Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Tech (CSE)/SEM-3/MCS-302D/2010-11

2010-11

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* of the following : 7 × 2 = 14

   i) "Monte-Carlo Algorithm is called a decision-based algorithm." Justify

   ii) State the advantages of Triple DES over double DES.

   iii) Find the additive inverse of m in Z_n, where m and n are both positive integers.

   iv) Find the g.c.d. of 220 and 85 using Euclidean algorithm.

   v) What do you mean by Cryptanalysis ?

vi) What is position of SSL in TCP/IP protocol suite ?

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

viii) What are the differences between Authentication and Authorization ?

2. a) Write an algorithm of Fermat Factorization Method.

b) Find the complexity of Pollard-Rho Factorization method.

c) Compute x^y, where y = 1, 2, ..., 10 in $Z_2[x]/(x^3+x+1)$. 5 + 4 + 5

3. a) Illustrate the method of generating a key-stream using Linear Feedback Shift Registrar (LFSR).

b) Show all steps to evaluate Jacobi symbol. Evaluate the Jacobi symbol $\left(\frac{7411}{9283}\right)$. 6 + (4 + 4)

4. a) What do you mean by Digital Signature Standard ? Describe the architecture of DSS.

b) Implement Elliptic Curve Digital Signature Scheme. 7 + 7

5. a) How do you encrypt and decrypt a plain text using RSA Algorithm ?

   b) Let x = 9501 be a plain text. Use RSA method to convert x to a Cipher text. Again recover the same plain text. (Given that p = 101, q = 113, b = 3533 where p, q be two prime numbers and b has its usual meaning).

   c) Describe Solovay-Strassen Primality Testing Algorithm. 5 + 4 + 5

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

   b) Why is Cipher block chaining better than Electronic code block ?

   c) Explain the operation of application gateway firewall and packet filtering firewall.

   d) Suppose plain text is : "West Bengal University of Technology". What will be the Cipher text in Rail fence technique. 4 + 4 + 4 + 2

7. a) Explain the authentication protocol Kerberos.

   b) What is the function of key distribution centre (KDC) ?

   c) What are the advantages and disadvantages of Asymmetric Key Cryptography over Symmetric Key Cryptography ? 8 + 3 + 3

8. 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