D 42578 (Pages : 2) Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION DECEMBER 2007

CS 04 702/IT 04 702—CRYPTOGRAPHY AND NETWORK SECURITY

(2004 Admissions)

Time : Three Hours Maximum : 100 Marks

Part A

Answer **all** *questions.*

I. 1 State Fermat's theorem and Wilson's theorem.

2 Discuss about steganography.

3 Explain RSA algorithm with an example.

4 Write a short note on MAC and hash functions.

5 Discuss about quantum crystography.

6 Give the features of undeniable digital signatures.

7 Draw the working model of Kerberos and explain.

8 Discuss about PEM and PGP.

(8 × 5 = 40 marks)

Part B

Answer **one** *question from each unit.*

UNIT I

II. 1 Explain the triple DES algorithm for eneryption and give its features.

Or

2 (a) Discuss about the various security attacks and security services. (7 marks)

(b) Give the role of random number generation in cryptography. (8 marks)

UNIT II

III. 1 Discuss about elliptic curve cryptography and the various implementation issues in public key cryptography.

Or

2 Explain SHA-1 algorithm and compare with MD5.

UNIT III

IV. 1 Explain GOST digital signature algorithm and give the advantages.

Or

2 Explain any *one* key distribution algorithm and give its advantages.

Turn over

UNIT IV

V. 1 Discuss about IP security in detail.

Or

2 Discuss about web security in detail.

(4 × 15 = 60 marks)