D 11253

Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION DECEMBER 2005

IT 2K 703—CRYPTOGRAPHY AND NET-WORK SECURITY

Time : Three Hours

Maximum : 100 Marks

Part A

1. Prove the general case of Chinese remainder theorem.
2. Explain the linear and Second degree Diophantine equations with examples.
3. Tabulate the types of attacks on encrypted messages.
4. What is covert channel ? Explain link and end-to-end encryption approach.
5. Compare conventional and public key Encryption.
6. Differentiate version 4 and version 5 of Kerberos.
7. What are the functions provided by S/MIME ?
8. Explain ESP format and its fields briefly.

(8 × 5 = 40 marks)

Part B

1. State and prove Fermat's and Euler's theorems.

Or

2. Prove the Wilson's theorem with examples.
3. What are the Substitution techniques ? Explain them briefly.

Or

4. Describe the placement of encryption function.
5. Explain the RSA algorithm with examples.

Or

6. What are the general areas focussed on authentication protocols ? Explain each one in detail.
7. Describe the keymanagement of IP Sec.

Or

8. Explain the design principles of Firewall.

(4 × 15 = 60 marks)