Tribhuwan University
Institute of Science and Technology
2076 (new)

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.

Section A

Attempt Any Two questions. (2 x10 =20)

1. Among monoalphabetic and polyalphabetic ciphers, which one is more vulnerable? Justify your statement. Which types of keys are considered as weak keys in DES? Explain round operations in IDEA.

2. State the Fermat's theorem with an example. Given the prime number p=29 and the primitive root g=8, private key of sender with X=9 and random integer K=11, encrypt the message m=13 using Elgamal cryptosystem.

3. Compare the SHA parameters between SHA-1 and SHA-2 families. Decrypt the ciphertext DRJI with key $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$ **using Hill cipher.**

Section B

Attempt Any Eight questions. (8 x5 =40)

4. Define discrete logarithm. Explain the procedure of sharing the secret key in Diffie Hellman.

5. Distinguish between stream cipher and block cipher. Encrypt the message WE ARE IN SAME RACE UNTIL OUR LIVE END using Rail fence cipher using 4 as number of rails.

6. Define digital signature. Describe the approaches of DSS.

7. What is the task of a firewall? List the elements of X.509.

8. How does the nature of worms differ from viruses? Define PKI with its architecture model.

9. Explain the procedure of mix column transformation in AES with an example.

10. What is the role of the prime number in Euler totient function? Find the GCD of 12 and 16 using Euclidean algorithm. 11.

Write down any two limitations of MAC? What does policy and mechanism mean in cryptography? Describe a scenario. 12.

Write short notes on (Any Two)

a. Classes of intruder

b. SSL

c. Dos Attack