End Semester Examination, 2022

Semester - VI

Subject - BCA

Cyber Security and Cyber Laws

PAPER - C13T

Full Marks : 40

Time : 2 Hours

Group - A

Attempt any five questions : **5x2=10**

1.a. What do you mean by message digest ?

b. State Kerckhoffs's principle.

c. What is the key length of DES ?

d. What is the additive inverse of 5 modulo 11 ?

e. What is dictionary attack ?

f. What is fire-wall ?

g. What is Hacking ?

h. What is salami attacks ?

Group - B

Attempt any four questions : **4x5=20**

2. Explain in brief about Diffie-Hellman key exchange protocol.

3. Design a simple LFSR based stream cipher.

4. Explain the three desirable properties of crypto-graphic hash function. Find multiplicative inverse of 3 modulo 13. 3+2

(Turn Over)

5. Explain the security challenges in cyber space.
6. What do you mean by confusion and diffusion ?
7. Explain the control measures against malicious software.
8. Describe IPsec protocol and security services.

Group - C

Attempt any <u>one</u> question : **1x10=10**

9. a) Suppose, $p = 7$, $q = 11$. For these two primes, find the public key and private key by following RSA algorithm. 6
   b) Write the algorithm of RC4 stream cipher. 4
10. a) Describe in brief about one round of DES block cipher. 5
    b) Describe in brief about MD4 hash function. 5