Enrolment No. 102CTBMCS21 2 [redacted]

NATIONAL FORENSIC SCIENCES UNIVERSITY, DELHI CAMPUS

B. Tech. - M. Tech. CSE (Cyber Security)-Sem IV, April 2023

Mid Semester Examination

Subject Code: CTBTCSE SIV P5	**Date: 21/04/2023**
Subject Name: Cryptographic Concepts	**Time: 1 Hr 30 Min**
	Total Marks: 50

Instructions:

1. This Question Paper consists of 7 Questions.
2. All the questions are compulsory.

Section A (2 * 5 Mark)

1. Perform encryption and decryption with the keyword "HEALTH" to the message "operating system paper was very difficult". (Hint: Use Vigenere cipher)
2. Distinguish between a substitution cipher and a transposition cipher with example.

Section B (5 * 8 Mark)

3. (a). Explain encryption and decryption process in Affine Cipher with example.

(4 Mark)

(b). Compare and contrast keyless and keyed transposition cipher with example.

(4 Mark)

4. (a). Encrypt the message, "LET US MEET AT OUR USUAL PLACE" using the Hill cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. **(5 Mark)**

(b). Decrypt any letter of the above plain text. **(3 Mark)**

5. If the key with parity bit (64 bits) is 0123 ABCD 2562 1456, find the first-round key.

(8 Mark)

6. (a). What is a fiestal cipher. Explain with suitable diagram. **(3 Mark)**

(b). What is the block size in DES? What is the cipher key size in DES? What is the round-key size in DES? **(5 Mark)**

7. (a). How many mixers and swappers are used in the encryption process using DES technique. **(3 Mark)**

(b). Differentiate with example block cipher and stream cipher. **(5 Mark)**

**~~~~~~~~~~~~~~ End~~~~~~~~~~~~~~**

Seat No. [redacted] Enrolment No. 102CTBMCS21[redacted]

NATIONAL FORENSIC SCIENCES UNIVERSITY

B.Tech.-M. Tech. Computer Science & Engineering - Semester - IV - July-2023

Subject Code: CTBTCSE SIV P5 **Date: 07/07/2023**

Subject Name: Cryptography

Time: 11:00am – 2:00pm **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Q1. Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7,2) in modulus 26.
10 marks

Q2. Find the multiplicative inverse of 23 in Z_{100} using extended Euclidean algorithm.
10 marks

Q3. Discuss in detail about access control policies and access control requirements.
10 marks

Q4. Explain cryptographic hash functions with an example. Describe the idea of the Merkle- Damgard scheme and why this idea is important for the design of cryptographic hash functions.
10 marks

Q5. Explain all the three criterions for a cryptographic hash function. **10 marks**

OR

Q5. Provide an explanation of the Feistel architecture and elucidate the methods employed within this design to achieve diffusion and confusion. **10 marks**

Q6. Explain the following architectures in detail in relation to SHA512

(a) word expansion
10 marks

(b) compression function
10 marks

Q7. Explain the following

(a) Diffie Hellman Key Exchange algorithm.
5 marks

(b) Explain man-in-the-middle attack.
5marks

Q8. Distinguish between symmetric-key and asymmetric key cryptosystems.

10 marks

Q9. Explain the RSA algorithm with a suitable example. **10 marks**

OR

Write short notes on the following

(a) S-box (For explanation you can make your own S box table)

(b) Vigenere Cipher **10 marks**