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?

   (b) Explain the parking lot attack that can be launched on wireless networks.

   (c) What are the vulnerabilities of WEP?

6 + 3 + 3 = 12

CRYPTOGRAPHY AND NETWORK SECURITY
(MCAP 3160)

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) _____ 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.

   (ii) 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.

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

   (iv) In _____, there can be multiple paths from fully or partially trusted authorities.
   (a) X509 (b) PGP
   (c) KDC (d) none of the above.

   (v) 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.

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

(vii) Meet in the middle attack is an attack where
(a) timing required for the attack via brute force is drastically reduced
(b) adversary uses two 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.

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

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

(x) "An attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges" - which wireless network threat is this?
(a) Man in the middle attack (b) Identity theft
(c) Accidental association (d) Network injection.

Group - B

2. (a) List and briefly define the categories of security mechanisms as mentioned in the X.800 security standard.

(b) Give an example of replay attack. Why are they considered to be fatal?

(c) Distinguish between phishing and pharming. Why is it easy to fall prey to pharming than phishing?

6 + 3 + 3 = 12

3. (a) Use Euclidean algorithm to determine gcd (24140, 16762).

(b) Prove the following: a ≡ b (mod n) implies b ≡ a (mod n).

6 + 6 =12

Group - C

4. (a) Briefly explain the Caesar cipher with an example.

(b) What is a Feistel cipher? Explain Feistel encryption and decryption with help of the Feistel structure diagram.

6 + 6 =12

5. (a) Encrypt the message "pay" using the Hill cipher with the key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

(b) What is triple encryption? Why is the middle portion of 3DES a decryption rather than an encryption?

9 + 3 = 12

Group - D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 7; q = 11, e = 17; M = 8

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

6 + 6 =12

7. (a) Explain with a diagram the role of a public key authority. Evaluate the importance of a nonce.

(b) What is the difference between direct and arbitrated digital signature? What are some threats associated with a direct digital signature scheme?

(4 + 2) + (2 + 4) = 12

Group - E

8. (a) In the context of Kerberos, what is a realm? What do you understand by realm and multiple kerberi?

(b) Why and how is an X.509 certificate revoked?

(3 + 3) + 6 = 12