Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Tech(CSE)/SEM-3/MCS-302D/2009-10

2009

CRYPTOGRAPHY AND COMPUTER SECURITY

Time Allotted : 3 Hours Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer question no. 1 and any *four* from the rest.

1. Answer any *seven* questions : 7 × 2 = 14

   a) State the use of S-Box in the context of encryption technology.

   b) What is the purpose of using Linear Key Stream Generator ?

   c) Find all elements belong to Quadratic-Residue mod 7.

   d) Find the inverse of 35 in Z_{18} using Euclidean algorithm.

   e) "HTTP is stateless." Justify the statement.

   f) What is VPN ?

   g) What do you mean by Cryptanalysis ?

   h) Mention four principles of security.

2. a) Distinguish between Steam Cipher and Block Cipher.

   b) What do you mean by Public Key Algorithm ?

   c) What are the advantages and disadvantages of Asymmetric key cryptography over symmetric key cryptography ?

   d) Write the basic principles of Digital Signatures Method.

   4 + 2 (2 + 2) + 4

3. a) Discuss the structure of Feistel Cipher.

   b) Describe the model of Triple DES.

   c) How do you encrypt a plaintext using El-Gamal cryptosystem ? 5 + 6 + 3

4. a) What do you mean by "Modes of Operations" ?

   b) Why Cipher Block chaining is better than Electronic Code Block ?

   c) Define Finite Field. Find all irreducible polynomial of degree four in $Z_2 [x]$. 4 + 4 (2 + 4)

5. a) Describe Miller-Rabin Primality Testing Algorithm.

   b) Explain "Point additional in a Elliptic Curve".

   c) "(E,*) form an abelian group, where E is a non-singular Elliptic curve and * is a binary operation which adds points on the Elliptic Curve". — Justify. 4 + 5 + 5

6. a) What do you mean by Bi-directional Authentication ?

   b) Describe algorithms of Diffie-Hellman key exchange algorithms. Explain mathematical theory behind the algorithm. 3 + 6 + 5

7. a) What are the differences between Authentication and Authorization ?

   b) What is the function of Key Distribution Center (KDC) ?

   c) Explain the authentication protocol Kerberos. 3 + 3 + 8

8. a) What is position of SSL in TCP/IP protocol suite ? How SSL works ?

   b) Explain the operation of Application Gateway Firewall and Packet Filtering Firewall.

   c) Suppose plain text is : "Netaji Subhash Engineering College". What will be the cipher text in Rail fence technique ? 2 + 6 + 4 + 2