Tribhuvan University
Institute of Science and Technology
2076
✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology (CSc.316)
(Cryptography)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Section A

Attempt Any *Two* questions **[2×10= 20]**

1. Among monoalphabetic and polyalphabetic cipher, which one is more vulnerable? Justify your statement. Which types of keys are considered as weak keys in DES? Explain the round operation in IDEA. [2 + 2 + 6]

2. State the Fermat's theorem with example. Given the prime number p=29 and its primitive root g=8, private key of sender with X=9 and random integer K=11, encrypt the message m=13 using Elgamal cryptosystem. [5 + 5]

3. Compare the SHA parameters between SHA-1 and SHA-2 family. Decrypt the cipher text DRJI with key $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$ using Hill Cipher. [3+7]

Section B

Attempt Any Eight questions **[8×5 = 40]**

4. Define discrete logarithm. Explain the procedure of sharing the secret key in Diffie Hellman. [2 + 3]

5. Distinguish between stream cipher and block cipher. Encrypt the message WE ARE IN SAME RACE UNTILL OUR LIVE END using Rail fence cipher using 4 as number of rails. [2 + 3]

6. Define digital signature. Describe the approaches of DSS. [2 + 3]

7. What is the task of firewall? List the elements of X.509. [2 + 3]

8. How does the nature of worms differ with virus? Define PKI with its architecture model. [1 + 4]

9. Explain the procedure of mix column transformation in AES with an example. [5]

10. What is the role of prime number in Euler totient function? Find the GCD of 12 and 16 using Euclidean algorithm. [2.5 + 2.5]

11. Write down any two limitations of MAC? What does policy and mechanism mean in cryptography?Describe with a scenario. [2 + 3]

12. Write short notes on (AnyTwo) [2.5 + 2.5]
    a. Classes of Intruder
    b. SSL
    c. DoS Attack