M.Tech. Computer Science & Engineering (CBCS Pattern) Sem-II

PCSS243/PCSS24C - Elective-II : Network Security & Cryptography

P. Pages : 1 **GUG/W/22/10998**

Time : Three Hours * 1 7 9 1 * Max. Marks : 70

Notes : 1. Attempt **any five** question.

1.	a)	Explain OSI security architecture?	**7**
	b)	What is multiple encryption? Explain what is triple DES?	**7**
2.	a)	Explain steganography?	**7**
	b)	What are block cipher design principles and modes of operations? Explain.	**7**
3.	a)	In a public key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?	**7**
	b)	Explain DES algorithm?	**7**
4.	a)	Discuss digital signatures and its standards?	**7**
	b)	Discuss Diffie-Hellman key exchange?	**7**
5.	a)	Explain public-key cryptosystem?	**7**
	b)	Discuss in detail the architecture and authentication about IP security?	**7**
6.	a)	Explain message authentication code?	**7**
	b)	Explain secure sockets layer?	**7**
7.	a)	Illustrate SHA algorithm. in detail? What basic arithmetic and logic functions are used in SHA?	**7**
	b)	Explain X. 509 authentication service?	**7**
8.	a)	Explain IPSec authentication header?	**7**
	b)	Explain cryptographic computation?	**7**

****