

(3 Hours)

[Total Marks: 80]

N.B. (1) Question No. 1 is compulsory.

(2) Attempt any three questions out of remaining five.

(3) Figures to the right indicate full marks.

(4) Assume suitable data if required and mention the same in answer sheet

1. Solve any four 20
- (a) Why we use DCT in JPEG?
 - (b) What is biometric authentication?
 - (c) Why we need data compression?
 - (d) What are the various models used for data compression?
 - (e) Explain Chinese Remainder theorem (CRT) with example
2. (a) A Source emits letters from alphabet $M = [m_1, m_2, m_3, m_4, m_5]$ with probabilities $P(m_1) = 0.15$, $P(m_2) = 0.05$, $P(m_3) = 0.25$, $P(m_4) = 0.05$ and $P(m_5) = 0.50$. 10
- i) Calculate entropy of this source. 10
 - ii) Find Huffman code for this source.
 - iii) Find Average length of this code.
 - iv) Find its redundancy.
- (b) What is the significance of prime numbers in public key cryptography? Explain RSA algorithm with suitable example.
3. (a) Explain : 10
- i) Fermat's little theorem with example.
 - ii) Euler's phi function with example
- (b) Take an alphabet string and show encoding procedure for LZ78 and LZW. Compare LZ78 and LZW 10

4. (a) Explain the working of standard. DES with suitable diagram. **10**
(b) Explain Ceaser Cipher and multiplicative ciphers with suitable examples and diagrams. **10**
5. (a) Explain Hashed MAC with suitable diagram. **10**
(b) Explain Intrusion detection system. **10**
6. Write short note on (**any four**) **20**
- (a) μ -law and A-law Companding with digital audio
 - (b) S/MIME
 - (c) JPEG 2000
 - (d) Diffie-Hellman key exchange
 - (e) MPEG-2