BTS (C) – VII – (S) – 09 – 038 – D

B.Tech. Degree VII Semester (Supplementary) Examination, July 2009

IT 705 (D) CRYPTOGRAPHY AND DATA SECURITY

(2002 Scheme)

Time: 3 Hours Maximum Marks: 100

I a) Distinguish between cryptography and crypt analysis. Explain the aspects of security in cryptography. (10)

b) Explain transposition ciphers and substitution ciphers with examples. (10)

OR

II a) Explain the general scheme of a cipher system. (8)

b) Explain the working of Hagelin machine. (12)

III a) Discuss the characteristics of DES. (10)

b) Explain the modes of DES. (10)

OR

IV a) Explain in Detail the DES encryption. (10)

b) Differentiate stream and block enciphering. (10)

V Describe the RSA public key system. (20)

OR

VI Discuss the public key systems based on elliptic curves. (20)

VII a) Explain the different cryptographic protocols. (10)

b) Explain message integrity with the aid of hash functions. (10)

OR

VIII a) Explain message authentication with MAC. (10)

b) Give a brief discussion on DSA algorithm. (10)

IX a) Explain the general aspects of key management. (10)

b) Discuss the methods to employ network security. (10)

OR

X a) Distinguish online and offline key distribution systems. (10)

b) What is a cryptosystem? Explain fair Diffie – Hellmann crypto system. (10)

****