BTS(C) – VII– 09 – 061 – D

B. Tech Degree VII Semester Examination, November 2009

IT 705 (D) CRYPTOGRAPHY AND DATA SECURITY

(2002 Scheme)

Time: 3 Hours Maximum Marks: 100

I.	a.	Explain different aspects of security.	(10)
	b.	Distinguish between transposition ciphers and substitution ciphers.	(10)
		OR	
II.	a.	Explain the working of Hagelin machine.	(12)
	b.	Write a short note on unicity distance.	(8)
III.		Explain DES algorithm in detail? Mention the characteristics of DES.	(20)
		OR	
IV.	a.	Explain IDEA.	(10)
	b.	Explain the use of Linear Feedback Shift Registers in Cryptography.	(10)
V.		Discuss in detail, RSA algorithm.	(20)
		OR	
VI.		Explain various public key system based on elliptic curves.	(20)
VII.	a.	Explain different cryptographic protocols.	(10)
	b.	Explain how message integrity is achieved with the aid of Hash function.	(10)
		OR	
VIII.	a.	Discuss in detail, message authentication with digital signatures.	(10)
	b.	Explain Zero knowledge techniques.	(10)
IX.	a.	Explain general aspects of key management.	(10)
	b.	Explain key distribution for asymmetrical systems.	(10)
		OR	
X.	a.	What does Network Security means? What are the ways to employ Network Security?	(10)
	b.	Write a note on Fair Cryptosystems.	(10)

***