1T01035 - T.E.(Electronics and Telecommunication)(SEM-V)(Choice Based) (R-19) (C Scheme) / 32226 - Department Optional Course-I: Data Compression and Cryptography
QP CODE: 10030348 DATE: 02/06/2023

Duration: 3hrs **[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.

Q.1		Attempt any FOUR	[20]
	a	Discuss the basic need and advantages of data compression with examples.	[05]
	b	What is motion compression in comparison to image compression?	[05]
	c	What is the difference between Active attack and Passive attack?	[05]
	d	Find the multiplicative inverse of 8 mod 11.	[05]
	e	State Fermat's theorem with their applications in cryptography.	[05]
Q. 2	a	Explain AES in detail with a neat block diagram.	[10]
	b	Explain HASH and MAC functions with their role in cryptography.	[10]
Q. 3	a	Encrypt the plain text 63 using the RSA algorithm which uses prime numbers p=7 and q=11. The public key e=13. Verify that the decrypted text is same as the plain text.	[10]
	b	Define Key management. Explain Diffie Hellman Key exchange algorithm with an example.	[10]
Q. 4	a	What is firewall and how they can be designed for effective security?	[10]
	b	Write a short note on JPEG-2000.	[10]
Q. 5	a	Explain Intrusion Detection System in detail.	[10]
	b	Explain caesar cipher and multiplicative cipher with suitable example and diagram.	[10]
Q. 6	a	Explain μ Law and A Law companding.	[10]
	b	Determine the Lampel Ziv code for the following bit stream 111010011000010110100. Recover the original sequence from the encoded stream.	[10]

****

46D32496D8CA1AA695506C8B49380230