CS113/DISCRETE MATHEMATICS-SPRING 2024

Worksheet 30

Topic: Cryptography

In today's session, we will study Cryptography where we'll learn how to secure information through encryption and decryption techniques and explore various algorithms. Get ready to uncover the art and science of secure communication that has shaped history and continues to play a vital role in the digital age. Happy Learning!

Student's Name and ID: _____

Instructor's name: _____

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   (a) f(p) = (p + 3) mod 26 (the Caesar cipher)

(b) $f(p) = (3p + 7) \bmod 26$

2. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \bmod 26$.
   (a) CEBBOXNOB XYG

3. Encrypt the message `GRIZZLY BEARS` using blocks of five letters and the transposition cipher based on the permutation of $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 2$, and $\sigma(5) = 4$. For this exercise, use the letter `X` as many times as necessary to fill out the final block of fewer than five letters.

4. Decrypt the message `EABW EFRO ATMR ASIN`, which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation σ of $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.