Tribhuvan University
Institute of Science and Technology
2072

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. What does Euler Totient function means? What will be the value of PHI (119)?
b. What properties does a good hash function should have?
c. What is the purpose of S-Box in DES?
d. Define each of the terms confidentiality, integrity and availability.
e. What do you mean by primitive root of a prime number p? Is 3 a primitive root of 7?
f. Describe the concept behind public key infrastructure.
g. What are the possible phases that a virus can go through, during its life cycle?

2. a) In a RSA system, a user has chosen the primes 5 and 19 to create a key pair. The public key is {e=5, n=?}
and the private key is {d=?, n=?}. Decide the private key {d, n}. Show encryption and decryption process for the message "TOGA" [6]
b)Encrypt the message "MEET ME TONIGHT" using the Hill cipher with the key
9 4
5 7
. Show your calculations and the result. [4]

3. a) Differentiate between SSL Session and SSL Connection. How SSL Record protocol provides confidentiality and message integrity. [2+3]
b)What basic arithmetic and logical functions are used in SHA-1? [5]

4. a) Briefly describe about MixColumns and AddRoundKey stages in AES. How many bytes in a state are affected by ShiftRows round? [5+1]
b)List the participants of Secured Electronic Transaction (SET). Discuss the key features of SET. [4]

5. a) In which situation using Kerberos system seem to be good? Describe what the major components of Kerberos system are. [2+4]
b)Given the plaintext "LOST IN PARADISE", compute the ciphertext for

i. The Ceaser cipher with key = 5
ii. The Railfence cipher with rails = 4 [4]

6. a) Differentiate between direct digital signature and arbitrated digital signature. How signing and verifying process is done in Digital Signature Standard. [2+4]
b)What do you mean by Man-in-Middle attack? Is man in middle attack possible in Diffie-Hellman algorithm for key exchange? How? [4]