18/7/13

ANNA UNIVERSITY, CHENNAI-25

B.E/B.TECH END SEMESTER ARREAR EXAMINATION APR/MAY 2013

INFORMATION TECHNOLOGY

SEVENTH SEMESTER

IT 9402 CRYPTOGRAPHY AND NETWORK SECURITY

DURATION: 3Hrs **MARKS: 100**

PART A (10 X 2 =20)

Answer ALL the Questions

1. State the Kerckhoffs's Principle in modern cryptosystem.
2. The ciphertext UCR was encrypted using the affine function 9x + 2 mod 26. Find the plaintext.
3. What are the stages in each round of Advanced Encryption standard (AES) structure?
4. What are the last three digits of 7^{803} ?
5. What are three approaches to attack RSA mathematically?
6. Specify the properties required for a hash function.
7. What is the difference between SSL connection and SSL session?
8. Mention the role of User agent in S/MIME.
9. What are the key features of trusted operation system?
10. List the requirement for database security.

PART B (5 X 16 =80)

11. i) Encrypt the message "howareyou" using the affine function 5x+7 (mod 26). What is the decryption function? (8)

    ii) Explain the Chinese Reminder Theorem and solve $x^2 \equiv 1 \ (mod\ 35)$. (8)

12. a) Explain the simplified DES algorithm with an example.

OR