B.Tech Degree VII Semester Examination December 2002

IT 705(C) CRYPTOGRAPHY AND DATA SECURITY

(1999 Admissions)

Time: 3 Hours Maximum Marks: 100

I.	(a)	Explain in detail, the different encryption methods.	(12)
	(b)	Explain, how secure is DES today.	(8)

OR

II.		Explain the working of Hagelin Machine.	(20)
III.		Explain International Data Encryption Algorithm.	(20)

OR

IV.		Explain the usage of Linear Feedback Shift Registers in Cryptography.	(20)
V.		Demonstrate how an NP-complete problem can be used for public-key cryptography.	(20)

OR

VI.		Describe in detail, the RSA Algorithm.	(20)
VII.		Explain different Cryptographic protocols.	(20)

OR

VIII.		Explain elliptic curve cryptography.	(20)
IX.		Discuss approaches to Public-key management.	(20)

OR

X.		Explain key distribution for symmetrical and asymmetrical systems.	(20)

***