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

## IT 705 (C) CRYPTOGRAPHY AND DATA SECURITY

*(Prior to 2002 Admissions)*

Time : 3 Hours Maximum Marks : 100

| | | | |
|---|---|---|---|
| I. | (a) | Explain how cryptography differs from coding theory. | (10) |
| | (b) | Suppose that an Affine Cipher uses the encryption function $C \equiv 11.P + 3 \pmod{26}$. Find the decryption function, $P = \alpha C + \beta$. What is the maximum number of keys possible here? | (10) |
| | | **OR** | |
| II. | (a) | Explain the following terms with respect to cryptography : (i) Practical security (ii) Provable security (iii) Absolute security. | (9) |
| | (b) | Give an example of seven words in English language each of length 5, and they differ one another only in the first letter. | (4) |
| | (c) | Briefly explain the working of Hageline Machine. | (7) |
| III. | (a) | Explain International Data Encryption Algorithm. | (10) |
| | (b) | Explain the usage of Linear Feedback Shift Registers in Cryptography. | (10) |
| | | **OR** | |
| IV. | (a) | Discuss on "DES has begun to show signs of age". | (10) |
| | (b) | Explain the role of finite state machine in cryptography. | (10) |
| V. | (a) | Describe in detail Massey -- Omura cryptosystem. | (8) |
| | (b) | Describe in detail, the RSA Algorithm with an example. | (7) |
| | (c) | Explain how to choose the values p, q, e and d in RSA algorithm. | (5) |
| | | **OR** | |
| VI. | (a) | A point P on the elliptic curve is said to be of order r, if r is the smallest +ve integer such that $rP = O$. Prove that the order of the point $P = (2, 3)$ on $y^2 \equiv x^3 + 1$ is 6. | (8) |
| | (b) | Explain any key exchange algorithm based on factorization algorithm. | (8) |
| | (c) | Explain discrete logarithm problem. | (4) |
| VII. | (a) | Explain different cryptographic protocols. | (8) |
| | (b) | Explain the role of Hash function in cryptography. Give *any two* Hash functions. | (12) |
| | | **OR** | |
| VIII. | (a) | Describe in detail, message authentication with digital signatures. | (10) |
| | (b) | Explain how can Zero-knowledge technique be used for password verification. | (10) |
| IX. | (a) | What does Network security mean? | (8) |
| | (b) | Explain the general aspects of key management and key distribution and key exchange. | (12) |
| | | **OR** | |
| X. | (a) | Discuss in detail key agreement protocols. | (10) |
| | (b) | What are the ways to employ Network security? | (10) |

***