Computer Science & Engineering (CBS and CBCS Pattern)
M.Tech. Second Semester Old+CBCS (C.B.S. Pattern)

PCSS243 - Elective-II : Network Security & Cryptography

P. Pages : 1 **GUG/W/18/10998**

Time : Three Hours * 3 1 2 2 * Max. Marks : 70

Notes : 1. All questions carry equal marks.
2. Answer **any five** questions.

1.	a)	What are the different uses of public key cryptography related to key distribution.	**8**
	b)	What is OSI security architecture.	**6**
2.	a)	Write Diffie-Hellman key exchange algorithm.	**7**
	b)	Discuss in detail the architecture and authentication about IP security.	**7**
3.	a)	List and define the parameters that define an SSL session state.	**6**
	b)	What are the principle elements of the public key crypto system.	**8**
4.	a)	Write a note on RIPEMD - 160.	**8**
	b)	Why is R.64 conversion useful for an e-mail application.	**6**
5.	a)	Describe Euler's and Chinese Reminder theorem.	**7**
	b)	What are the characteristics needed in a secure hash function.	**7**
6.	a)	What is the difference between weak and strong Collis ion resistance.	**7**
	b)	Discuss in detail C-MAC Algorithm.	**7**
7.	a)	What is the difference between differential and linear cryptanalysis.	**7**
	b)	What are the approaches for producing manage Authentication.	**7**
8.	a)	List three general approaches to dealing with replay attacks.	**7**
	b)	What is Message digest algo.	**7**

****