Roll. No.	

B.E/B.TECH. (Full Time) DEGREE END SEMESTER EXAMINATIONS, APR/MAY 2012

COMPUTER TECHNOLOGY

SEVENTH SEMESTER

63

CS9402 / CRYPTOGRAPHY AND SECURITY
(REGULATION 2008)

Time: 3hour Max. Mark: 100

ANSWER ALL QUESTIONS
Part – A (10 x 2 = 20 Marks)

1. Differentiate passive and active attacks.
2. Find GCD (18,300) using Euclid's algorithm?
3. Define Avalanche effect?
4. What is the difference between diffusion and confusion?
5. What is a public –key certificate?
6. Why is SHA more secure than MD5?
7. List the requirements of Kerberos.
8. Give the S/MIME content types and their description
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 a public-key system using RSA ,you intercept the cipher text C=10 sent to a user whose public key is e=5,n=35.What is the plaintext M? (6)

    (ii) Describe Elliptic curve cryptography in detail. (10)

12. a. (i) Derive the equation using the properties of Jacobi symbols (4567/12345) (8)

    (ii) State and prove Chinese Remainder theorem. (8)

Or