D 26542

Name..

Reg. No...

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, DECEMBER 2006

IT 2K 703—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 100 Marks

Answer **all** *questions.*

I. 1 Explain Chinese remainder theorem and its significance.

2 Explain what is congruence and its properties.

3 Compare DES, AES, IDEA & Blowfish algorithms in terms of Data size, Key size, Number of rounds. Security Level.

4 Write notes on traffic confidentiality.

5 What is the importance of Key management and sharing ? Explain the problems involved in key sharing.

6 From the concepts of public key and private key, explain how message authentication is achieved.

7 Compare System Level and Network level security issues. What is a virus ?

8 Explain the various protocols used in E-mail security.

(8 × 5 = 40 marks)

II. (a) State and explain :

(i) Euler function. (7 marks)

(ii) Fermat's theorem. (8 marks)

Or

(b) (i) Explain the use of mathematics in Cryptography. (5 marks)

(ii) Explain Wilson's theorem and its applications. (10 marks)

III. (a) Explain *any* one classical encryption algorithm and its cryptanalysis process. With example, explain the process of substitution and diffusion.

Or

(b) Explain the algorithm of DES. Comment on the security level of 'S' boxes.

IV. (a) Explain RSA algorithm with example. What is the advantage and disadvantage of this method ?

Or

(b) Explain the algorithm of MD5. What is its significance ?

V. (a) Write notes on IP layer security. Explain the header of IP protocol. What is S/MIME ?

(4 + 4 + 7 = 15 marks)

Or

(b) What is a firewall ? Explain the Design and Breaking of firewalls.

[4 × 15 = 60 marks]