for each letter and provide the final ciphertext. *[(CO3)(Apply/IOCQ)]*

   (b) Evaluate the Feistel encryption and decryption scheme with help of the Feistel structure diagram. *[(CO3)(Evaluate/HOCQ)]*

5 + 7 = 12

Group - D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 7; q = 11, e = 17; M = 8. *[(CO4)(Apply/IOCQ)]*

   (b) In an ElGamal scheme with common prime q = 17 and a primitive root a = 6.
   a. If B has private key $X_B = 5$, find the public key of B.
   b. If A chose the random integer k=2, what is the ciphertext of M=30?
   [(CO4)(Apply/IOCQ)]

6 + (3 + 3) = 12

7. (a) Explain the concept and working of a Digital Signature. Discuss how it ensures authenticity and integrity in a communication system. *[(CO4)(Analyse/HOCQ)]*

   (b) How can Digital Signatures be combined with the Diffie-Hellman Key Exchange to enhance the security of a communication session? *[(CO4)(Understand/LOCQ)]*

8 + 4 = 12

Group - E

8. (a) Defend the decision to have a separate Change Cipher Spec Protocol in SSL/TLS rather than including it in the Handshake Protocol. *[(CO5) (Analyse/IOCQ)]*

   (b) Explain the difference between statistical anomaly detection and rule-based intrusion detection. *[(CO5) (Remember/LOCQ)]*

6 + 6 = 12

9. (a) Analyze the role of key-management functions in ensuring the security and integrity of messages in S/MIME. *[(CO5) (Analyse/IOCQ)]*

   (b) Interpret the parking lot attack that can be launched on wireless networks. What security measures can be taken to mitigate this attack? *[(CO6) (Analyse/IOCQ)]*

6 + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	40.63	36.46	22.91