CSC 316-2079 ✡

Tribhuvan University

Institute of Science and Technology

2079

✡

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. Illustrate the concept of security policy and mechanism with an example. Differentiate between block cipher and stream cipher. Explain the process of key expansion in AES. (3+2+5)
2. Describe the properties of hash functions. Discuss how hash value is generated using SHA-1 algorithm. (4+6)
3. Show that Z_5 is a field. John publishes the ElGamal public key $(q, \alpha, Y_A) = (101, 2, 14)$. Jane desired to send the secret message "CSIT" to John. Using the equivalence A=0, B=1,… ., Z = 25 , encrypt the message using John's public key. Use a random number k = 4. (5+5)

Section B

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

4. Differentiate between Trojan horse and virus. Describe any two types of intruders. (2+3)
5. The message "IMOGUN"was encrypted with a Playfair cipher using keyword "GALOIS". Decrypt the message. (5)
6. How encryption is done using IDEA algorithm. (5)
7. Describe the services provided by Pretty Good Privacy protocol to secure email. (5)
8. What is the condition of for two integers, x and y, to be relatively prime? Find whether 61 is prime or not using Miller-Rabin algorithm. (1+4)
9. Define challenge response system. Why do we need Kerberos? (2+3)
10. How direct digital signature is different from arbitrated digital signature? How digital signature generation and verification is done using RSA. (2+3)
11. Which one is more secure, monoalphabetic cipher or poly alphabetic cipher? Justify. Using Rail fence cipher, encrypt the text "LEARNING AND TEACHING ARE DIFFERENT", using 3 as rails. (1 +4)
12. Why do we need discrete logarithm over normal logarithm? Find out whether 3 is primitive root of 7 or not. (2+3)