Tucker David Yazdani

Professor Mark Faucette

Senior Project

November 29, 2019

A modern approach to Dr. Faucette’s Coding Project

Cryptography is a subject that uses mathematic concepts such as number theory and linear algebra to decode a message by mapping letters onto numbers. For example, A could map to 1, B could map to 2…,Z could map to 26. Cryptography then takes these numbers and performs some enciphering techniques to encode the message. The goal of this is to make it as close to as impossible to decipher the message for anyone besides the intended party. This usually involves having a known key between the two parties. This project focuses on finding a way using mathematics and computer science to decode an affine diagraph cipher, by building an algorithm that returns the key to the enciphered message, and then building an algorithm that takes the known key to decipher it.

First observe the equation for an Affine Diagraph Cipher. Where *c­* denotes the coded text coefficients, *m* denotes the encoding matrix coefficients, *p* denotes the plain text coefficients, and *b* denotes the coefficients on the encoding vector.

Every ciphering code outputs a ciphered text which gives us the *c* in this problem. In this project the first 5 pairs of plain text letters *p* were given. This means that that in this equation we have information concerning the coded text vector, and the plain text vector for the first 10 letters. Through some basic matrix multiplication, we can transform this code into a more computer friendly equation.

This equation is much easier to input to a computer program, since it does not require the program to know linear algebra. This leaves us only to discover what the coefficients on the encoding matrix are, and what are the coefficients on the encoding vector. Since we are working in modulus 26, the only possible entries for any numbers used in this equation are 0 through 25. This narrows the possibilities for each entry to 26. Also, there is something very important to note here. Notice the equation for c1 does not depend on m21, m22, and b2 for now (this will come up later). We can then find solutions for the equations for c1 and c2 independently. This is very important as if we had to put these all into a nested for-loop the program will take forever to load. Now that we have this equation in this form, we can begin constructing the algorithm.

To begin the algorithm, we start by creating a for-loop that sets m11 equal to the values 0 through 25, changing m11 to be equal to the number of iterations the loop has gone through, which tests all its possible values. Since the equation also depends on m­12, we create a nested for loop similarly that iterates what m12 is equal to for every possible value of m11. For instance, in the first iteration both m11 and m12­ are equal to zero, but the next iteration m11 remains 0 and m12 is now equal to 1. Since in this iteration the values for m11 and m12 are fixed, if we solve for b1 we remove the necessity to iterate 26 times per loop which makes the program run much faster. We will use from the first pair of coded letters “XS” the letter “X” to create a shortcut to solving b1 as follows:

Once b1 and b­2 are solved for, we can then check to see if our equation is correct in the given iteration by evaluating if the previous equation for c1 is correct. For instance, consider the second pair of the coded message “ZW”. We know from the given information the letters “CH” maps to “ZW” after decryption. Since “Z” maps to 0(mod26), this condition must be true for the generated solution to be valid.

Since there were 10 given letters and we used to first pair to make solutions for b1, there are 4 conditions left including the one just given that each of these possible values (m11,m12­,b­1) much pass in order for it to be a valid solution. This leaves us with these three final conditions:

This eliminates a lot of the possible solutions to the equation but remember that each of these coefficients can be any number from 0 to 25. This algorithm only returns some possible solutions to the equation as there will be multiple possibilities for each value that make it a valid solution but only one is correct. We will need additional requirements for an equation to be valid.

Since we are working in modulus 26, a matrix is invertible only if its determinant is relatively prime to 26. There are 12 integer numbers relatively prime to 26 that are at most 26, since every even number is not relatively prime to 26 and 13 is also a divisor. Remember before we stated that c1 and c2 did not depend on each other for now, but now they do. Now an additional requirement is imposed on the equation. If m11,m12, and b1 are solutions for c1, and m21,m­22, and b­2 are solutions for c2, then now the determinant of the matrix coefficients must be relatively prime to 26.

The coefficients on the matrix coefficients from each previous iteration now must fit the condition that:

This finally gives us our encoding matrix, and the encoding vector

Now that we have the encoding matrix, we can decode the parts of the message that were not given to us. First recall from earlier that the Affine Diagraph Cipher uses this equation to encode the plain text *p* to the cipher text *c*.

In order to decode the message, we must multiple both sides by the inverse of the enciphering matrix to both sides of the equation to obtain a solution for the plain text.

By taking the inverse of the matrix we obtained we have that

Now we have a way to solve for the plain text *p*, through only the cipher text, since M­-1 and b are fixed. We arrive at this formula for decoding the cipher text into plain text:

Now that we have computer friendly equations for the plain text, we can take the ciphered text and input them into the equation as pairs. We then finally obtain the original decrypted message.

“Archimedes like Plato held that it was undesirable for a philosopher to seek the results of science to any practical use but in fact he did introduce a large number of inventions. The stories of the detection of the fraudulent gold smith and of the use of burning lasses to destroy the ships of the roman blockading squadron will recur to most readers. Perhaps it is not as well known that Hiero who had built ships so large that he could not launch it off the slips applied to Archimedes the difficulty was overcome by means of an apparatus of cog wheels worked by an endless screw, but we are not told exactly how the machine was used it is said that it was on this occasion in acknowledging the compliments of Hiero that Archimedes made the well known remark that had he but a fixed fulcrum could move the earth.”