B.Sc.CSc.313-2071 ✡

Tribhuvan University
Institute of Science and Technology
2071

✡

Bachelor Level / Third Year /Fifth Semester/Science — Full Marks: 60
Computer Science and Information Technology (CSc.313) — Pass Marks: 24
(Introduction to Cryptography) — 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.
Attempt any ten questions.

1. Answer following questions in short (**any five**). [5x2=10]
   a. Suppose a key logger program intercepts user password and is used to modify the user account. Now, justify whether it's a violation of confidentiality, integrity, or availability or some of combination of them.
   b. How zombies differ from logic bombs?
   c. Mention the advantages of using stream ciphers over block ciphers.
   d. What does Euler Totient Theorem states? What is the value of Totient(15)?
   e. Differentiate session keys from interchange keys.
   f. How Message Authentication Codes differ from Hash Functions?
   g. Briefly describe SubBytes and ShiftRows in AES.

2. a. In public key cryptosystem, each of the communicating parties, in general, should know the public keys of each other before attempting security encryptions. How this can be achieved? Write a Public Key Authority Protocol for public-key distribution among any two users. [4]
   b. How Kerberos Version 4 differs from Kerberos Version 5? How once per type of service approach is ensured by Kerberos Protocol. [6]

3. a. Configure a Vignere table for the characters from A-H. Use the table to encrypt the text DAD CAFÉ EACH BABE using the key FADE. [4]
   b. Mention the details of logical operations used in MD4. How the Majority function in Pass 1 of MD4 works? [6]

4. a. Encrypt the message "help" using the Hill cipher with the key $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and the result. [4]
   b. What do you mean by arbitrated digital signature? How signatures are generated using Digital Signature System? [6]

5. a. In a RSA system, a user Named Alice has chosen the primes 7 and 11 to create a key pair. Compute the public key (e_{Alice}, n) and the private key (d_{Alice}, n). Now encrypt the message = "bye" using the public key of Alice. [6]
   b. How Transport Mode of IPSec Operation differs from the Tunnel mode? [4]

6. a. How subkeys are generated in DES encryption procedure? Write a protocol for decrypting ciphertext using DES. [6]
   b. How Jailing and Backoff can be used to demotivate online dictionary attack in authentication system. [4]