22/11/2024 EXTC SEM-V C SCHEME DLOC-DCC QP CODE: 10066368

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	Compare lossy and lossless data compression techniques with examples.	[05]
	b	Define H.264 encoder and decoder video standard with suitable diagrams.	[05]
	c	Differentiate between Active attack and Passive attack?	[05]
	d	Solve the following: (any 02) 1. 4^{-1} mod 55 2. 3^{144} mod 13 3. 6^{-1} mod 17 4. Euler's totient function Φ (49)	[05]
	e	State Fermat's Little Theorem, Euler's Theorem, Totient function used in modular arithmetic.	[05]
Q. 2	a	Explain the concept of key generation using DES with a neat block diagram.	[10]
	b	Define message integrity? Explain HMAC algorithm with an example.	[10]
Q. 3	a	Explain the RSA encryption- decryption algorithm. Specifically explain why the decrypted message is the same as the plain text.	[10]
	b	How authentication can be provided for securing an Electronic Payment System?	[10]
Q. 4	a	Alice chooses her private key of x=3 and Bob chooses y=6. If both the parties used the primitive root g=7 for prime p=23, explain the key exchanged between Alice and Bob using Diffie Hellman key exchange method?	[10]
	b	Explain the principles of Public Key Cryptography using message integrity and message authentication.	[10]
Q. 5	a	Explain Intrusion Detection System in detail.	[10]
	b	Explain caesar cipher and multiplicative cipher with suitable examples and diagrams.	[10]
Q. 6	a	Define audio compression and explain μ Law and A Law companding.	[10]
	b	Take an alphabet string and code it using LZ78. What are the limitations of LZ78 and how can they be overcome with LZW.	[10]