Tribhuwan University
Institute of Science and Technology
2075

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 following questions in short (any five)

a. The larger the size of key space, the more secure a cipher? Justify your answer.

b. Differentiate between virus and Trojan horse.

c. What is the weak collision resistance property of hash function?

d. Differentiate between transposition cipher and substitution cipher?

e. What does $Z_n$refer to in cryptography? Illustrate with an example.

f. What is the additive inverse of 2 in Z_{10}?

g. John copies Mary's homework. Does it violate confidentiality or integrity or both? Justify.

2. **a) What do you mean by "Fiestel Structure for Block Ciphers"? Explain.**

OR

How can a number be tested for primality testing using Miller-Rabin algorithm? Explain. **b)**

Divide $5x^2$+4x+6 by 2x+1 over GF(7).

3. **a) Find the result of the following operations.**

(i) 2 mod 5 (ii) 33 mod 3 (iii) -13 mod 10 (iv) -23 mod 10 (v) -8 mod 7 b) How

can Diffie-Hellman be used for key exchange? Explain.

4. **a) Encrypt the message "machine passed turing test" to playfair cipher using key "ALANTURING".**

b) What is the digital signature for, authentication of confidentiality? Justify your answer. What does security handshake pitfall refer to?

5. **a) Explain about PGP. OR What is the role of the SSL Record Protocol in**

SSL/TLS? Explain.

b) Describe the method for generating the Round Constant table in the AES algorithm in the Add Round Key phase. Assume the number of rounds is 10.

6. **a) Does hash and MAC resemble the same meaning? Explain how SHA generates 160 bit digest value?**

b) Define field. Differentiate between public key cryptography and private key

cryptography.