Tribhuwan University
Institute of Science and Technology
2074

Bachelor Level / fifth-semester / Science — Full marks: 60
Computer Science and Information Technology(CSC316) — 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 questions.

1. Answer the following questions in short (Any Five).

a. What are the typical phases of operation of virus?

b. Find Multiplicative inverse of each nonzero elements in Z_5.

c. Why Hash Functions are often known as one way functions?

d. how Vignere Cipher can be used to ensure poly-alphabetic substitution?

e. Using extended Euclidean Algorithm, find multiplicative inverse of 550 and 1769.

f. Define PKI Trust Model.

g. What do you mean by odd round in IDEA?

2.

a) What do you mean by transposition cipher? Decrypt the ciphertext UIESTNVRIY using the Railfence cipher using the rail size 2.

b) Consider the message blocks m1, m2, m3. If the Cipher Block Chaining mode DES encryption can be expressed as $C_i = DES(m_i \oplus m_{i-1} \oplus C_{i-1}); \; m_0 \oplus C_2 = IV.$ **Now, write the expressions for the DES decryption to extract each of the message blocks m1, m2, m3.**

3.

a) How padding is done in MD5? What enhancements in MD4 are done to get better hash function MD5?

b) Construct a playfair matrix with the key CRYPTO. Using this matrix encrypt the message "have a nice day".

4.

a) In a RSA system, a user named Messi has chosen the primes 5 and 11 to create a key pair. Now show the generation of public key pair (e_{Messi}, n) and private key pair (d_{Messi}, n). Show how Messi can encrypt the message "Soccer" using his own public key.

b) What is the role of SSL Handshake Protocol in Secure Socket layer Protocol?

5.

a) What is the use of digital signature? Discuss the working mechanism of Digital Signature Algorithm.

b) Encrypt the message "Eight Ten" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ **. Show your calculations and the result.**

6.

a) Suppose there are two users Xavi and Persie who agreed to use Deffie-Hellman algorithm to exchange a key. Consider there is an eavesdropper Balotelli who attemps attack on the procedure. Show how Balotelli can perofrm Man-In-Middle attack in the Deffie-Hellman Key exchange protocol?

b) What do you mean by password aging? How online dictionary attacks differ from offline attacks?

