A1\_Report  
Tyler Janvrin

Matrix Algebra

1.

By row 1:  
2x = 8  
x = 4

By row 2:  
2y=6  
y=3

2.

a+b = 5, ab = 6  
Therefore a=2, b=3

3.

Determinant:

Multiply each cofactor Aij = (–1)i+j Mij, where M is the minor of aij, by a row or column of the matrix.

[2 -3 -2]

[1 -1 -1]

[0 2 1]

= -1

Inverse:

[1 -1 1]

[-1 2 0]

[2 -4 1]

4.

A + 3X = I3  
3X = I3 – A  
X = 1/3 (I3 – A)

X = 1/3 \* [-3 3 -6]  
[-3 18 6]  
[3 -12 18]

X = [-1 1 -2]  
[-1 6 2]  
[1 -4 6]

4.

A^2 = [9 8 8] [8 9 8] [8 8 9]

4A = [4 8 8] [8 4 8] [8 8 4]

5I = [5 0 0] [0 5 0] [0 0 5]

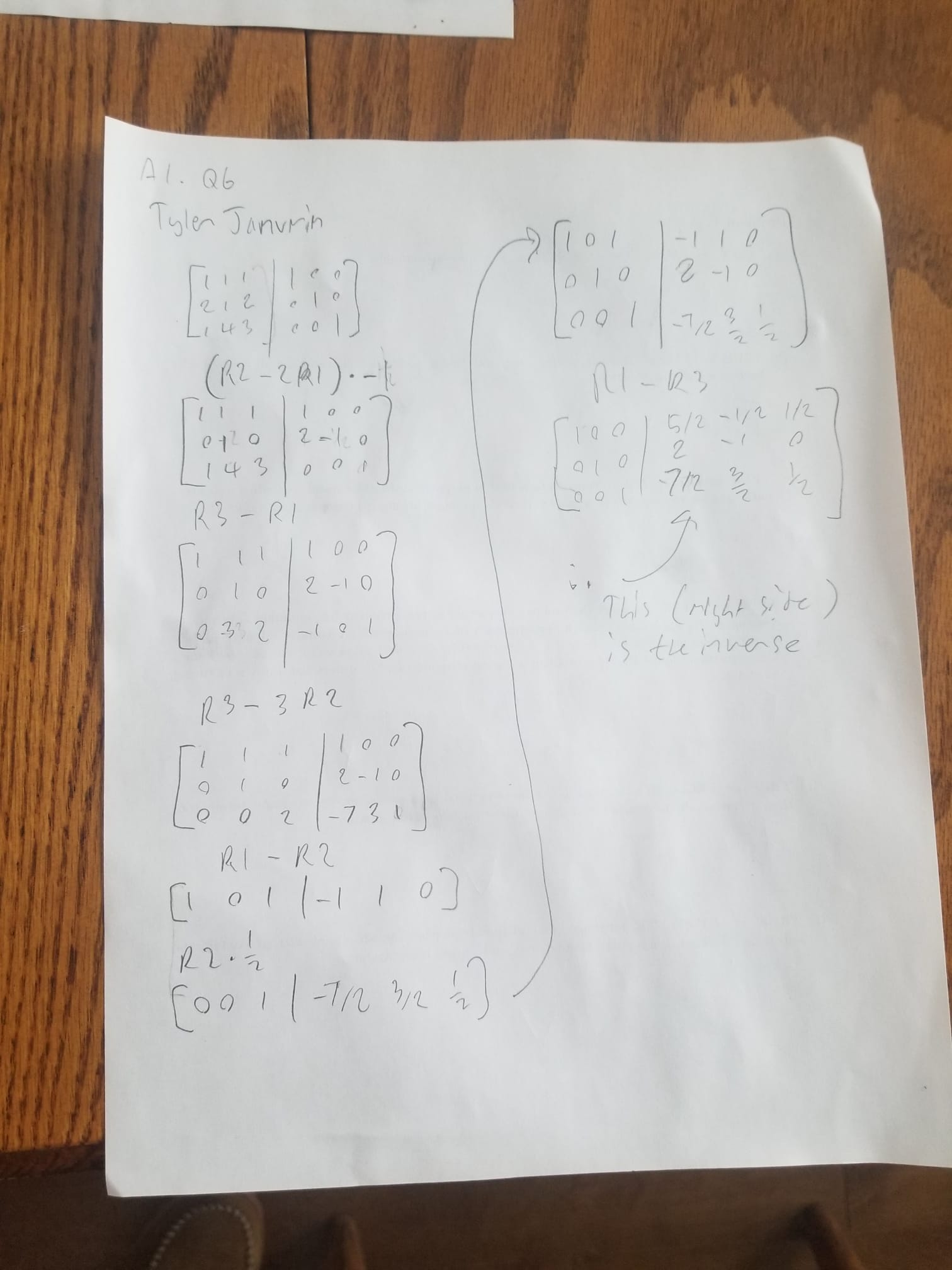
Obviously, then, A^2 – 4A – 5I = 0  
Just look at at!

Finding A^-1

A^2 – 4A – 5I = 0  
A^2 – 4A = 5I  
A(A-4I) = 5I  
A \* 1/5(A-4I) = I

Therefore, 1/5(A-4I) = A-1 = [-3/5 2/5 2/5][2/5 -3/5 2/5][2/5 2/5 -3/5]

6.



Since A^-1 = [5/2 -1/2 1/2] [2 -1 0] [7/2 3/2 ½], and since we have

Ax = b  
A^-1Ax = A^-1b  
x = A^-1b

Therefore, a quick matrix multiplication gives:  
x = [1] [-1] [1]

Substitution Ciphers:

1.  
JUHDWMRE  
KVIEXNSF  
LWJFYMTG  
MXKGZNUH  
NYLHAOVI  
OZMIBPWJ  
PANJCQXK  
QBOKDRYL

…  
  
Actually, wait. There’s a faster way  
  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

JKLMNOPQRSTUVWXYZABCDEF**G**HI  
UVWXYZABCDEFGHIJKLMNOPQ**R**ST  
HIJKLMNOPQRSTUVWXYZABCD**E**FG  
DEFGHIJKLMNOPQRSTUVWXYZ**A**BC  
WXYZABCDEFGHIJKLMNOPQRS**T**UV  
MNOPQRSTUVWXYZABCDEFGHI**J**KL  
RSTUVWXYZABCDEFGHIJKLMN**O**PQ  
EFGHIJKLMNOPQRSTUVWXYZA**B**CD

The cipher is a +3 shift, and the message text is GREATJOB

2.

Not sure how to do this one… maybe he’ll go over it in class?

3.

Ooh. This one’s tricky.

Ciphertext 1  
UFKTLHTRLVXCETSGKSPTCHTFGYYEISPZLVTZNFTTKHJVUDKZFWPDFHJVSH  
MCWBRDVOPRBPMVGGMABHKTYAEOPUQRTDGZQRAOPXGCZAGRLLAWNVG  
IBGFZDUBQWCRIHGGVUWXFGNCPKSIFGCZDQCGIBQCCJNTGVYCXGTNRRXH  
BJRQHDMTFAZXHGURWXWPKCGXGVIYIXGCICHMWNCFXZVCEBIASOFPIZOIV  
PPMSURPTGCVECPKZANFTKSVYCNPSTVRWKSGPCPKGCXMNHIYFLSXFYYC  
IASTNCPKSULDUXFKEEUKCOFVNFCTFLMXBQGFDUWEJWCWFQDCDKRQNC  
XNGVJNTEZVYYIJIKTIARKKKFPS

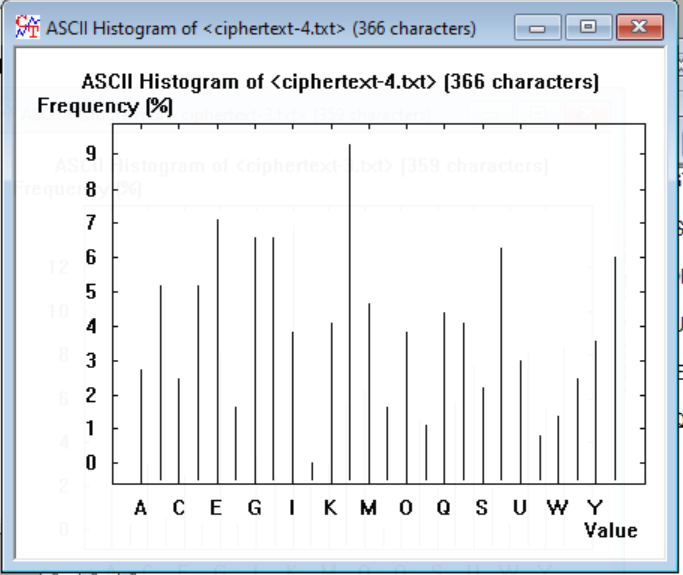
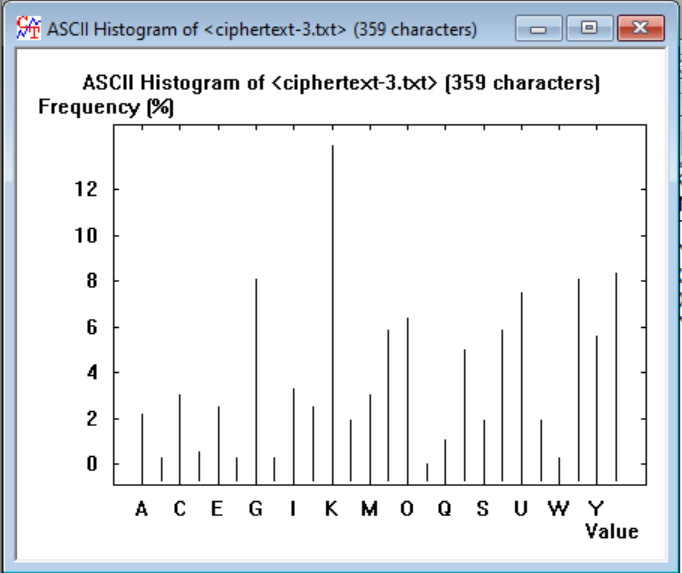
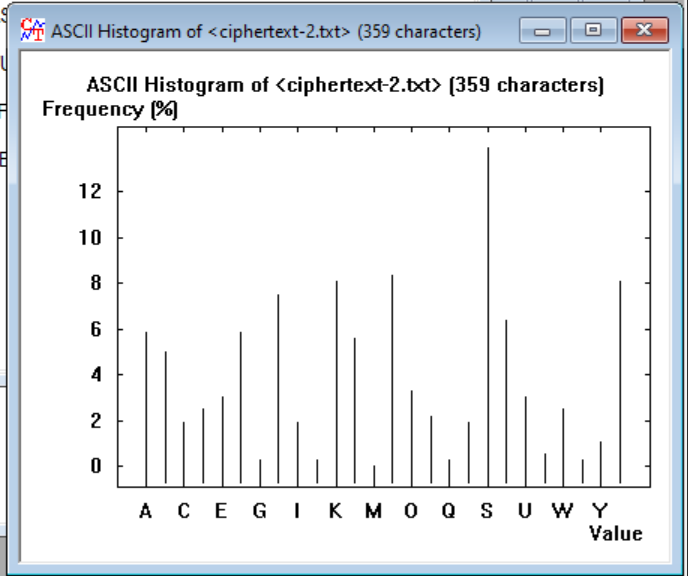
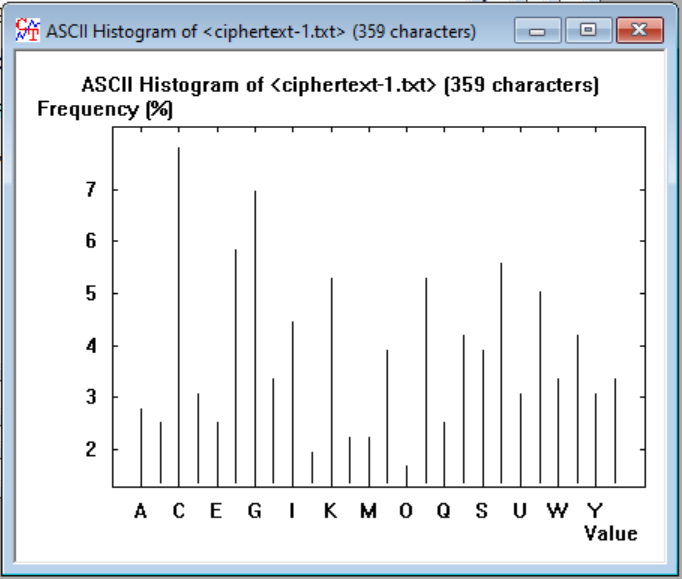
Ciphertext 2  
LHCSLNKZFESHOOPKKSFOSLZKSAZIISFTFEZBBHQSKNASUHKBDRKHCNASP  
LNHPYNHOZFZDZNASIHBTNTOZBBZFDLOZISTLOAZFETFECSZFUATBSTNTLD  
TRRTOPBNNHLSSUASKSUSZKSEHTFEIHBTNTOZBBWZLNASTFRBZNTHFAZLL  
YWKHOYSNSDNASTFNSKSLNKZNSLZKSLNTBBATEAZFDNASCHKNEZESKZNS  
LZKSFHNFSZKBWUASKSNASWUSKSNAKSSWSZKLZEHWHPUHFDSKUASNAS  
KUSZKSLPRRSKTFERKHCHVWCHKHFVSFHIAHGTOLWFDKHCSHKDHUSTPLN  
LISBBNAZNJPTOYBWUTNAZX

Ciphertext 3  
YUSKYZXGTMKUIIAXXKTIKYGXKNGVVKTOTMGRRUBKXZNKCUXRJL  
XUSZNKAYZUAQZUIGTGJGZNKVUROZOIGRRGTJYIGVKOYINGTMOT  
MSKGTCNORKOZOYJOLLOIARZZUYKKCNKXKCKGXKMUOTMVUROZ  
OIGRREGYZNKOTLRGZOUTNGYYQEXUIQKZKJZNKOTZKXKYZXGZK  
YGXKYZORRNOMNGTJZNKSUXZMGMKXGZKYGXKTUZTKGXRECNK  
XKZNKECKXKZNXKKEKGXYGMUEUACUTJKXCNKZNKXCKGXKYALL  
KXOTMLXUSUDESUXUTDKTUVNUHOIYETJXUSKUXJUCKOAYZYVK  
RRZNGZWAOIQRECOZNGF

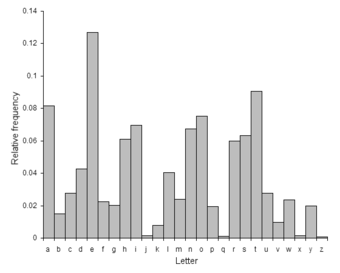
Ciphertext 4  
BKLGTUAZMHILYPASYQTLKZDTZAGICVQDOHMHRMMKQGTEIGXNTQHSYLL  
UIGFTBLSMBLRZMZGCFEDQKMEBDYRMMRKHDSCVGDDSGZMHHOMVGRW  
ZIDQLEBDBEDBWBHASQEBLTDHQIGTLQHZAGHXOMHXKOEBERZOQORCUF  
EGDWHMRBEKOGZBPDPCAKYLDELESIGHOELTLTUAZELUCTLTUEONEDHGZ  
KHFEGLLYUEUMLTRUDTZAHLLBLHZAORZNLTLEIGZXLTLEEZIQIRGRCTUMXB  
MBXNKHLTZNLEIGZQGRTLTFBWTHYEMHTZKNXYAOLYKOQIOKWDXIDYBCKH  
YLLGLYIKQHGBTUDCLQQEGZERBGSPORXHFEZY

-

The first thing I’ll do is take a histogram of all 4 ciphertexts.



Let’s compare these to the English alphabet (image taken from https://www3.nd.edu/~busiforc/handouts/cryptography/letterfrequencies.html):



Looking at these histograms, it looks like ciphertext 3 could be the English alphabet shifted so that E = K ( a shift of +6). Applying that shift reversed (-6) to the cipher text gives us:

SOMESTRANGEOCCURRENCESAREHAPPENINGALLOVERTHEWORLDF

ROMTHEUSTOUKTOCANADATHEPOLITICALLANDSCAPEISCHANGIN

GMEANWHILEITISDIFFICULTTOSEEWHEREWEAREGOINGPOLIT

ICALLYASTHEINFLATIONHASSKYROCKETEDTHEINTERESTRATE

SARESTILLHIGHANDTHEMORTGAGERATESARENOTNEARLYWHE

RETHEYWERETHREEYEARSAGOYOUWONDERWHETHERWEARESUFF

ERINGFROMOXYMORONXENOPHOBICSYNDROMEORDOWEIUSTSPE

LLTHATQUICKLYWITHAZ

-

This looks like the plaintext! Therefore, ciphertext 3 is encrypted using the Caesar cipher. Now that we have the plaintext, we can use it to find the keys for the other three.

-

I tried ciphertext 1 first. Subtracting the plaintext from the ciphertext for 1 gives:

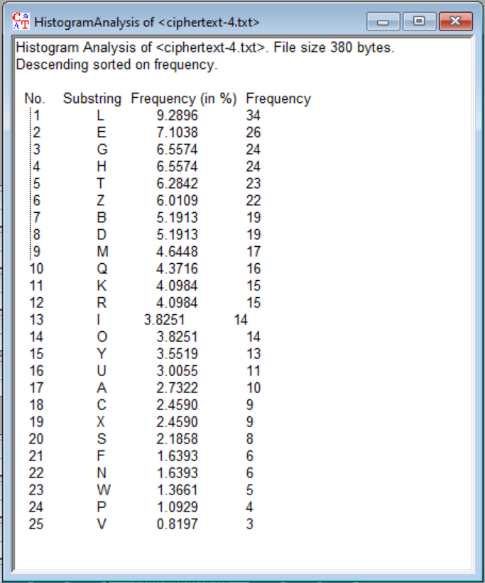
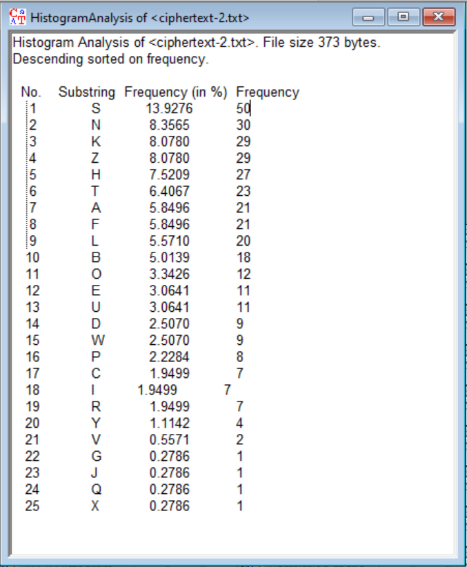
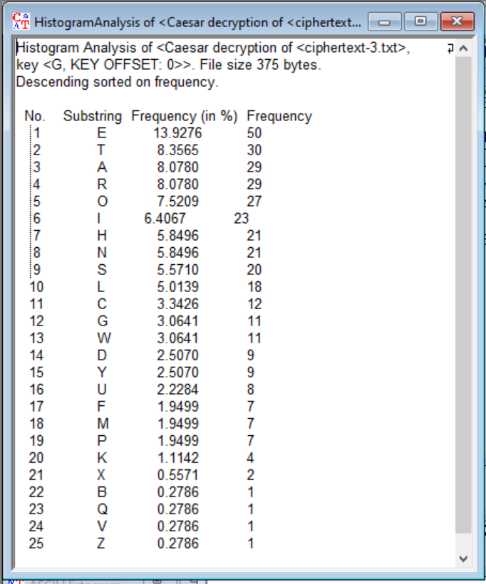
CRYPTOCRYPTOCRYPTOCRYPTOCRYPTOCRYPTOCRYPTO

Which I think is a pretty good sign that ciphertext 1 is Vigenère, and the key is CRYPTO.

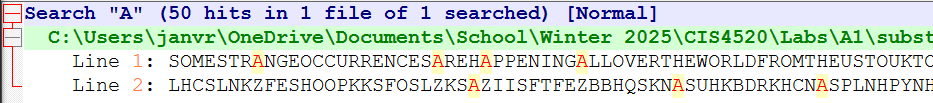
So, we now have: CT1 = Vigenère, CT2 = ?, CT3 = Caesar, CT4 = ?

-

To find the substitution cipher, we can use E’s. Since we know how many E’s there are in the plaintext, we can compare the n-grams of CT2 and CT4 to that to see if they match.



Looking at this, we can see that the letter frequencies of the of the plaintext (left box) and ciphertext 2 (middle box) are the same, which indicates that CT2 was encrypted using a substitution cipher. The key to this cipher can be found by going through the plaintext and ciphertext and finding matches for each key. I did this by lining them up in a text file, and CTRL-Fing to find a match for each character.



Plaintext->Ciphertext

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
ZGODSREAT\_YBCFHIJKLNPQUVWX

J doesn’t appear in the original text, but since it’s the only one that doesn’t appear, we can guess that it must map to M.

Therefore, the final key must be:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
ZGODSREATMYBCFHIJKLNPQUVWX

Checking this key against the ciphertext gives the plaintext.

-

Now, we have CT1 = Vigenere, CT2 = Substitution, CT3 = Caesar. By process of elimination, CT4 must be the Playfair cipher.

I’ll solve that one later.