CSC 316-2082(O) ✡

Exam Roll No.....

Tribhuvan University

Institute of Science and Technology

2082

✡

Bachelor Level / Third Year /Fifth Semester/Science

Computer Science and Information Technology (CSC316)

(Cryptography)

(OLD 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. Make a comparison between parameters of SHA family. Explain about digital signature standards. [4 + 6]

2. What do you mean by X.509 certificate? Differentiate between SSL and TLS. Explain about PGP. [2 + 3 + 5]

3. Explain one way and mutual authentication with example. Describe the types of intruders. [5 + 5]

Section B

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

4. Define policy and mechanism. Encrypt the message "GENERATIVEAI" taking 3 as shift key. [2 + 3]
5. Write the encryption and decryption process in double DES. List the properties of field. [2 + 3]
6. What is primality test? Test whether 3 is primitive root of 7 or not. [1 + 4]
7. Describe about different passes in MD4. [5]
8. Explain about vigenere and vernam cipher with example. [5]
9. Find the multiplicative inverse of 5 in Z_7 using Extended Euclidean algorithm. [5]
10. Define co – prime numbers. Discuss about Euler's totient function with an example. [2 + 3]
11. Explain in brief about AES encryption process. [5]
12. Define active and passive attack. Write the algorithm for Diffie – Hellman key exchange protocol. [2 + 3]