CIS 3362 Homework #3: Vigenere Code Breaking, Playfair, Hill, ADFGVX
Due: Check WebCourses for the due date.

Directions: To be done in pairs. If you can't find someone to work with, you must submit individually. Either way, first join a group in the Group Set HW3-Groups. Please figure out the correct way to submit. About 20 of you failed to do so on Homework #2. Ask one of the many(about 100)classmates who correctly figured out how to do so.

1)Decode the following message, which was encrypted using the **Vigenere** cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

oswelcbxoemfinzyipipqvjaiwpdmpipvusgtzgieymqfenoqcgqlmwzsuwsqstkekmesecgigzqvtwariu
gdbpcsiawmbmioekjyspxjmlvvuqvikictdaeeexhlxkbxztifxtjypqfbizoxecquwupxjmiteitnglulfrcjhk
aiymsvxizrcvndepkysepkstalvciawieqeoiijaoyxvmascfvahpvgbwltijdetwkviomjnisdeimxuwkfede
lgrdiswulidqgahhkvjwjfwvbdaicmcofxjiialvsiwtpnjthtijdelrfqizwgfgiqmetdjekjsnhmntqlhvtgrtfgl
xuqvtwarivpglirohtsiewcaieuwoqxjmeymqfaiwpdmspwtmssphkvblwjbkeeaq

In order to decode this message, we first look at the index of coincidence for several possible keyword lengths. I used Cryptool in order to get these values. I started at 6 because most words are around 6 letters:

Six: Index 0: 4.52 Index 1: 4.87 Index 2: 3.33 Index 3: 5.13 Index 4: 5.17 Index 5: 4.38
Seven: Index 0: 4.29 Index 1: 3.69 Index 2: 5.2 Index 3: 4.35 Index 4: 5.56 Index 5: 4.11 Index 6: 4.17
Eight: Index 0: 5.09 Index 1: 5.41 Index 2: 4.31 Index 3: 4.62 Index 4: 5.64 Index 5: 4.73 Index 6: 3.26 Index 7: 4.08
Nine: Index 0: 5.95 Index 1: 4.94 Index 2: 3.53 Index 3: 4.54 Index 4: 5.75 Index 5: 5.35 Index 6: 4.04 Index 7: 3.63 Index 8: 4.33
Ten: Index 0: 4.26 Index 1: 5.36 Index 2: 4.63 Index 3: 3.46 Index 4: 5.12 Index 5: 3.71 Index 6: 3.97 Index 7: 4.74 Index 8: 4.74 Index 9: 4.61
Eleven: Index 0: 8.85 Index 1: 7.35 Index 2: 7.2 Index 3: 6.15 Index 4: 6.3 Index 5: 6.75 Index 6: 6.98 Index 7: 6.5 Index 8: 6.98 Index 9: 7.77 Index 10: 7.46
Twelve: Index 0: 5.16 Index 1: 7.3 Index 2: 3.03 Index 3: 6.59 Index 4: 6.06 Index 5: 4.16 Index 6: 4.35 Index 7: 3.97 Index 8: 3.4 Index 9: 4.73 Index 10: 4.35 Index 11: 4.73

After reaching twelve, the values started to drop which indicated that our keyword length is most likely eleven. Doing this, we then take each letter of each bin to see if we can find the shift of each of the letters as each letter in the same bin array position should be the same as the others. I then took 3 of the bins so try to calculate the shift from these:

oswelcbxoem
finzyipipqv
jaiwpdmpipv

I then used my program from the last assignment, vigenere.c to see if I could find any plaintext words from characters that are in the array. I was able to find the word “Now” in the first bin via the output: {
Key: beat
Decoded Text: NOWLKYBENAM

Key: beautiful
Decoded Text: NOWKSUWDDDI
}

This indicated to me that the first 3 shifts would be 1, 14, and 0. By doing this, I could figure the other strings to be “een” and “iwi”. “Een” could be quite a few words, but “iwi” could only map to a few. Ignoring the I, I assumed that “wi” would map to “will”. Upon shifting the rest of the message, I would that the first statement became “Nowth”. Th is a common beginning for many words as well, but looking at our second bin after the shift I found it now became “eenou”. “Enou” could only map to a few words, one being “Enough”. After shifting the rest of the letters, I found that the other bins became “Nowthat” and “Iwillbe”. Judging from the remaining four letters, these words would have to be four letter words, with the exception of “xoem”, as there is still an extra “e” before enough. I also saw that the last two letters of bin 2 and 3 were “v”, which means they ended similarly. I then brute forced the shifts by hand to find that they were “time” and “able”. This made the final shift on the first bin “ihav”. Adding the extra e from the original bin made this “I have”.

nowthatihav
eenoughtime
Iwillbeable

I then converted all of the shifts (Ie; 1, 14, 11, etc…) and was able to get the assumed keyword “BEALECIPHER”. I then added this to my “dictionary.txt” (swapped our the 3rd to last word) and got the following message:
nowthatihaveenoughtimeiwillbeabletogiveaprizeandmaybeifyoulookedatlastyearsmessagesyoullrealizethatiusethewordprizealotandthatitisprettyuniqueintermsofitsletterfrequencydistributionanywayjustlikethebealecipheriwonttellyouwheretheprizeisinthismessageinsteadthejobofthismessageisjusttotellyouthattherewillbeaprizeanditsspecificlocationwillbedescribedinmessagethreeandthecontentsoftheprizewillbedisclosedinmessagetwo

2)Decode the following message, which was encrypted using the **Vigenere** cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

perpbawtgvjatufcjaclhuikvtemponyimhiygiqssjmzkebzmvvjwfsdifcktginvelhzmuijiiwfwvwwksb
wyxzhiqgvdjxfphvuirwxcccbxzmsflqgqmujjeamjhvmmkufnxznmqblujigmniivqghiydvighjgvnph
swyiszxolmdvalohykyzxsgcijbxbkipkpxaphvpqliqjfjmtzmckjohcezfiqlooctvjnfsckfnkcnkufjt

Again, to start this process I used Cryptool to find the length of the keyword by finding the indexes of coincidence, starting at 6:

Six: Index 0: 3.29 Index 1: 4.63 Index 2: 4.39 Index 3: 3.41 Index 4: 4.14 Index 5: 5.12

Seven: Index 0: 4.7 Index 1: 6.21 Index 2: 9.57 Index 3: 7.39 Index 4: 5.88 Index 5: 7.39 Index 6: 6.41

Eight: Index 0: 3.87 Index 1: 4.3 Index 2: 4.73 Index 3: 3.9 Index 4: 2.75 Index 5: 4.13 Index 6: 3.44 Index 7: 3.21

Luckily, it appears that 7 was the best candidate almost immediately, with all the indexes being very high. I then took the bins of length 7:

perpbaw
tgvjatu
fcjaclh
Uikvtem

I then ran Vignere.c once again to see if the dictionary file would catch anything similar. After analyzing the output, I found that the anticipated keyword “Marriage” contained seven letters and prompted some legitimate values from our bins 2, 3 and 4. I then got the output for bin 1 as well:
{
Bin 2
Key: marriage
Decoded Text: HGESSTO
}

{
Bin 3
Key: marriage

Decoded Text: TCSJULB
}

Bin 4{
Bin 4
Key: marriage
Decoded Text: IITELEG
}

{
Bin 1
Key: marriage
Decoded Text: DEAYTAQ
}

What caught my eye about this word was in the fouth bin, as I spotted “ESS” because the last decoded phrase used “Message” a lot. This means that message probably lied within bin one and two. Knowing this, the shifts backwards would be “20” (G to M), “17”, (V to E), “18” (J to S), “18” (A to S), “8”(T to A), “14” (U to G), “1” (F to E). Because message is 7 characters, we found the key by all this shifts. “1” maps to B, “20” maps to U, “17” maps to R, “18” Maps to T, “8” maps to I and “14” maps to O. This makes the key BURRITO. I added this to my dictionary.txt once again, and decrypted the final message to the one found below:

okaythismessageisjusttotellyouwhattheprizeisitwillbesomecoolcashtendollarsapieceforeachgroup memberonedayiwilltellyouinclasswhyinevergetgiftcardsanymoreinthemeantimewhoeverbreaksm essagethreefirstenjoythemoneyisupposeallitsgoodforisaniceburritofromqdoba

3) Decode the following message, which was encrypted using the **Vigenere** cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

wykllivrvfhqxvccahppluahhiyhhmhftcaiwzyvfhljliymhiuzmifvozfoxcuirbhyohkiwpuodioclcudw
ykjyicvcbpckkcinrrlvjhrweklzcdeyjsiwftwlyrllcudlkvflavvryamhbtidsrknuaowyklzdrezavprbohn
aufahkdudgbhldeuvpsvflzpchknibgkknuawrlrxieilthflhksyrnrnuzhnbwahuyvkulpevzlnoawygjwe
qj

To start, I found the indexes of coincidence once again starting from 6:

Six: Index 0: 9.41 Index 1: 6.75 Index 2: 6.96 Index 3: 6.5 Index 4: 5.34 Index 5: 5.57

Seven: Index 0: 5.4 Index 1: 5.07 Index 2: 5.71 Index 3: 4.76 Index 4: 4.28 Index 5: 4.44 Index 6: 6.34

Eight: Index 0: 6.85 Index 1: 5.04 Index 2: 5.24 Index 3: 4.43 Index 4: 6.02 Index 5: 4.73 Index 6: 6.02 Index 7: 4.73

I noted that 6 looked frequent already, but I went back and found the IoC for 5 just to be sure:

Five: Index 0: 4.0 Index 1: 4.86 Index 2: 4.54 Index 3: 3.37 Index 4: 4.31

And it appears that Six was still the highest frequency.

I then got the first 3 bins again from the ciphertext of length 6:

wyklli
vrvfhq
xvccah

I then ran the first bin through Vigenere.c to see if I could find anything frequent. The only thing I was able to find that peaked my interest was that all words beginning with “DR” mapped to “TH”.
{Key: draw
Decoded Text: THKPIR

Key: dream
Decoded Text: THGLZF

key: drive
Decoded Text: THCQHF
}

This specifically peaked my interest as “That” or “The” could easily start a statement in any sentence. I started shifting each of the characters by “E” (or 4) as well and our three bins and assumed key turned into the following:

Key values: DRGXXX

THElli
SAPfhq
UEWcah

I immediately assumed that SAP could turn into SAPLING and attempted to shift the key, then realized sapling is seven letters. I then assumed that each of the remaining unknowns appeared like this so I wouldn’t make a mistake: THE _ LLI _ SAP _ FHQ _ UEW _ CAH _
I still felt alittle confused as nothing really appeared to map to a recognized phrase so I went back and got 2 more bins to see if anything would correlate before I attempted to try “that” in place of the:

MYFuah
ERShhm

This output made a bit more sense to me as “MYF___ERS could correlate to a few known words, with “MYFATHERS” being the first one that popped into mind. This means that UAH would need to shift to ATH. I immediately saw that H would shift to H, meaning that there is no shift at all. Our key would then become this: DRGXXA. Our current bins would also change to:

THEllI
SAPfhQ
UEWcaH
MYFuaH - We know UA probably maps to AT.
ERShhM

I then shifted U to A (20) and A to T(7). Shifting these characters would result in DRGUHA. This actually makes a ton of sense considering the previous messages and “MYFATHER” being in the plaintext we already decrypted. I then put the assumed key in our dictionary.txt file and found the following plaintext message:

Thereisaplaquewithmyfathersnameonititisbyhisformerofficeifyoulookbehindityouwillfindthepriz
ewhichtwogrouppartnerscansplitonceyoufinditpleaseletmeknowsothatothersdontgopokingaround
drmahalanobissofficethoughthatwouldbefunnyletmeknowofanyfunnystoriesifthathappens

4) You have intercepted a message encrypted with **Playfair** and know what the first few words of the message are. Break the rest of the message!

TrsrleciveidisorbsaevelеareuidsfmeaesfgelnrcoamsotptaiedfpptNqbelkdfftthtrdnorhumisvheieqea
emnrnmervmslkevecvkhyptpteaseOmaogpapalotfxsrabmhismlombytronsnsbicmlorecsr

The beginning of the plaintext is: "Here is a little secret".

HERE IS A LITQTLE SECRET IT IS BEST QTO COME TO CAMPUS BEFORE NINE AM TO FIND PARKING AND THEN USE THE QEXTRA TIME TO DO HOMEWORK IT IS A WIN WIN IN TERMS OF EFQFICIENCY REGARDLESQS OF WHEN YOUR CLASQSES ARE.

We left the padding character Q in for reference.

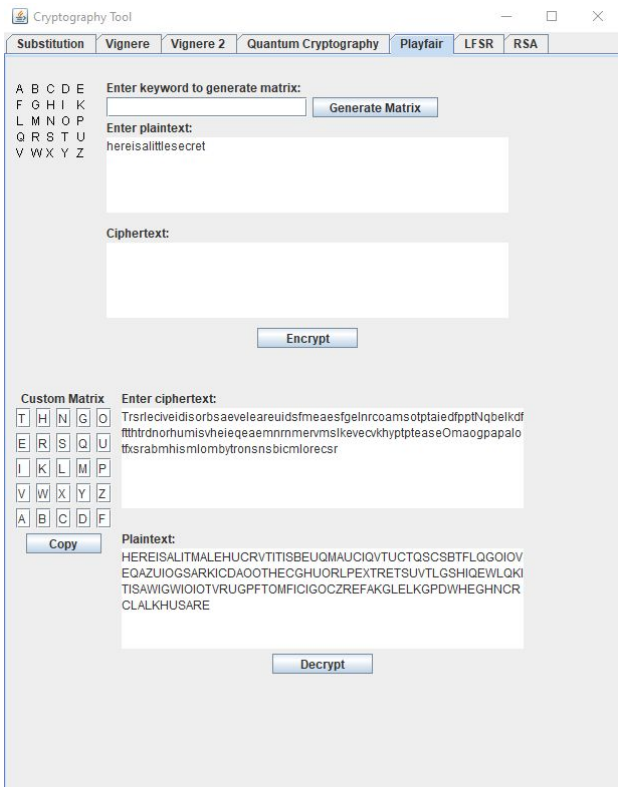

FIG 1

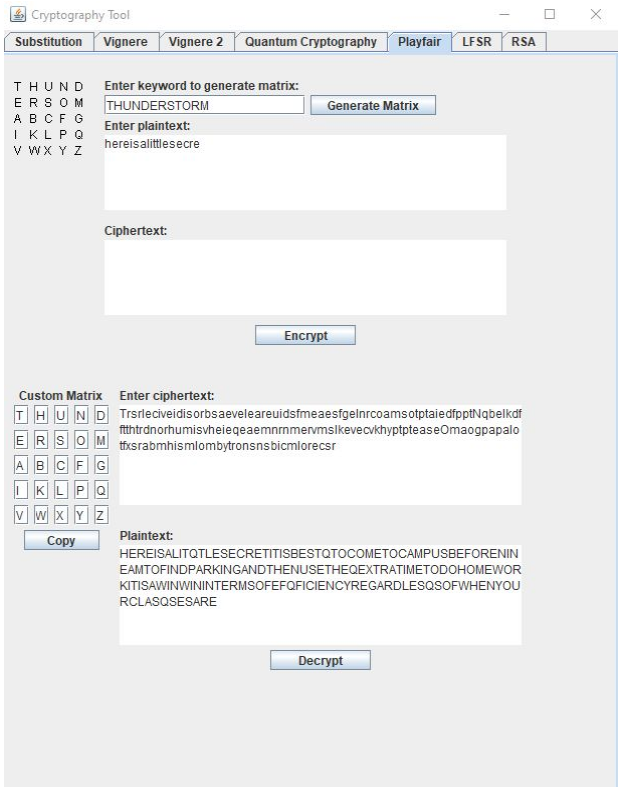

FIG 2

We started with the word “here”, mapping to “trsr”, and because ‘r’ maps to ‘e’, we thought it could be a box pairing (not vertical, or horizontal). So we made a box of four letters, and moved onto the word “is” which maps to “le”. Since we already had ‘e’ on the board, we saw where ‘s’ could fit and make sense and where ‘l’ maps to ‘i’. And we saw that making another box pairing was the only solution, so we put it to the bottom right of the first box. Then we moved onto the

next word which is “a”, but it cannot be by itself so we looked at “al” and it maps to “ci”. Since we already had ‘i’, we just added ‘c and ‘a’ to make another box pairing. Then we moved onto the next word “ittles” mapping to “veidis”. Since we already have ‘i’ and ‘t, we could place ‘v’ below in a row. 

We could guess that the bottom row is “vwxyz”. And the third row is “abc--” and the fourth row is ‘ikl--’. And examining the deciphered text so far shows that there is an extra letter in the middle of “little”. There is also a missing ‘t’ in the deciphered text. So we just plug in random letters to just try to make shift something and we use the most common letters to place at the top of the matrix. So we have fig 1, and we move the rows to make sense in alphabetical order. Switching the letters to make words in the decipher text lead to fig 2, and see the keyword taking up the first two rows and probably having repeat letters in the keyword. And we guessed it was thunderstorm(s).

5) Write some code to encrypt the following plaintext via the **Hill** cipher, using blocks of characters of size 4. The key to use is included below. Turn in your code as an attachment and in the text of your homework display the corresponding ciphertext.

$$\begin{bmatrix} 16 & 4 & 5 & 22 \\ 11 & 14 & 4 & 24 \\ 5 & 7 & 2 & 25 \\ 15 & 22 & 19 & 19 \end{bmatrix}$$

Plaintext: "jackandjillwentdownahilltofetchapailofwaterx"

Ciphertext: “kjnzfukujinbrkqknuqfzdyxfbrkjftuctcoqatkbbep”

Attached code

6) Encrypt the plain text shown below by hand using the **ADFGVX** cipher and the keyword, "CHAPEL" and the key square shown below:

Key Square:

k	3	g	7	v	i
u	a	q	d	m	2
y	l (letter L)	r	5	s	o (letter O)
4	0 (number)	b	z	8	e
p	j	x	n	h	6
c	9	t	f	1 (number)	w

Plaintext: "letusmeetat4pmat9270knightscircle"
Do not use any padding characters.