CRYPTOGRAPHY AND NETWORK SECURITY
(MCAP 2160)

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) If a|b and b|c, then a|c.
(a) true (b) false (c) maybe (d) can't be said

(ii) Use Caesar's Cipher to decipher: HQFUBSWHG WHAW
(a) ABANDONED LOCK (b) ENCRYPTED TEXT
(c) ABANDONED TEXT (d) ENCRYPTED LOCK

(iii) A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.
(a) S-box (b) P-box (c) T-box (d) none of the above

(iv) _____ means that a sender must not be able to deny sending a message that he sent.
(a) Confidentiality (b) Integrity (c) Authentication (d) Non-repudiation

(v) Which of the following is a valid property of modular arithmetic?
(a) a = b (mod n) if n|(a-b)
(b) a = b (mod n) implies b = a (mod n)
(c) a = b (mod n) and b = c (mod n) implies a = c (mod n)
(d) All of the mentioned.

(vi) 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.

(vii) In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.
(a) 1024 (b) 512 (c) 256 (d) 1248

(viii) Meet in the middle attack is an attack where,
(a) timing required for the attack via brute force is drastically reduced
(b) adversary uses 2 or more machines to decrypt thus trying to reduce the time
(c) messages are intercepted and then either relayed or substituted with another message
(d) cryptanalysis takes lesser time than the brute force decryption.

(ix) "A user intending to connect to one LAN may unintentionally lock onto a wireless access point from the neighboring network." Which type of wireless network threat would you classify this under?
(a) Malicious threat (b) Network injection
(c) Denial of service (d) Accidental association.

(x) A packet filter firewall filters at the
(a) application or transport layer (b) physical layer
(c) network or transport layer (d) data link layer.

Group- B

2. (a) Define the categories of security mechanisms as mentioned in the X.800 security standard. [(CO1)(Remember/LOCQ)]
(b) Reproduce the replay attack? [(CO1)(Remember/LOCQ)]
(c) Recall the difference between phishing and pharming. Why is it easy to fall prey to pharming than phishing? [(CO1)(Remember/LOCQ)]
6 + 3 + 3 = 12

3. (a) Let P = P [gcd (a, b) = 1]. Prove that P [gcd (a, b) = d] = P/d^2.
[(CO2)(Understand /LOCQ)]
(b) Prove the following: a ≡ b (mod n) implies b ≡ a (mod n).
[(CO2)(Understand /LOCQ)]
6 + 6 = 12

Group - C

4. (a) Using the Vigenère cipher, encrypt the word "explanation" using the key "leg".
[(CO3)(Apply/IOCQ)]
(b) Interpret the concept of diffusion and confusion? [(CO3)(Apply/IOCQ)]
9 +3 = 12

5. (a) Illustrate the process of encryption and decryption of the message "pay" using Hill cipher
with the key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. [(CO3)(Apply/IOCQ)]
(b) Choose an RC4 key value that will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order. [(CO3)(Apply/IOCQ)]
9 + 3 = 12

Group - D

6. (a) Calculate the cipher text (encryption) and the consequent plain text (decryption) using the RSA algorithm, for the following: p = 7; q = 11, e = 17; M = 8.
[(CO4)(Analyze/IOCQ)]

(b) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7.
(i) If user A has private key $X_A = 5$, what is A's public key Y_A?
(ii) If user B has private key $X_B = 12$, what is B's public key Y_B?
What is the shared secret key? [(CO4)(Analyze/IOCQ)]
6 + 6 = 12

7. (a) (i) How can two parties Bob and Alice initiate a secure communication using symmetric key cryptography in an open network environment, if they do not possess any asymmetric keys? You can assume that a public key authority is available.
(ii) Now if they possess asymmetric keys, how will Bob and Alice initiate a secure communication using symmetric key cryptography in the open network environment? [(CO4)(Analyze/IOCQ)]
(b) Outline with a diagram the role of a public key authority. [(CO4)(Analyze/IOCQ)]
(4 + 4) + 4 =12

Group - E

8. (a) Evaluate realm, in the context of Kerberos? What do you understand by realm and multiple kerberi? [(CO5)(Evaluate/HOCQ)]
(b) Summarize why and how is an X.509 certificate revoked? [(CO5)(Evaluate/HOCQ)]
(3 + 3) + (3 + 3) = 12

9. (a) Consider a situation: an attacker (A) creates a digital certificate, puts a genuine organizations name (say Bank B) and puts the attacker's own public key. You get this certificate from the attacker, without knowing that the attacker is sending it. You think it is from the Bank B. How can this be prevented or resolved?
In another situation, the attacker (A) changes the bank's genuine certificate by replacing the bank's public key in the certificate with his own. How can this be prevented or resolved? [(CO5)(Evaluate/HOCQ)]
(b) A phonetic password generator picks two segments randomly for each six-letter password.
The form of each segment is CVC (consonant, vowel, consonant), where V = <a, e, i, o, u> and C = $\bar{V}$
(i) What is the total password population?
(ii) What is the probability of an adversary guessing a password correctly?
[(CO5)(Evaluate/HOCQ)]
(3 + 3) + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	25	50	25

Course Outcome (CO):

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