Reg. No. [ ]

B.E./B.Tech.(Full Time) DEGREE END SEMESTER EXAMINATIONS, NOV/DEC 2011
COMPUTER SCIENCE & ENGINEERING BRANCH
SEVENTH SEMESTER
CS9402 – CRYPTOGRAPHY AND SECURITY
(REGULATION 2008)

56

Time: Three Hours **Max.Marks: 100**

PART A (10 x 2 = 20 Marks)
Answer All Questions.

1. Suppose we work with mod 27 instead of mod 26 for affine ciphers. How many keys are possible?
2. Suppose we build an LFSR machine that works for mod 3 instead of mod 2. It uses a recurrence of length 2 of the form
   $X_{n+2} \equiv C_0 X_n + C_1 X_{n+1} \pmod 3$
   To generate the sequence 1,1,0,2,2,0,1,1. Set up and solve the matrix equation to find the coefficient C_0 and C_1.
3. What are the two methods for frustrating statistical cryptanalysis?
4. Give the differences between conventional and public key encryption techniques.
5. What are the requirements for the use of public key certificate scheme?
6. Suggest some situation in which a message authentication code is used?
7. What problem was Kerberos designed to address?
8. What are the different phases a virus goes through its lifetime?
9. List the key features of a trusted operating system.
10. What are the factors to be considered while determining the sensitive data?

PART – B (5 x 16 = 80 Marks)

11 (i) In an RSA system, the public key of a given user is e = 19, n = 2257. What is the private key of this user? (6)
(ii) Describe a man-in-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates one public-private key for the attack. (10)

12 a.(i) A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over, and if they line up five to a row, three people are left over. What is the smallest possible number of people? What is the next smallest number? (Hint: Interpret this problem in terms of the Chinese remainder theorem.) (8)

(ii) State and prove Euler's theorem. (8)

(OR)

b. (i) Suppose you have a language with only the 3 letters "x, y and z," and they occur with frequencies 0.7, 0.2 and 0.1 respectively. The ciphertext was encrypted by the Vigenere method (shifts are mod 3 instead of mod 26, of course) :

XYZYXYYYXZ.

Show that the key length is probably 2, and determine the most probable key. (8)

(ii) Use the Legendre symbol to determine whether a solution exists for (8)

$X^2 \equiv 123 \pmod{401}$

13 a.(i)Show how the byte 14 is transformed to FA by subbyte routine and transformed back to 14 by the invsubbyte routine in AES algorithm. (8)

(ii)How meet-in-middle attack is performed on triple DES? (8)

(OR)

b.(i) In DSS algorithm, prove ((H(M) + xr)w) mod q =k. (8)

(ii) Discuss briefly about any one of the hash algorithms. (8)

14. a. What are the five principal services provided by PGP? Discuss in detail about the PGP technique used for E-mail security.

(OR)

b. Discuss briefly about IP security architecture.

15. a. Discuss in detail the security models involved in trusted operating systems.

(OR)

b. Discuss in detail about the multilevel secure database.