B. Tech Degree VII Semester (Supplementary) Examination July 2010

IT 705 (D) CRYPTOGRAPHY AND DATA SECURITY

(2002 Scheme)

Time : 3 Hours Maximum Marks : 100

I.	a.	Explain various aspects of security.	(10)
	b.	With suitable examples, distinguish between transposition cipher system and substitution cipher system.	(10)
		OR	
II.	a.	Explain the working of Hagelin machine.	(12)
	b.	Write a note on unicity distance.	(8)
III.	a.	Briefly explain DES algorithm.	(12)
	b.	Explain different modes of DES.	(8)
		OR	
IV.	a.	Explain IDEA.	(10)
	b.	Distinguish between linear shift registers and non linear shift registers.	(10)
V.	a.	Explain RSA system in detail.	(12)
	b.	Write a short note on Knapsack system.	(8)
		OR	
VI.		Discuss public key systems based on elliptic curves with suitable examples.	(20)
VII.	a.	Briefly explain Authentication protocols.	(10)
	b.	Explain how message integrity can be achieved with the help of Hash functions.	(10)
		OR	
VIII.	a.	What is meant by digital signature? Explain how it is used in message authentication.	(10)
	b.	Discuss zero knowledge techniques.	(10)
IX.	a.	Explain the general aspects of key management.	(10)
	b.	Describe briefly asymmetric key distribution system.	(10)
		OR	
X.		Write notes on:	
		(a) Network Security	
		(b) Fair crypto system.	(2 x 10 =20)

***