BTS(C) – VII– 09 – 61 – AA

B. Tech Degree VII Semester Examination, November 2009

IT 705 (C) CRYPTOGRAPHY AND DATA SECURITY

(1999 Scheme)

Time: 3 Hours Maximum Marks: 100

I.	a.	Explain the working of Hagelin Machine.	(10)
	b.	Explain the following terms (i) Transposition Ciphers (ii) Substitution Ciphers	(5 x 2=10)
		OR	
II.		Explain the following concepts: (i) Aspects of security (ii) Cryptanalytic attacks.	(10 x 2=20)
III.		Explain the DES algorithm.	(20)
		OR	
IV.	a.	Distinguish between stream and block ciphers.	(10)
	b.	Discuss the application of finite state machines in cryptography.	(10)
V.		Explain the RSA algorithm.	(20)
		OR	
VI.	a.	Explain the public key system based on elliptic curves.	(10)
	b.	Explain the Knapsack system.	(10)
VII.		Explain the following terms (i) Zero knowledge techniques (ii) Hash functions.	(10 x 2=20)
		OR	
VIII.	a.	Explain Digital Signature algorithm.	(15)
	b.	Write short notes on message authentication.	(5)
IX.	a.	Discuss the various aspects of key management.	(10)
	b.	Write notes on Network Security.	(10)
		OR	
X.	a.	Explain the concept of key distribution in asymmetrical systems.	(10)
	b.	Write notes on Fair Cryptosystems.	(10)

***