Tribhuvan University
Institute of Science and Technology
2080
✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology (CSC316)
(Cryptography)
(NEW COURSE)

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. Define discrete logarithms. How key generation, encryption and decryption is done in RSA. In a RSA cryptosystem, given p=13 and q=7, determine private key, public key, and perform encryption and decryption for the text M= "hi" using 0 to 25 for letters from a to z. (10)

2. Write down the encryption and decryption process at 2-DES and 3-DES. Explain the Fiestel cipher structure. Divide $5x^2 + 4x + 6$ by $2x + 1$ over GF (7). (3+3+4)

3. What are the applications of hash functions? Discuss how SHA-1 algorithm generates hash value from a given message. (2+8)

Section B

Attempt Any EIGHT questions. **(8×5 = 40)**

4. Show encryption and decryption of "csit" using hill cipher having key $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$. (5)

5. Give the formal definition of Authentication system. Describe about one way and mutual Authentication system. (2+3)

6. List the stage of certificate life cycle. What are the types of firewalls? (3+2)

7. What is malicious logic? How Zombies are different from Trojan horses? (1+4)

8. How Miller Rabin test is used for primality testing? Show whether the number 561 passes the test. (2.5+2.5)

9. Show that the set of integers is Ring under addition and multiplication. (5)

10. How substitution ciphers are different from transposition ciphers? Given a message M="CSIT PROGRAM IS A HOT CAKE", encrypt M using Rail Fence cipher with rail size=3. (2+3)

11. Describe about IPSec. List the five services of PGP. (3+2)

12. How does meet in middle attack work in Diffie Hellman key Exchange protocol? Explain. (5)