EXTC/VII/29/05-/19

Paper / Subject Code: 42405 / Elective - I 1)Data Compression & Encryption

Duration: 3 Hours **Marks: 80**

Note:

1) Q.1 is **compulsory**.
2) Attempt any **three** questions from the remaining **five** questions.
3) Assume Suitable data wherever necessary

Q.1 (a) In JPEG compression why DCT is the preferred transform? (20)
(b) State Fermat's theorem and describe its application in cryptography.
(c) Compare image and video compression concepts.
(d) What are 'active 'and 'passive' attacks on security system? List two attacks for each type.

Q.2 (a) Draw and explain the block diagram of JPEG2000 image compression standard. (10)

(b) Explain why RSA works? In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? (10)

Q.3 (a) What is 'frequency' and 'temporal' masking? Explain how it is used and implemented in MP3 audio compression. (10)

(b) Explain Hash function. What characteristics are needed in a secure hash function? (10)

Q.4 (a) Encode and decode the sequence 'abababababaab' using LZW. Initial dictionary (a,b).Compare LZ77 and LZ78. (10)

(b)Describe Diffie-Hellman key exchange protocol and also a man-in-the-middle attack on the protocol. (10)

Q.5 (a) Consider a source with symbols = {m, n, o, p, q} with corresponding probabilities {0.1, 0.1, 0.2, 0.3, 0.3}. Using arithmetic coding, determine the output tag for the message "nqpo". Also, reconstruct the message using this tag. (10)

(b) Draw and explain the working of AES encryption algorithm. (10)

Q.6 (a) Explain μ Law and A Law Companding. How it is used in audio compression? (10)
(b) Write short notes(Any two)
(i) Chinese remainder theorem in cryptography (10)
(ii)Triple DES
(iii) Intruders and viruses
