Tribhuvan University
Institute of Science and Technology
2069

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. How monoalphabetic substitution differs from polyalphabetic. Briefly define with suitable example.
b. What are the components of authentication system? Give an example of authentication system.
c. What do you mean by avalanche effect?
d. How chosen plaintext attack differs from chosen ciphertext attack?
e. What do you mean by multiplicative inverse? Find multiplicative inverse of each nonzero elements in Z11.
f. Even though we have a strong algorithm like 3-DES, still AES is preferred as a reasonable candidate for long term use. Why?
g. Give an example for a situation that compromise in confidentiality leads to compromise in integrity.

2. a) Consider a Deffie-Hellman scheme with a common prime p = 11 and a primitive root g = 2.

i. Show that 2 is a primitive root of 11.
ii. If user A has public key Ya = 9, what is A's private key Xa?
iii. If user B has public key Yb = 3, what is shared key K, shared with A. (3x2=6)

b)Construct a playfair matrix with the key "KEYWORD". Using this matrix encrypt the message "WHY DON'T YOU". (4)

3. a) How Trojan horse differs from viruses? Discuss about possible types of Trojan horses. (2+3)
b)Does Kerberos protocol ensures authentication and confidentiality in secure system? Explain. (5)

4. a) How Hash functions differ from MAC? Given a message m, discuss what arithmetic and logical functions
are used by MD4 to produce message digest of 128 bits. (2+4)
b)Discuss the five principle services provided by PGP protocol. (4)

5. a) What is the purpose of S-Boxes in DES? Prove that DES satisfies complementation property? (6)
b)Given the plaintext "ABRA KA DABRA", compute the ciphertext for (4)

i. The Ceaser cipher with key = 8
ii. The Railfence cipher with rails = 3

6. a) What do you mean by digital signature? How digital signatures can be enforced using encryptions? Illustrate with an example. (1+5)
b)Determine whether the integers 105 and 294 are relatively prime. Explain your answer using Euclidean algorithm. (4)