E- comp - sem VI - R-19- C- Scheme

16.05.25

Duration: 3 hours **[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	Describe different attacks in system security.	5
	b	Find gcd of 270 and 192 using the Euclidean algorithm.	5
	c	List the benefits of MAC over message digest. compare HMAC and CMAC.	5
	d	What is the purpose of S-boxes in DES? Explain the avalanche effect.	5
	e	Explain buffer overflow attack.	5
2	a	Explain man in middle attack on Diffie Hellman. Explain how to overcome the same.	[10]
	b	Explain AES algorithm. Discuss the parameters which make AES better than DES.	[10]
3	a	What is DDOS Attack and how it is launched?	[10]
	b	How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP.	[10]
4	a	Encrypt and decrypt the message "ENEMY ATTACKS TONIGHT" with a keyed columnar transposition cipher with encryption key 25134 and decryption key 31452.	[10]
	b	Use the Play fair cipher with the key "CRYPTOGRAPHY" to encrypt the message "INSPIRE HUMAN"	[10]
5	a	In the RSA system the public key (E,N) of user A is defined as (7,33). Implement RSA digital signature algorithm to find the private keys of user A. User A wishes to send the message 'C' to user B . Examine the message signing and verification process using RSA digital signature algorithm.	[10]
	b	Explain different types of firewalls.	[10]
6	a	Differentiate between DES & AES algorithms with respect to various operations.	[10]
	b	Draw and describe X.509 digital Certificate format.	[10]

QP code
82196

Prog code
1T00736