

- N.B.** (1) Question No. 1 is **compulsory**.
 (2) Attempt any **four** out of remaining **six** questions.
 (3) Assume suitable data wherever **necessary**.

1. Attempt any **four** :- 20
- State and explain different classes of complexity.
 - Explain convolution codes.
 - State Fermat's Little Theorem, Justify its need.
 - Give various probable a Hacks on cryptography.
 - What are lossy and lossless compression techniques ?
2. (a) Give significance of prime numbers in Information Theory. Give the steps of Rabin Miller test for identifying prime number. 10
 (b) Describe various properties of Modular Arithmetic with suitable examples. 10
3. (a) State Chinese Remainder Theorem using it solve for X . 10

$$X = 1 \text{ MOD } 2$$

$$X = 2 \text{ MOD } 3$$

$$X = 2 \text{ MOD } 5$$
 (b) Explain the term Entropy in Information Theory and also prove that Entropy is maximum when all source outputs have equal probability. 10
4. (a) Consider the source probabilities { 0.20, 0.20, 0.15, 0.15, 0.10, 0.10, 0.05, 0.05 } 10
 (i) Determine the efficient fixed length code for the source.
 (ii) Determine Huffman code for this source.
 (iii) Compare the two codes and comment.
 (b) Find parity check matrix and all possible code-words for the following generator matrix- 10

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

5. (a) Explain DES and give outline of algorithm. 10
 (b) Differentiate between Block cipher and Steam cipher. 10
6. (a) A systematic Block code is described with following equations- 10

$$P_1 = m_1 + m_2 + m_4$$

$$P_2 = m_1 + m_3 + m_4$$

$$P_3 = m_1 + m_2 + m_3$$

$$P_4 = m_2 + m_3 + m_4$$
 where m_i — message bits
 P_i — Parity check digits.
- Find generator and parity check matrix for this code.
 - How many errors this code can correct ?
 - Is the vector 10101010 a code-word ?
- (b) Write a short note on digital signature. 10
7. (a) Explain Adaptive Huffman encoding technique. Encode the data pattern " accabbc daad " using above technique. 10
 (b) Explain one-way Hash Function. 10