Math 312 Portfolio

Nathan Wichman
C. Wells

Winter 2019

Contents

Part I

Discussion of Course Grade

This course has encouraged me to alter my technical thinking and communication having to deal with representations of data, encryption, and security. There are a lot of techniques that I have developed over this semester including a deeper understanding of topics, exploration of material, and communication of material. I believe my development over this course merits a B.

Industry, Initiative, and Independence I have shown a foundation of understanding in many problems shown in this document, including <++>, <++>, and <++>. These are problems that I completed correctly and express a breadth of knowledge. I demonstrated an ability to complete problems independently in <++> and <++>. Furthermore, I expressed an ability to explore in the <++> and <++>. I demonstrated a variety of proof methods, including <++>, <++>, <++>, and <++>. My foundation of knowledge and independence should justify a B+.

Curiosity, Conjecturing, and Connections I showed exploration and curiosity in <++> by looking for reasons why <++>. I also showed an ability to explore in the <++>. I showed an ability to create connections between topics and conjectures in my exploration of <++>. Another example of exploration is in <++> where I recognized several patterns in order to gain more knowledge about the problem. I revisit past work in my reflections of <++> and <++>. I recognized <++> as an opportunity in my <++> on the problem. I expressed an infrequent amount of errors in problems <++>, <++>, and <++> in Assessment 2 where I correctly completed these problems. I believe this merits a B+.

Communication I have shown an ability to write clear well-reasoned, and well-organized papers, as well as clear, correct, well-organized mathematical arguments. I am particularly proud of <++>, the <++> and my discussion of <++>. I have presented polished work in <++> and <++>. I have also been able to communicate my work with other students as is explained in <++>. My communications skills should therefore justify a B.

Revisiting, Reflection, and Revising I learned to revisit my work often, reflecting on progress, revising computations and clarifying explanations, and extending existing work. In particular, the progress I made in <++> from the beginning of the semester to the end shows strong evidence of my ability to learn from previous work. I treated obstacles as learning opportunities, as well. The frustration I initially felt with the Vigènere cipher led me to a much deeper understanding of multi-alphabet ciphers, as shown in <++>. My performance in this area justifies an A-.

Part II

Supporting Evidence

1 High Level Concepts Learned

1.1 Overview

This section describes the more abstract concepts I have learned during the semester. That includes course textbook readings and class knowledge. This section does not go into depth on any specific ciphers but instead inspects the more general and abstract concepts I have gleaned throughout this class.

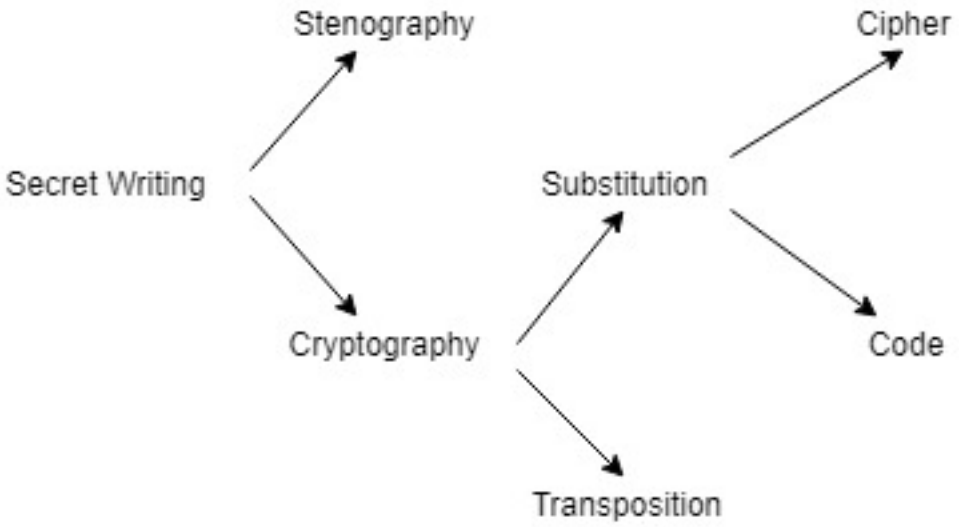
1.2 Chapter 1: The Cipher of Mary Queen of Scots

From reading chapter 1 of The Code Book: the Science of Secrecy from Ancient Egypt to Quantum Cryptography I learned the difference between stenography and cryptography.

Stenography is secret communication achieved by hiding the existence of a message. One of stenography's weaknesses is that if the secret message happens to be intercepted, the meaning of the message is discovered at once by the interceptor.Examples described in the book of stenography include points in history where a Stenographer shaved the head of their servant, wrote a message on the back of his head, and waited for the hair to grow back. After that, the servant was sent to the recipient, who in turn shaved their head to reveal the message. Another example is where hard boiled eggs were painted with a special ink that seeped into the shell without leaving a mark on it. When received, the egg could be peeled and the message would be stained into the egg itself. A final example is when Mary Queen of Scots received messages hidden within a barrels.

Cryptography involves hiding a messages meaning, not necessarily its existence. Cryptography is considered more powerful, because it does not allow for interceptors to understand the message. Intercepting stenography results in the recipient not receiving knowledge and the attacker receiving that knowledge. Cryptography that is intercepted only results in the receiver not receiving the message, as the attacker cannot understand the message without some sort of cryptography.

Two Branches of Cryptography There are two main branches of cryptography. Transposition and Substitution. Transposition involves moving or scrambling the letters or symbols of a message, similar to an anagram. Transposition does not add any new ones. Examples are Rail Fence Ciphers, Columnar Transposition, and the ADFGVX Cipher (which includes Columnar Transposition). The second branch of Cryptography is Substitution. This involves changing the symbols or letters of the plain text to other symbols or letters. Examples include One Time Pad, and the Vigenere Cipher. Substitution ciphers are mathematical functions by definition. They take in a domain (plain text) that maps to the same co-domain (cipher text) every time.



This diagram was in the book, I found it strange though that Transposition Ciphers are mentioned but there is no branch shown in this diagram for Transposition Ciphers.

Code vs Cipher Ciphers are substitutions at the level of letters. Individual characters are replaced for other characters. Codes are substitutions at the level of words or phrases. Entire blocks of letters or symbols are replaced for other blocks of letters and symbols. These strings are called code words.

Nomenclatures are a system of encryption that mixes ciphers and codes. Most of the message is encrypted by a cipher alphabet/s while a limited number of code words are

used to replace selected words or phrases. Mary Queen of Scots cipher was an example of a nomenclature.

Frequency Analysis is a common method of decryption ciphers without knowing the cipher's key. Generally a long text of the language the plain text of the cipher is in is required, unless the letter's frequency and patterns are already known. The letters are ranked from the most common to the least common within the language and the cipher text. Then, starting with the most frequent letters, such as 'e' in English, the cipher text letters are replaced by the English letters of similar frequency. In addition, common pairs of letters or other patterns can be noticed, such as 'ee' and 'qu' being common in English. It is not a sure way to decipher, but it is a good place to start with mono-alphabetical ciphers.

Nulls are symbols or letters that are added into the cipher text which actually hold no meaning at all. Their purpose is solely to confuse frequency analysis. For example, by adding many meaningless 'zz's into the cipher text, English frequency analysis would most likely assign 'z' = 'e', when in reality 'z' means nothing. Nulls are a further method of protecting the secrecy of the message from interceptors.

1.3 Chapter 2: Le Chiffre Indechiffrable

A Breakthrough in Cryptography The Vigenere Cipher became the most powerful cipher in the world and was considered unbreakable for hundreds of years. It involved 26 unique cipher alphabets, all one Caesar Shift from each other. A word or phrase could be used as the key. To encrypt/decypt, one would cycle through each letter of the key and encrypt the plain text letter in the row that's first letter was the same as the current letter of the key. This created an incredible secure cipher because multiple symbols represented the same plain text letter and multiple plain text letters could be represented by the same cipher text letter. This through off frequency analysis for generations.

Mono-alphabetic Substitution is substitution where only one Cipher alphabet is used.

Poly-alphabetic Substitution is substitution where two or more Cipher alphabets are used, such as the Vigenere Cipher's 26.

Homophonic Substitution is a process where each letter of the plain text can be replaced by several cipher text symbols in an attempt to throw off frequency analysis. The number of cipher symbols a plain text letter gets depends on its frequency. For example, a letter that had six percent frequency might be represented by six different letters. Any of those letters could be used instead of it. This results in all letters of the cipher text having around a one percent frequency. Despite having more letters than the plain text alphabet, these ciphers are still mono-alphabetic, as they just extend the alphabet instead of creating a distinctly separate one.

Charles Babbage Cracks the Vigenere Cipher Charles Babbage invented the first computer, the speedometer, and the cow catcher, among other inventions. In addition, he cracked the seemingly impossible Vigenere Cipher without a key. By looking for repeated sequences, he laid out the factors of their intervals. Next he looked for common factors between different sequences. In this way, he was able to discover which rows of the Vigenere Square were used. After that, it was simple frequency analysis.

2 In-Class Assessments

There have been no assessments yet.

3 Class Activities

3.1 Simple Substitution Ciphers

The following Cryptogram "Crypto Quip" puzzle was taken from `http://www.wordles.com/getcrypto.aspx`, downloaded Friday, January 6, 2017 at 2:30 P.M. (EST)

K Q T K E U U F E W D J W K Q

R T F A M D W K W L J U I R O

O P H W M W K P R A H P P R O W L - D F I M K R P O.

Hint: K=t

This cryptogram is a simple substitution cipher. That is, each letter has been replaced by another every time it occurs. From the hint, “Q=b,” we know that every instance of “Q” in this puzzle represents the letter “b” in the solution.

Using punctuation, small words, and letter frequency, we were able to quickly solve the puzzle.

A translation table and the solution to the puzzle are given below.

3.1.1 Using Frequency Analysis

By using frequency analysis, we were able to solve this cryptogram together as a class. Starting with the first word of the Cipher text, KQTK, we were given K = ’t’, so I thought it probable that Q = ’h’ as there are several common four letter English words that begin in Th and end in t, such as "that" and this".

As "UU" and "PP" appear in the cipher text, both in the middle of four letter words, I guessed that one was ’o’ and the other ’e’ as those letters appear together most often in English. ’e’ is the most common English letter, and so as ’P’ occurred far more often than ’U’, I penciled in ’P’ as ’e’.

By following frequency analysis as a group, replacing frequent cipher letters with plain text letters of similar frequency in English, we were able to decipher the message.

The deciphered message read: That poor pig with laryngitis would definitely feel disgruntled.

CODE	A	B	C	D	E	F	G	H	I	J	K	L	M
clear	y			g	p	r		f	u	w	t	s	n

CODE	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
clear		d	e	h	l		a	o		i			

Table 1: Translation Table

3.1.2 Notes

It may be noted that although we successfully deciphered the plain text message, we did not uncover the entire cipher alphabet. This is not a problem though, as our goal was not to know the complete cipher alphabet but the message. Unfortunately, if we were to intercept other messages encrypted with this same cipher, there is a possibility that we would have to use frequency analysis and guesswork on the remaining letters. That would most likely be easy work though, as we already know 17 cipher letter’s plain text identities.

3.1.3 Possible Improvements to this Cipher

There are many possible improvements to this cipher. In its current state it is extremely weak, as it only requires basic frequency analysis, which was mastered long ago and published by the Arab world.

The first strategy to employ needs to be confusing further frequency analysis. One good method would be to add nulls into the cipher text. In other words, pepper in meaningless characters to confuse frequency analysis. Another method would be to turn the cipher homophonic. This means allowing more possible letters to represent plain text letters with higher frequencies. For example, if 'e' appears 11 percent in English dictionaries, perhaps 11 symbols should represent it, which we would use at random to represent 'e'. By having at least 100 symbols in our cipher alphabet, we could ensure that each cipher text letter does not have a frequency of greater than 1 percent.

A final method would be to look for common patterns of letters, such as 'ee', and replace them with code words for those common phrases. For example, 'ee' could become 'z' or '1'. Now frequency analysis would not be able to locate common patters of 'ee' and deduce the single 'e's.

3.2 Using a One-Time Pad

The idea of a *one-time pad* is similar in some ways to a simple substitution cipher, but differs in some important ways.

Using the translation key in Table 2, we encrypted the first half of the quote

> *Tradition becomes our security, and . . .*

to get

The second half of the quote (shown below) had already been encrypted using the key in Table 3. We decrypted it to get the clear text shown below the cipher text.

> Cipher text: UFIA OFI KSAV SY YIMWDI SO SY SA VIMPE.
> Clear text:

Next, <My Partner> and I used the key shown in Table 4 to pass notes to each other. She passed me the cipher text <.....>, which I decrypted to get

I passed her the phrase "<.....>," which I had encrypted as <.....>.

Some important differences advantages and disadvantages of using a one-time pad versus a single substitution key are

Encryption Key

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
I	Z	T	D	A	M	C	P	H	X	B	J	U	O	Y	G	R	W	L	N	E	V	F	Q	S	K

Decryption Key

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
e	k	g	d	u	w	p	i	a	l	z	s	f	t	n	h	x	q	y	c	m	v	r	j	o	b

Table 2: One-Time Pad, “Page 1”

Encryption Key

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
P	J	M	V	I	B	X	F	S	L	G	Q	K	A	R	Z	N	D	Y	O	W	C	U	H	E	T

Decryption Key

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	f	v	r	y	h	k	x	e	b	m	j	c	q	t	a	l	o	i	z	w	d	u	g	s	p

Table 3: One-Time Pad, “Page 2”

4 C-Sharp Class To Automate Frequency Analysis

using System;

namespace Cryptography class FrequencyAnalyzer private int[] charHashMap; //97 - 122 private int total;

public FrequencyAnalyzer() this.charHashMap = new int[26]; this.total = 0;

public void assignFrequencies(String text) int index; foreach(char letter in text) if (letter >= 97 letter <= 122) index = letter - 97; charHashMap[index]++; else Console.WriteLine("Unrecognized letter: " + letter);

findTotalNumberOfLetters(); printFrequencyTable();

public int findTotalNumberOfLetters() foreach (int integer in charHashMap) total += integer;

return total;

public void printFrequencyTable() double percentage; for (int i = 97; i < 123; i++) percentage = (((charHashMap[i - 97])*100) / total); Console.Write(Convert.ToChar(i)); Console.WriteLine(": " + percentage + "

static void Main(string[] args) FrequencyAnalyzer frequencyAnalyzer = new FrequencyAnalyzer(); frequencyAnalyzer.assignFrequencies("Hello World");

Console.ReadKey();

Encryption Key

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	P	F	C	W	V	E	M	G	U	H	D	Q	B	L	X	K	S	T	O	Y	I	J	N	R	A

Decryption Key

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
z	n	d	l	g	c	i	k	v	w	q	o	h	x	t	b	m	y	r	s	j	f	e	p	u	a

Table 4: One-Time Pad, “Page 3”