

Tribhuvan University
Institute of Science and Technology
2080
☆

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology (CSC.313)
Cryptography
(OLD COURSE)

Full Marks: 60
Pass Marks: 24
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)** (5× 2=10)
 - a. Define trojan horse.
 - b. Differentiate between cryptography and cryptanalysis.
 - c. What is the primitive root of a number?
 - d. What is the multiplicative inverse of a number?
 - e. How the CBC mode of block cipher works?
 - f. Define public key cryptography.
 - g. How subkeys are generated in the IDEA algorithm?
2.
 - a. Show the encryption and decryption process using Ceasar cipher for plaintext="csitchance". [4]
 - b. Show encryption and decryption of RSA for p=7, q=5, and M=10. [6]
3.
 - a. How SSL record protocol ensures confidentiality in SSL protocol? [4]
 - b. How a hash value is generated in SHA-1? [6]
4.
 - a. Describe digital signature. How one-time signature works? [3+2]
 - b. Discuss the working mechanism of the Kerberos Protocol. [5]
5.
 - a. Explain the services provided by the PGP protocol. [5]
 - b. Describe how mix-column and add-round key operations are done in AES. [5]
6.
 - a. How threat is different from attack? [4]
 - b. Given two users A and B having public key parameters p=7 and g=17, compute their private and public keys and shared secret key K between A and B. [6]