

T.E. / COMP / Sem-VI / CBCGS / R-19 / 'C' Schemes / Subj - CBSS / S.H. 2024

Date: - 05/12/2024

Q.P. Code: - 10089762
[Max Marks: 80]

Duration: 3 hours

- N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

- Q1.** 20
- a. Explain TCP/IP vulnerabilities layer wise.
 - b. Give examples of replay attacks. List three general approaches for dealing with replay attack.
 - c. Explain algorithmic modes encryption process of symmetric key.
 - d. Explain different hash algorithm properties.
- Q2 a.** Apply Diffie Hellman key exchange algorithm, two users P & Q will agree on two numbers as $n=11$ common prime & $g=7$ is generator. $x=3$, $y=6$ are private keys of P & Q respectively. What is shared secret key? 10
- b.** Discuss DES with reference to following points 10
1. Block size and key size
 2. Need of expansion permutation
 3. Role of S-box.
 4. Weak keys and semi weak keys
 5. Possible attacks on DES
- Q3 a.** What characteristics are needed in secure hash function? Explain secure hash algorithm on 512 bits. 10
- b.** Use RSA algorithm, user A has public key (17,321), B has public key (5,321). Calculate private keys of both the users. Encrypt $m=7$ by B's public keys. How B can decrypt the same. 10
- Q4 a.** How does PGP achieve confidentiality and authentication in emails? 10
- b.** Use the Play fair cipher with the key "DOCUMENT" to encrypt the message "ALL THE BEST" 10
- Q5 a.** Why are digital certificates and signatures required? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm. 10
- b.** What are different types of firewalls? How firewall is different from IDS. 10
- Q6 a.** Explain DES algorithm with flowcharts. 10
- b.** What is DDOS Attack and how it is launched? 10