18/4/13

Roll. No								42	

B.E / B.Tech (Full Time) DEGREE END SEMESTER EXAMINATIONS, APRIL / MAY 2013

COMPUTER SCIENCE AND ENGINEERING

SEVENTH SEMESTER

CS 9402 – CRYPTOGRAPHY AND SECURITY

(REGULATIONS 2008)

Time: 3 hr Max.Mark:100

Answer All Questions

Part – A (10 X 2 = 20 Marks)

1. Show the number of elements in Galois filed in terms of prime number
2. Define congruence and compare with equality
3. List the parameters (block size, key size, and no. of rounds) for the three AES versions
4. Why do we have only one substitution table(S-Box) in AES but several in DES?
5. List the security services provided by a digital signature
6. What is the padding for SHA-512 if the length of the message is: a) 5120 bits: b) 5121 bits: c) 6143 bits?
7. Define ESP and the security services it provides
8. What is the difference between a firewall and IDS?
9. List out the drawbacks of partitioning as a means of implementing multilevel security for databases.
10. What is multi level database security?

Part – B (5 X16=80)

11. A. i) State and prove the Chinese remainder theorem and also solve $x^2 = 1 \pmod{35}$. (8)
    ii. Explain the hill cipher and its cryptanalysis with an example. (8)

12. A.i) Perform the encryption and decryption for the text M =5 using RSA algorithm by for the given values P=7 & Q=11. (Choose 'e=13'). (8)
    ii). Explain the various stages of AES algorithm in detail (8)

    (OR)

    B. i) Explain the cryptanalysis of RSA algorithm with suitable example (8)
    ii) Illustrate the Simple DES structure and its key generation (8)

13. A) i. Explain the Elgamal cryptosystem and its key generation with suitable example (8)
    ii. Discuss in detail about the DSS algorithm (8)

    (OR)

    B) i. With suitable example, explain the process of MD4 hash function in detail (8)
    ii. Discuss the four birthday attacks in detail (8)

14. A) i. Explain MIME and its parameters in detail (8)

ii. Name the seven types of packets used in PGP and explain their purposes. (8)

(OR)

B) i. Explain the X509 certificate format and specify the certificate renewal and revocation (8)

ii. Describe the SET participants and sequence of events that are required for a transaction in Secure Electronic Transaction (8)

15. A) i. Write the set of rules combining the secrecy controls of the Bell-La-padula Model with the integrity controls of the biba model in trusted operating system. (16)

(OR)

B) i. Explain the multilevel security for databases. (8)

ii. Discuss the purpose of encryption in a multilevel secure database management system? (8)