B. Tech Degree VII Semester Examination
November 2005

IT 705 (D)   CRYPTOGRAPHY AND DATA SECURITY
(2002 Admissions onwards)

Time : 3 Hours   Maximum Marks : 100

1.	(a)	Distinguish Cryptography and Coding Theory.	10
	(b)	Explain the following terms in cryptography:	
		(i) Visual Cryptography (ii) Steganography	10

OR

2.	(a)	Explain the working of Hagelin Machine.	10
	(b)	Explain in detail, any probabilistic encryption method.	10
3.	(a)	What is secret sharing? Explain with an example.	08
	(b)	Explain in detail, the DES encryption.	12

OR

4.	(a)	Explain in detail, any stream cipher. Also explain the uses of stream ciphers.	10
	(b)	Explain International Data Encryption Algorithm.	10
5.	(a)	Explain in detail, the most common purposes for which public key cryptography has been applied.	12
	(b)	Is there anything harm in decrypting arbitrary cipher text (encrypted using RSA Algorithm) presented by an adversary? Explain.	08

OR

6.	(a)	Explain the role of the class NP hard problems in cryptography.	10
	(b)	Discuss the public key systems based on elliptic curves.	10
7.	(a)	Explain different cryptographic protocols.	10
	(b)	Discuss the applications of Zero-knowledge proof techniques.	10

OR

8.	(a)	Explain the massage integrity with the aid of Hash functions.	10
	(b)	Explain what do you mean by bit commitment.	10
9.	(a)	Explain the general aspects of key management.	10
	(b)	Explain the criteria for a cryptosystem to be practical.	10

OR

10.	(a)	What does network security mean? What are the ways to employ Network security?	10
	(b)	Explain the Diffie-Halman key exchange system.	10