CENTRAL INSTITUTE OF TECHNOLOGY KOKRAJHAR
(Deemed to be University)
KOKRAJHAR :: BTR :: ASSAM :: 783370

END – SEMESTER EXAMINATION
DIPLOMA

Session: July-December, 2022 Semester: V Time: 3Hrs. Full Marks: 100

Course Code: **DCSE504** Course Title: **Cryptography and Network Security**

Answer 1 [both A and B] is Compulsory. Attempt any three from rest!

1 A. 2 x 10 = 20

i. Unauthorized disclosure violates _____ security service.
ii. Unauthorized modification violates _____ security service.
iii. _____ technique is used for source authentication.
iv. In _____ same key used for both encryption and decryption.
v. Disruption in service violates _____ security service.
vi. Using public cryptography if public key is used for encryption _____ is used for decryption.
vii. _____ type cipher block of plaintext is encrypted in to block of ciphertext.
viii. Playfair cipher use ___x___ matrix and letter__/__ are placed in the same cell.
ix. Integrity can be achieved by _____ technique.
x. Masquerade is type of _____

B. Short answer questions 2 x 10 = 20

i. What is a Security Attack?
ii. Difference between mono alphabetic and polyalphabetic cipher?
iii. What is Cryptanalysis Attack?
iv. What is a Stream Cipher and Block Cipher?
v. What are the Differences between Symmetric Cipher and Asymmetric Cipher?
vi. What is a Vernam Cipher?
vii. What is a Digital Signature?
viii. Write any two examples for Public Key Cryptosystem.
ix. What is Denial of Service?
x. What are Security Threats?

2 a. What is a Caesar Cipher? Explain the Caesar Cipher Algorithm for Encrypting and Decrypting the plaintext message. 10 + 10 = 20

b. Write the rules for Playfair Cipher Algorithm for encrypting a message. Using Playfair algorithm Encrypt the message BALLOON with the key CIPHERWORK.

3 a. What is a Public Cryptography? Explain RSA algorithm? 10 + 10 = 20

b. Suppose two entities A and B wanted to communicate securely with each other using RSA algorithm. Design a communication system using public key cryptography so that Receiver can get the encrypted message along with capability of authenticating the sender as well verify the integrity of the message.

4 Find the inverse of a matrix K that can be used for Hill Cipher Decryption Algorithm 20

$$\text{Given } K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Find K^{-1} mod 26?

5 a. Explain Extended Euclid Algorithm for finding the inverse of a modular number. 10 + 6 + 4 = 20

b. Using extended Euclid algorithm find 23^{-1} mod 26?

c. What is value of -300 mod 26?

6 Short notes (any four) 4 x 5 = 20

a. Confidentiality
b. Authentication
c. Brute Force Attack
d. Spoofing
e. DES Algorithm
f. Vigenere Cipher

******