Paper / Subject Code: 32226 / Department Optional Course-I: Data Compression and Cryptography

1T01035 - T.E.(Electronics and Telecommunication)(SEM-V)(Choice Base Credit Grading System) (R-20-21) (C Scheme) / 32226 - Department Optional Course-I: Data Compression and Cryptography

QP CODE: 10015109   DATE: 02/12/2022

Duration: 3 Hrs   **[Max Marks:80]**

N.B. : (1) Question No 1 is Compulsory.
         (2) Attempt any three questions out of the remaining five.
         (3) All questions carry equal marks.
         (4) Assume suitable data, if required and state it clearly.

1		Attempt any FOUR	[20]
	A	State the advantages of JPEG-2000 over JPEG –LS.	
	B	Explain motion compensation in detail.	
	C	Discuss different types of active and passive attacks.	
	D	Find (i) 2^{16} mod17 (ii) 2^{50} mod17 Using Fermat's little theorem.	
	E	Write different types of biometric authentications methods used for security.	

2 A Consider a source with alphabet A= {a_1, a_2, a_3} with probability P(a_1)=0.6, P(a_2)=0.3, P(a_3)=0.1 respectively. Perform the arithmetic coding operation to generate tag for the sequence $a_2 a_1 a_3 a_1$ and also decipher the tag to get back. [10]

   B Explain in detail about H.264 encoder and decoder. [10]

3 A Explain how DES algorithm is used for data encryption with necessary diagrams. [10]

   B Illustrate Diffie-Hellman key exchange algorithm with suitable example. [10]

4 A Discuss Chinese Remainder Theorem with example. [08]

   B Write short note on A-law and μ-law Companding standards. [12]

5 A How RSA Algorithm is used to secure the data, explain in detail with example. [10]

   B Discuss various types of transposition and substitution cipher with examples. [10]

6 A What do you mean by HASH and MAC functions. Explain with examples. [10]

   B Explain in detail how Intrusion Detection System is used to secure the system. [10]