CSCI 325 - Fall 25 - Homework2

Due date:
Sunday, Sep. 14th, 11:59 PM for question 1 and 2.
Thursday, Sep. 18th, 11:59 PM for question 3 and 4.

1. (3 points) An affine cipher has the form $c = (am+b) \mod n$. Suppose m is an integer between 0 and 25, each integer representing a letter. Let $n = 26$, $a = 3$, and $b = 19$. What is the ciphertext corresponding to the phrase THIS IS A CIPHER MESSAGE.

2. (3 points) Please answer the following questions.

   (a) What is the index of coincidence (IoC)?

   (b) What is the relationship between the IoC of plaintext and ciphertext using affine cipher for encryption and explain the reason?

   (c) How does the IoC helps you decrypt the ciphertext using Vigenere cipher?

3. (10 points) Write a program to allow the user to encrypt and decrypt Vigenere ciphertext using a user-specified keyword. For example, `"MAYTHEFOURTHBEWITHYOU"` encrypts to `"XUIXSYPSFLDLMYGMEBISF"` using keyword `"LUKE"`. Demonstrate that your code works by decrypting the Vigenere ciphertext in `cipherKnownKey.txt` with the keyword `"TAGORE"` on Canvas. Your submission should include code for encryption and decryption using Vigenere cipher and a decrypted file `plainKnownKey.txt`.

   Please have another student in the class grade your program using the following rubric:

   - Code readability (0–5)
   - Correctness (0–5)
   - Written or oral explanation and efficiency (0-5)

   The final grade will be calculated as 50% instructor grade and 50% peer grade. Be sure to include the name of your peer grader in your submission.

4. (10 points) Write a program to cryptanalyze Vigenere ciphertext when the keyword is *unknown*. Demonstrate that your code works by decrypting the Vigenere ciphertext in `cipherNoKey.txt` on Canvas. Your submission should include code for cryptanalysis and a decrypted file `plainNoKey.txt`.

   Please have another student in the class grade your program using the following rubric:

   - Code readability (0–5)
   - Correctness (0–5)
   - Written or oral explanation and efficiency (0-5)

   The final grade will be calculated as 50% instructor grade and 50% peer grade. Be sure to include the name of your peer grader in your submission.