Roll No.									

B.E./B.TECH. (FULL TIME) DEGREE EXAMINATIONS, NOV.2011

Branch : B.Tech. (Information Technology) Semester : VII (All Batches)

IT 9402 – Cryptography and Security

Time : 3 hours Max. Marks : 100

Answer All questions

Part – A (10 x 2 = 20 Marks)

1. Using the Extended Euclidean algorithm, find the greatest common divisor for the numbers 161 and 56.
2. Define Fields and Galois Field.
3. What is triple DES? State its uses.
4. Compare Fermat's test with square root test for primality testing.
5. What are birth day attacks?
6. Using Elgamal Cryptosystem, compute the Cipher text for the Plain text 7 with $p = 11$, $e_1 = 2$, $d = 3$ and $r = 4$.
7. Explain the recovation of X.509 certificates?
8. How is authentication carried out with Key Distribution Centres?
9. State the reasons for enforcing user authentication in operating systems.
10. List the requirements for database security.

Part – B (5 x 16 = 80 Marks)

11. (i) Write the Chinese Remainder theorem. Using this theorem, find the solution to the simultaneous congruences.
$X \equiv 1 \pmod{11}$, $X \equiv -1 \pmod{13}$ and $X \equiv 1 \pmod{17}$ (5)

(ii) Using the formula used in Affine Cipher the plain text word "if" has been translated into "PQ" in Cipher text. Find the values of α and β. Using α and β, find the Cipher text corresponding to the plain text "me". (6)

(iii) Explain the playfair cipher using a suitable example. (5)

12. (a) (i) Write the steps involved the simple DES algorithms. Explain it using the following boxes, the 8-bit plain text 1011 1101 and the 10-bit key 1010000010. (8)

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

IP							
2	6	3	1	4	8	5	7

IP – 1							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

(ii) Explain the AES algorithm in Detail. (8)

(OR)

(b) (i) Write the RSA algorithm. Using this algorithm find the cipher text for the plain text 88 using p = 5, q = 11 and e = 7. (8)

(ii) List the modes of operation used in symmetric key algorithm and explain them. (8)

13. (a) (i) Define Group, Finite Multiplicative group, order of an element of a group, cyclic group and Discrete logarithm. Find the value of x in the following cases.

(A1) $4 \equiv 3^x \pmod 7$

(A2) $6 \equiv 5^x \pmod 7$ (8)

(ii) Explain the Diffie Hellman Key exchange procedure. How is it used in Elliptic key Cryptography? (8)

(OR)

(b) (i) Explain the SHA-1 algorithm in detail. (8)

(ii) Write the Digital Signature Algorithm (DSA). Using this algorithm and with p = 11, q = 5, $\alpha = 3$ and $\kappa = 3$, show that

$(\alpha^\kappa \pmod p) \pmod q \neq (\alpha^\kappa \pmod q) \bmod p$ (8)

14. (a) (i) Explain the Kerberos user Authentication Protocol. (8)

(ii) Explain the "Pretty Good Privacy" protocol. (8)

(OR)

(b) (i) Explain IP Security in detail. (8)

(ii) What is secured Socket Layer? Explain it in detail. (8)

15. (a) (i) Explain the Bell-La Padula confidentiality model for OS security. (8)

(ii) List the components of a Trusted operating system. Explain them in detail. (8)

(OR)

(b) (i) What is access control? How is it useful in database security. (4)

(ii) List the attacks on databases and explain them. (4)

(iii) How will you provide multi-level database security? Explain the design of Databases with Trust Database Manager and trusted front end. (8)