Roll No. | | | | | | | | |

B.E / B.Tech (Full Time) DEGREE END SEMESTER EXAMINATIONS, April / May 2014

Computer Science and Engineering

VII Semester

CS9402 Cryptography and Security

(Regulation 2008)

Time : 3 Hours | Answer ALL Questions | Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. Suppose we work mod 27 instead of mod 26 for affine ciphers. How many keys are possible?
2. Determine $\varphi(231)$. (Eulers Totient function)
3. Give the differences between RC4 and RC5.
4. Discuss the timing attack on RSA and how it can be overcome.
5. What is meant by birthday attack in hash functions?
6. How MAC is different from hash techniques?
7. What is the purpose of X.509 certificate?
8. What problem was Kerberos designed to address?
9. List the key features of a trusted operating system.
10. What are the factors to be considered while determining the sensitive data in data base security?

Part – B (5 x 16 = 80 marks)

11. (i) Suppose we build an LFSR machine that works mod 3 instead of mod 2. It uses a recurrence of length 2 of the form (8)

$$X_{n+2} \equiv C_0 X_n + C_1 X_{n+1} \pmod 3$$

To generate the sequence 1,1,0,2,2,0,1,1. Set up and solve the matrix equation to find the coefficients C_0 and C_1.

(ii) 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? (interpret this problem in terms of the CRT) (8)

12. a) (i) Show how 12 is transformed to C9 by *subbyte* routine using GF(2^8) field with the irreducible polynomial ($x^8+x^4+x^3+x+1$) in AES algorithm. (8)
(ii) Discuss the key expansion in AES – 128. (8)

OR

b) (i) Discuss any one primality testing algorithm that is used to test whether a given number is a prime or a composite number. (8)

(ii) Perform encryption and decryption using the RSA algorithm (8)
p = 7, q = 11, e = 17, M = 8

13. a) (i) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α = 2.
- Show that 2 is a primitive root of 11. (2)
- If user A has public key $Y_A = 9$, what is A's private key X_A? (3)
- If user B has public key $Y_B = 3$, what is the shared secret key K? (3)

(ii) Discuss in detail about the secure hash algorithm. (8)

OR

b) (i) Discuss in detail about the digital signature standard algorithm. (8)
(ii) Discuss how the key exchange is done using elliptic curve cryptography. (8)

14. a) Discuss briefly about the PGP used for E-mail security. (16)

OR

b) Discuss briefly about IP security architecture. (16)

15. a) Discuss briefly about the security models involved in trusted operating systems. (16)

OR

b) Discuss in detail about the multilevel secure database. (16)