CSC 316-2081✡

Tribhuvan University

Institute of Science and Technology

2081

✡

Bachelor Level / Third Year /Fifth Semester/Science

Computer Science and Information Technology (CSC316)

(Cryptography)

(NEW COURSE)

Full Marks: 60

Pass Marks: 24

Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.

The figures in the margin indicate full marks.

Section A

Attempt Any TWO questions. **(2×10= 20)**

1. Let us consider the 4 bits key set as { 1100, 1010, 0000, 1111, 0101, 1001} and input text as {1011, 1110, 1011, 1000}. Now trace the first full round operation of IDEA algorithm. (10)
2. What is message authentification code? List the operations of computing digest value in different passes of MD4. Describe about Needhom-Schroeder protocol. (1+5+4)
3. Why do we need discrete logarithms? Illustrate with an example. Consider a Diffie-Hellman scheme with a common prime p=13 between user A and user B. Suppose pulic key of A is 10 and public key of B is 8. Now determine their private keys and shared secret key. Select any valid primitive root of 13. (3+7)

Section B

Attempt Any EIGHT questions. **(8×5 = 40)**

4. Show encryption of plaintext "ALGORITHM" using the key "PSEUDOCODE" using playfair cipher. (2+3)
5. Discuss the working mechanism of the Kerberos protocol. (5)
6. What is the use of firewall? How circuit level gateway differs from stateful inspection firewall? (2+3)
7. What is intrusion? Explain any two types of intrusion detection system. (1+4)
8. Find the multiplicative inverse of polynomial {95} using Extended Euclidean Algorithm. (5)
9. What is DoS attack? Discuss about PKI trust model. (2+3)
10. Using Vigenere cipher with key="worlds", encrypt the plain text "hello everyone". (5)
11. Describe the different modes of block cipher encryption. (5)
12. Write short notes on (any two) (2×2.5=5)
    a) Totient value of a positive integer.
    b) Properties of hash function.
    c) Virus Vs Worms.