Roll No……..….. **Total No. of Printed Pages: 1**

Total No. of Questions: [09]

B. Tech. (CSE) (Semester – 7th)
CRYPTOGRAPHY & NETWORK SECURITY
Subject Code: BCSED1723
Paper ID: [18111145]

Time: 03 Hours **Maximum Marks: 60**

Instruction for candidates:

1. Section A is compulsory. It consists of 10 parts of two marks each.
2. Section B consist of 5 questions of 5 marks each. The student has to attempt any 4 questions out of it.
3. Section C consist of 3 questions of 10 marks each. The student has to attempt any 2 questions.

Section – A **(2 marks each)**

Q1. Attempt the following:

a) Differentiate between stream ciphers and block ciphers.
b) Write a short note on finite fields.
c) What is the primary difference between AES and DES encryption algorithms?
d) Discuss some of the methods used to test for primality?
e) Discuss the role of a one-way hash function.
f) What is the purpose of a digital certificate in X.509?
g) What is the primary function of Kerberos in network security?
h) Define the role of a firewall in securing a network.
i) Discuss Fermat's Little Theorem.
j) What is a classical cryptosystem, and how does it differ from modern cryptosystems?

Section – B **(5 marks each)**

Q2. Explain the role of security services in cryptography and their significance in modern security systems.
Q3. Explain the concept of differential cryptanalysis and how it can be used to attack block ciphers like DES.
Q4. Explain how the ElGamal public key cryptosystem works and discuss its main advantages.
Q5. Explain the working of the SSL/TLS protocol and how it ensures secure web communication.
Q6. What are LFSR sequences, and how are they used in stream ciphers?

Section – C **(10 marks each)**

Q7. Discuss the RSA encryption algorithm in detail. Explain its key generation, encryption, and decryption processes, with examples.
Q8. Discuss the security implications of the birthday attack and how it can be mitigated in hash functions.
Q9. Discuss the structure and functioning of the Public Key Infrastructure (PKI) with X.509 certificates. How does PKI enhance the security of digital communications?