BTS(C) – VII – 06 –048 (Z)

B.Tech. Degree VII Semester Examination, November 2006

IT 705 (C) CRYPTOGRAPHY AND DATA SECURITY

(Prior to 2002 Admissions)

Time: 3 Hours Maximum Marks: 100

I a) Define cryptography and cryptanalysis. (5)

b) Explain the terms:

(i) Interception (ii) Fabrication

(iii) Non repudiation (15)

OR

II With the help of neat diagram, explain the Hagline cryptograph. (20)

III Explain the DES algorithm. List the merits and demerits of it. (20)

OR

IV Explain IDEA. Compare it with DES. Which algorithm is more secure? Why? (20)

V Explain the different approaches to attacking the RSA algorithm. (20)

OR

VI Describe the various public key systems using elliptical curves. (20)

VII Explain the message authentication with digital signatures. (20)

OR

VIII a) Explain the different knowledge techniques. (10)

b) How can we achieve message integrity with hash codes. (10)

IX Explain the various approaches to public key management. (20)

OR

X a) What do you mean by network security? How it is achieved? (10)

b) Explain the key distribution for symmetric algorithms. (10)

***