13/06/2025 TE EXTC SEM-V C-SCHEME DCC QP CODE: 10088078

Duration: 3 hours **Max Marks: 80**

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.

Q.1 Solve **any FOUR** questions. **[20]**

a What is a firewall? Explain its design principles. **[05]**

b Differentiate between arithmetic and dictionary coding techniques. **[05]**

c Explain the role of Discrete Cosine Transform (DCT) in image compression. **[05]**

d What are the major goals of data security? **[05]**

e State and prove Fermat's Little Theorem. **[05]**

Q. 2 **a** Explain DES algorithm in detail with its architecture. **[10]**

b Describe the H.264 video encoding and decoding process. **[10]**

Q. 3 **a** Compare JPEG and JPEG-2000 compression standards with respect to their architecture and performance **[10]**

b Explain RSA algorithm to encrypt the plain text message, M=9 for prime numbers p=11 and q=13, public key e =7. Verify that the decrypted text is the same as plain text. **[10]**

Q. 4 **a** Given a message "ABACAB" and the following probability distribution: **[10]**

- P(A) = 0.5
- P(B) = 0.3
- P(C) = 0.2

Perform **Arithmetic Coding** for the given message. Show all the intermediate steps, including the range calculation for each symbol.

b How Bob and Alice can do the key exchange using Diffie-Hellman Key Exchange algorithm? Explain with appropriate example. **[10]**

Q. 5 **a** Explain Intrusion Detection System and its types with examples. **[10]**

b What are the drawbacks of LZ77 dictionary technique and explain how it is overcome using LZ78 method with appropriate example and initial dictionary. **[10]**

Q. 6 **a** What is the difference between digital signature and message authentication code? Explain their roles in ensuring secure communication. **[10]**

b Prove the Chinese Remainder Theorem and illustrate it with a practical application in modular arithmetic. **[10]**
