B. Tech Degree VII Semester (Supplementary) Examination June 2006

IT 705 (D) CRYPTOGRAPHY AND DATA SECURITY

(2002 Admissions onwards)

Time : 3 Hours Maximum Marks : 100

I.	(a)	Define cryptography, cryptology and cryptanalysis.	(10)
	(b)	Explain with the help of a neat diagram, Heugline cryptograph?	(10)
		OR	
II.	(a)	Explain the various classical cipher systems.	(10)
	(b)	Discuss the various types of cryptanalytic attacks.	(10)
III.		How encryption and decryption is performed using DES algorithm? Mention the different makes of DES.	(20)
		OR	
IV.		Write short notes on ***any two*** : (i) LFSR (ii) Finite state machine (iii) Stream and block enciphering.	(20)
V.		Bring out the concept of RSA algorithm. Mention its features, merits and demerits.	(20)
		OR	
VI.		Discuss the various public key systems based on elliptic curves.	(20)
VII.	(a)	Explain message integrity with the aid of hash functions.	(10)
	(b)	Explain MDS.	(10)
		OR	
VIII.	(a)	Explain zero knowledge technique.	(10)
	(b)	How message authentication is achieved with digital signature?	(10)
IX.		Write short notes on ***any four*** : (i) Diffe – Halman key exchange system (ii) Fair cryptosystem (iii) Network security (iv) Key distribution for asymmetric systems (v) The knapsack system.	(5 x 4 = 20)

***