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
(Cryptography)	Time: 3 hours

Candidates are required to give their answers in their own words as far as practicable.
The figures in the margin indicate full marks.

Attempt all the questions
1. Answer the following questions in short (Any Five). (5 × 2 = 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 Vigenere table for the characters from A-H. Use the table to encrypt the text DAD CAFE 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
3 3
2 5
. 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) How do you create public and private keys in the RSA algorithm for public-key cryptography? (5)

OR

What are the notions Public Key Ring and Private Key Ring in PGP?

b)What is the difference between a connection and a session in SSL/TLS? Can a session include multiple connections? Explain the notions “connection state” and “session sate” in SSL/TLS. What security features apply to each? (5)

6. a) How hash function differ from MAC? Discuss how data integrity can be achieved from either of them. (5)

b)What is a certificate and why are certificates needed in public key cryptography? (5)