CPT_S 327 - Homework 1

In this homework, please send one pdf file with the following information: (1) Your name, (2) your WSU ID, (3) the write up for the following two questions. More details are specified in each question.

Problem 1

Prove that the shift cipher for a single character is perfectly secure. Particularly, consider the following private-key encryption scheme:

- Message space: English alphabets lowercase letters a - z, represented by 0 to 25, respectively. Ciphertext and secret key spaces: the same as the message space.
- KeyGen: pick a random lower case letter, i.e., pick $\mathsf{sk} \leftarrow [0, 25]$ uniformly at random, and interpret the number as the english letter.
- $\mathsf{Enc}(\mathsf{sk}, m)$: given a message $m \in [0, 25]$, output $c = m + \mathsf{sk} \mod 26$.
- $\mathsf{Dec}(\mathsf{sk}, c)$: given a ciphertext $c \in [0, 25]$, output $m = c - \mathsf{sk} \mod 26$.

Note: all lowercase letters and numbers from 0 to 25 are used interchangeably.

For this problem, you need to write (1) the definition of "perfectly secure" which you are going to use next, and (2) a proof that the construction satisfies the definition. You don't need to prove correctness as that is very trivial.

Problem 2

If the message length is larger than the secret key length, then this scheme cannot be perfectly secure.

Below we describe an encryption scheme for you to attack. Please take your WDU ID modulo 8, and then attack txt file with the resulting number. For example, if your WSU ID is 0000008, then attack the file "cipher0.txt". Similarly, if your WSU ID is 00000010, then attack "cipher2.txt".

Now the scheme works as follow:

- Message space: English lowercase letters for a certain length, including ",", "-", etc. Ciphertext space: the same as message space. Key space: lowercase letters of length 6 - 10.

- KeyGen: pick a random lower-case string of length between 6 and 10 for sk.
- $\mathsf{Enc}(\mathsf{sk}, M)$: Given message lower-case words M, each character is shifted by the next letter of sk (modulo 26). If you reach the end of sk, goto the first character, and repeat. Here the encryption algorithm keeps punctuation and space intact.

  The encryption algorithm is provided in the "**cipher.cpp**".
- $\mathsf{Dec}(\mathsf{sk}, C)$: Unscramble each character one-by-one.

For this problem, you need to write: (1) your WSU ID modulo 8, (2) the plaintext in the corresponding file (3) the secret key (Note: between length 6 - 10 lowercase characters), (4) your method (described briefly about how you figure things out). If you write a code to do that, please attach your code (in a separate page in the same pdf file).