CSC 429 Assignment 1

Alexander Williams

January 19, 2025

Question 1

a)

Given a block length of $\ell = 1$, and a key of $k_0, k_1, ..., k_{\ell-1}$, the encryption of the i^{th} character in a block where $0 \leq i \leq \ell - 1$ is:

$$c_i = k_i + m_i + j$$

The corresponding decryption function will be written as:

$$m_i = c_i - k_i - j$$

b)

First, find the key length with the index of coincidence.

Since each character in a block is shifted by a different amount, we only want to calculate the IC of all the i^{th} characters in a block together. For example, We take all the 1^{st} characters in a block, and find their IC. Then the 2^{nd}, then 3^{rd}, up to the ℓ^{th} character, and we take the average to find the overall IC for a key of that length.

We do this for all possible key length, and we take the length with the closest IC to 0.065, we try to minimize the function $|\sum_0^{25} q_i^2 = 0.065|$, where q_i is the the probability that a given character in the text is the i^{th} character in the alphabet

Since the j^{th} block increments the value of each character by j, we'll have to subtract j from the value of each character before taking the IC.

Once we have the block length, we have to find the key.

Once again, we'll take the i^{th} character of each block, subtract j, and this time we want to find the key character k that minimizes $|\sum_0^{25} p_i q_{(i-k)mod26} - 0.065|$, where $q_{(i-k)mod26}$ is the probability of any character in the text is the $i - k^{th}$ character in the alphabet, and p_i is the chance any character in the english language is the i^{th} character in the alphabet.

Once we've done this to get all ℓ characters of the key, we can use the earlier mentioned decryption function to get back the original message.

c)

Running our ciphertext through a python program I made for this assignment, I got a key length of 6, and the key was $(2, 8, 15, 7, 4, 14)$ (C I P H E R).

Once decoded, the message reads:

AGEDTWENTYSIXVIGENEREWASSENTTOROMEONADIPLOMATICMISSION
ITWASHERETHATHEBECAMEACQUAINTEDWITHTHEWRITINGSOFAL-
BERTITRITHEMIUSANDPORTAANDHISINTERESTIN CRYPTOGRAPHY-
WASIGNITEDFORMANYYEARSCRYPTOGRAPHYWASNOTHINGMORETHANATOOL
THATHELPEDHIMHISDIPLOMATICWORKBUTATTHEAGEOFTHIRTYNINEVI-
GENEREDECIDEDTHATHE HADAMASSEDENOUGHMONEYTOBEABLE-
TOABANDONHISCAREERANDCONCENTRATEONALIFEOF STUDYITWA-
SONLYTHENTHATHEBEGANRESEARCHINTOANEWCIPHER