Homework Assignment 1

CIS 5371 — Austin Leach — Fall 2023

1. If both are encrypted with the same one-time pad then the first cipher text $C1$ and the second $C2$ along with the first decrypted message $M1$ and second $M2$ will result in $C1 \oplus C2 = M1 \oplus M2$. Let $M = C1 \oplus C2$. Let N be the set of every 11 character word in the dictionary with $n \leftarrow\!\!\$\; N$. With this we can do $M \oplus n$ for every n in order to find both $M1$ and $M2$. This gave me two words, **obfuscation** and **certificate** from the given cipher text which makes it a reused one-time pad.

2.a. A simple encryption method for Alice and Bob to use is $C = (M+K) \bmod N$. The decryption method for this $M = (C-K) \bmod N$. To show correctness for this scheme lets use $n = 1$ and $N = 3$ and a message of $M = 0$ the key K is uniformly distributed over $\{0, 1, 2\}$. The encryption would be

$$K = 0, (0+0) \bmod 3 = 0$$
$$K = 1, (0+1) \bmod 3 = 1$$
$$K = 2, (0+2) \bmod 3 = 2$$

The decryption for this is

$$K = 0, (0-0) \bmod 3 = 0$$
$$K = 1, (1-1) \bmod 3 = 0$$
$$K = 2, (2-2) \bmod 3 = 0$$

This shows that there is a ciphertext space of $\{0, 1, 2\}$ and they all will decrypt to the correct message $M = 0$.

b. To prove this is perfectly secret we have to show that every ciphertext is equally as likely as any other ciphertext. To show that each ciphertext is equally likely for a set M, N, and K lets use $n = 1$, $N = 3$ and a message $M = 0$ with key K uniformly distributed over $\{0, 1, 2\}$. The encryption for this is

$$K = 0, (0+0) \bmod 3 = 0$$
$$K = 1, (0+1) \bmod 3 = 1$$
$$K = 2, (0+2) \bmod 3 = 2$$

These keys have a ciphertext space of $\{0, 1, 2\}$. Because there are 3 keys and also 3 possible ciphertext each with a $1/3$ chance of happening this shows that the ciphertext is uniformly distributed.

To show that this is also true for any general M, N, and K we can do the following. For N with a key K uniformly distributed over $\{0, 1, ..., 1 - N\}$. Since K is in the range of 0 to $N - 1$ this means that no matter what the M is when you do $(M + K) \bmod N$ it will result in a ciphertext space of $C \xleftarrow{\$} \{0, 1, ..., 1 - N\}$. Since there is N possible ciphertext and N possible keys this means there is an equally likely chance of $1/N$ to get any ciphertext which proves that it is uniformly distributed and therefore perfectly secret.