Department of Computer Science and Engineering

Central Institute of Technology Kokrajhar

End Semester Examination

Diploma

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

Session: **July-Dec, 2024** Full Marks: **100** Time: **3:00** hrs

---

Figure in the margin indicates full marks.

Question 1 is compulsory. Answer any three from rest of the questions!

1 [A] Fill in the blanks. 2 x 10 = 20

a. The process of converting readable data into a coded format to prevent unauthorized access is known as _____.
b. In _____ cryptography, the same key is used for both encryption and decryption.
c. _____ is a common mode of operation for symmetric block ciphers that involves chaining the ciphertext blocks.
d. _____ key cryptography involves using two different keys for encryption and decryption; one public and one private.
e. The security of RSA, an asymmetric algorithm, relies heavily on the difficulty of factoring large _____ numbers.
f. A _____ attack is when an attacker intercepts and possibly alters messages in transit between two parties.
g. _____ is the process of determining the original plaintext from the ciphertext without knowing the key.
h. In cryptography, _____ refers to the property that a small change in the plaintext or key should produce a significant change in the ciphertext.
i. The Key Size of DES algorithm is _____ bits.
j. In _____ technique a piece of plaintext is hidden inside another file or image.

[B] Write short notes (any ten) 2 x 10 = 20

a. Confusion
b. Diffusion
c. Masquerade Attack
d. Phishing
e. Confidentiality
f. Hashing Function
g. Modes of Operation
h. Caesar Cipher
i. Transposition Cipher
j. Digital Signature
k. Hill Cipher
l. Playfair Cipher

2 a. Explain the Principles of Network Security or Security Services. 10 + 5 + 5 = 20
b. What are the Mechanism of Security?
c. Map any five mechanisms of security with principle of security?

3	Explain Data Encryption Standard algorithm for Encrypting and Decrypting the messages. Show the intermediate calculation for i^{th} round of encryption.	20
4	a. Explain RSA algorithm for Key Generation, Encryption and Decryption. b. For a particular communication a Ciphertext = 5 was intercepted using a modulus n = 77 and public key e = 7. Calculate the plaintext.	10 + 10 = 20
5	a. Explain any five applications of Hashing Functions. b. Design MAC that can achieve the following functionalities integrity, authentication and confidentiality of the message.	10 + 10 = 20
6	Explain any four of the following a. Key Exchange Protocol b. Firewall c. Authentication and Authorization d. Rotor Machine e. Man in the Middle Attack f. Virus, Trojan, Worms	5 x 4 = 20

xxXxx