

(2) Attempt any **four** questions out of remaining **six** questions.

(3) Assume **suitable** data wherever **necessary**.

1. Attempt any **four** :- 20
- (a) Explain 'Digital Signature'.
 - (b) State and explain different classes of complexity.
 - (c) Give Rabin-Miller Test for identifying prime numbers.
 - (d) Explain cyclic codes.
 - (e) Differentiate Block Cyphers from stream Cyphers.
2. (a) Explain RSA Algorithm with suitable example. 10
(b) Explain RLE compression technique. 10
3. (a) Name the source coding techniques used in the following types of files 10
and classify them as lossy or lossless.
(i) .zip (ii) .jpg
(iii) .mpg (iv) .bmp
(v) .gif
- (b) Explain security feature in DES algorithm. 10
4. (a) A systematic block code is described with following equations :- 12
- $$P_1 = m_1 + m_2 + m_4$$
- $$P_2 = m_1 + m_3 + m_4$$
- $$P_3 = m_1 + m_2 + m_3$$
- $$P_4 = m_2 + m_3 + m_4$$
- where $m_i \rightarrow$ message bits
 $p_i \rightarrow$ parity check digits
- (i) Find generator and parity check matrix for this code.
 - (ii) How many errors this code can correct.
 - (iii) Is the vector 10101010 a code vector.
- (b) Compare symmetric and asymmetric key cryptography. 8
5. (a) Explain convolution code in brief. 10
(b) Explain role of Fermat's little theorem and Chinese Remainder theorem 10
in Information Theory.
6. (a) Explain the term Entropy in Information theory and also prove that entropy 10
is maximum when all source outputs have equal probability.
(b) Find Entropy, Redundancy and Information rate of a four symbol source 10
(A, B, C, D) with a rate of 1024 symbols/sec. and symbol selection probabilities
of 0.5, 0.2, 0.2 and 0.1 when the source is memoryless.
7. Write short notes on (any **four**) :- 20
- (a) Properties of Modular Arithmetic
 - (b) One way Hash function
 - (c) Dictionary method of compression
 - (d) Lossy and lossless compression techniques
 - (e) Probable Hacks on cryptography.