l No. □□□□□□□□□□

No. of Printed Pages—3 **CS-023 / IT-701**

B. TECH.

SEVENTH SEMESTER EXAMINATION, 2003-2004

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note : (1) Attempt **ALL** questions.

(2) Choices are given in each question set.

1. Attempt any *FOUR* of the following questions :— **(5×4=20)**

(a) Explain Feistel Encryption and Decryption Algorithm. What is the difference between Diffusion and Confusion ?

(b) What is triple DES ? Explain the term meet-in-the-middle attack.

(c) What is a Key Distribution Center ? List the ways in which secret keys can be distributed to two communicating partners. Differentiate between Session key and Master key.

(d) What is a Transposition Cipher ? Illustrate an example. What is Steganography ?

(e) What is the difference between a Block cipher and a Stream cipher ? Explain the term, one-time pad.

(f) Explain random number generation techniques.

2. Attempt any *FOUR* of the following questions :— **(5×4=20)**

(a) Briefly define a Group, Ring and Field.

(b) Determine gcd (1970, 1066).

41

(c) Explain Fermat's theorem. What is Euler's totient ?

(d) Find all primitive roots of 25.

(e) Perform encryption and decryption, using RSA algorithm for P=3; q=11, e=7; M=5.

(f) Explain Diffie-Hellman key exchange algorithm. What is an elliptic curve ?

3. Attempt any *TWO* of the following questions :— **(10×2=20)**

(a) What is a message authentication code ? What characteristics are needed in a secure hash function ?

(b) What is the difference between Direct and Arbitrated digital signatures ? Explain Digital Signature Algorithm.

(c) What basic arithmetical and logical functions are used in MD 5 ? Explain SHA-1 logic. Give comparison of SHA-1 and MD 5.

4. Attempt any *TWO* of the following :— **(10×2=20)**

(a) What is PGP ? How different is it from X.509 ? Give Services provided by PGP and their brief description. Why are the segmentation and reassembly functions in PGP needed ? How does PGP use the concept of trust ?

(b) What is S/MIME ? Why is it used ? What are the main functions S/MIME provides ?

(c) Explain full-service Kerberos environment. What are the principal differences between version 4 and version 5 of Kerberos ?

Attempt any *TWO* of the following :— (10×2=20)

(a) What are the services IPSec provides ? Explain Oakley key determination protocol.

(b) What is SSL and SET ? What is the difference between SSL connection and SSL session ? Discuss SSL protocol architecture. How does SET work ? Describe dual signature for SET and its purpose.

(c) *(i)* What are the types of Firewall ? Explain them.

(ii) What do you understand by Trusted Systems ? Explain the concept of reference monitor.