[Time: 3 Hours] **[Marks: 80]**

N.B. : (1) Question No.1 is compulsory.
(2) Answer any 3 questions from remaining.
(3) Figures to the right indicate full marks
(4) Assume suitable data if required

Q1. a) Differentiate between Lossy and Lossless compression. 4M
b) Explain Properties of Information. 4M
c) Differentiate Compression Rate from Compression Ratio 4M
d) State and explain Fermat's Little theorem with suitable example. 4M
e) Explain Security attacks with respect to cryptography. 4M

Q 2 a) Explain JPEG Encoder and Decoder in detail (10M)
b) Describe DES in detail. (05M)
c) Define following terms (05M)
1. Code Efficiency
2. Hamming Distance
3. Minimum Distance (d_{min})
4. Hamming Weight
5. Cyclic code

Q.3 a) For (6,3) systematic linear block code, the parity check bits are C4,C5, &C6 are formed from following equation. (10M)
C4=d1+d3
C5=d1+d2+d3
C6=d1+d2
+ indicates ex-or operation
1. Write down generator matrix
2. Construct all possible codewords
3. Find parity check matrix

b) Differentiate between block cipher and stream cipher. (5M)
c) Explain cyclic codes and BCH codes. (5M)

Q 4.a) Explain Convolution code. (05M)
b) Encode the string using LZW Technique. (10M)
bananan an
c) Write short notes on Random number generator. (05M)

Turn Over

Q 5 a)	Explain Diffie –Hellman Algorithm.	(05M)
b)	A discrete source emits one of five symbols once every 1mS ,the symbol probabilities are 1/2, 1/4 ,1/8 ,1/16, & 1/16 respectively Find Source entropy and Information rate	(10M)
c)	Find gcd of (1575,231). by Euclid's Algorithm.	(05M)

Q6. Write short notes (20M)

a. Security Goals
b. Chinese Remainder Theorem
c. Digital Signature
d. Speech Compression
