

Data Compression & Encryption

Q. P. Code: 27401**Time: 3 hours****Marks: 80**

1. Q. 1 is compulsory. Solve any 3 questions from remaining 5.
2. Assume required data where ever necessary with proper justification.

- Q.1 (a) What is the significance of modeling and coding in data compression? (20)
 (b) What are the goals of cryptography? Explain any one in detail.
 (c) List techniques used for lossless image compression.
 (d) Solve the following
 (i) $4^{-1} \bmod 55$
 (ii) $3^{144} \bmod 13$
 (iii) $6^{-1} \bmod 17$
 (iv) Euler's totient function $\Phi(49)$
- Q.2 (a) What is 'frequency' and 'temporal' masking? Explain how it is used and implemented in MP3 audio compression. (10)
 (b) Explain Diffie Hellman Key exchange with the help of an example. (10)
- Q.3 (a) Explain standard JPEG with neat block diagram. What are advantages of JPEG 2000 over standard JPEG? Justify the use of DCT in JPEG? (10)
 (b) Explain RSA in detail and also discuss attacks on RSA. (10)
- Q.4 (a) State following theorems with their applications in cryptography (10)
 (i) Fermat's Theorem (ii) Euler's Theorem (iii) Chinese Remainder Theorem.
 (b) Explain Hash and MAC functions with their role in cryptography. (10)
- Q.5 (a) Consider the probabilities $p(a)=0.2$, $p(b)=0.3$, $p(c)=0.1$, $p(d)=0.4$. Encode and decode the sequence 'abcd' using arithmetic coding technique. (10)
 (b) What is Motion compensation and Motion Estimation in video compression? Explain how they are used in MPEG video compression with appropriate block diagram. (10)
- Q.6 (a) Encode and decode the sequence 'abbacbbabbacc' using LZ78. Compare LZ77 and LZ78. (10)
 (b) Write short notes(Any two) (10)
 (i) μ Law and A Law Companding
 (ii) Fire walls
 (iii) Intruders and viruses
