Fall 2024 CIS 3362 Homework #2 Solutions

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

```
kmpjynrjkdkckddmbkdzivvvkmowyerymtvmpkygpmctedzjkxkwyezivvni
gomdjyxrgyrknxycckinwyexkrxikskrjmrgyrklxigbirryckmgowyezivv
bkrrkgoyvvmxdnyxrjidnixdrfekdriygwyezivvnigorjkpyxxkdtygoigb
gyrkskxwpvydkrycwynnipkrjkxkidmdrmphynlyyhdnxyccwomomgooxoer
rygrjmrmxklkigbbiskgmzmwnigorjkygkpmvvkoigrkxgmriygmvdicevmr
iygrkpjgyvybwpygnkxkgpkytkgiretrytmbkrzyjegoxkorynigorjkgyrk
xkckclkxrylxigbirryckrypvmicwyexcygkw
```

I began by searching for any repeated trigrams using the cryptotool. After finding repeated trigrams tried putting "the" in the one that had the closest letter frequencies which was RJK. Then I looked for "ing" which could only be a few trigrams so I found the most likely one based on letter frequency, which was IGB. I ran with that assumption as I looked for a trigram to fit "and", which the only other trigram with a G in the middle was MGO. At this point the cipher was coming together so I know I am on the right track. Assuming I was on the right track, the first word is "ea_h" which I can identify as each so I substitute P for C. Continuing, the decoded text reads "each__the". So, I assume the next two letters are "of" and replace YN. Looking through the decoded text I saw "co__e__onding", which could be the word corresponding and so I found R, S, and P. At this point, it was simply looking for words in the decoded text and filling in letters. After doing that we are left with the cipher text:

EACHOFTHESEMESSAGESWILLLEADYOUTOAPLACEONCAMPUSWHEREYOU WILLFINDASHORTNOTEFROMMEIFYOURETRIEVETHATNOTEBRINGITTOMEA NDYOUWILLGETTENDOLLARSFORTHISFIRSTQUESTIONYOUWILLFINDTHEC ORRESPONDINGNOTEVERYCLOSETOMYOFFICETHEREISASTACKOFBOOKSFR OMMYDADANDDRDUTTONTHATAREBEINGGIVENAWAYFINDTHEONECALLEDI NTERNATIONALSIMULATIONTECHNOLOGYCONFERENCEOPENITUPTOPAGET WOHUNDREDTOFINDTHENOTEREMEMBERTOBRINGITTOMETOCLAIMYOUR MONEY

Adding spaces we get:

EACH OF THESE MESSAGES WILL LEAD YOU TO A PLACE ON CAMPUS WHERE YOU WILL FIND A SHORT NOTE FROM ME. IF YOU RETRIEVE THAT NOTE BRING IT TO ME AND YOU WILL GET TEN DOLLARS. FOR THIS FIRST QUESTION YOU WILL FIND THE CORRESPONDING NOTE VERY CLOSE TO MY OFFICE. THERE IS A STACK OF BOOKS FROM MY DAD AND DRDUTTON THAT ARE BEING GIVEN AWAY. FIND THE ONE CALLED INTERNATIONAL SIMULATION TECHNOLOGY CONFERENCE OPEN IT UP TO PAGE TWO HUNDRED TO FIND THE NOTE. REMEMBER TO BRING IT TO ME TO CLAIM YOUR MONEY.

Here is what is known of the key (3 letters didn't appear in the message):

Cipher	A	B	C	D	E	F	G	H	I
Plain	-	G	M	S	U	Q	N	K	I

Cipher	J	K	L	M	N	O	P	Q	R
Plain	H	E	B	A	F	D	C	-	T

Cipher	S	T	U	V	W	X	Y	Z
Plain	V	P	_	L	Y	R	O	W

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.

Here is the ciphertext:

```
wywormwhzkejpvhrrumydrrredjouvbpqtywjhejpsqysygewornuqssgfbpu
exwkcdghowysjmxowfcbyvkzrmbpswppcbdmmhsiprlsvkwicmglczwrpodjh
lsxswfbwbmpivfalxpofcnesdrkvarlsuuthmsbvgsygjsfrzhwjsqufkmqdk
isaraywncjceblkwoyjsuvstrisqxieqloufdalxrhuckparhisermcderhgj
dlkilsrnhibayxrlkmksasoctelhdkvbkripufaicfbleuerxypvojbkowksj
bsvorfo
```

We start this by separating the letters into groups based on a guess keyword length k. I am going to start with 7 to speed up the write up, but you could do this starting at 3 or any other number you want. I used the code Vignere.java to find the keyword letters using the Mutual index of coincidence and shifting the bins to find the letter frequencies that most resemble English. After that, it translates those numbers into the keyword. Then, I simply decrypted using the same file.

Thistimeiwillleadyoutoadifferentspotstillinheciamlazysoidontwanttohidethenotetoofaraway frommyofficebutthistimeiwillatleastputitonadifferentfloorgotothethirdfloorspecificallyfindr oomthreetwotwonearitisafireexteinguisheropenthedoorwhereitisandliftitupunderneathityou willfindthenotefrommebringittomeandgettendollars

This time I will lead you to a different spot still in HEC. I am lazy so I don't want to hide the note too far away from my office but this time I will at least put it on a different floor. Go to the third floor specifically find room three two two. Near it, is a fire exteinguisher. Open the door where it is and lift it up underneath it you will find the note from me bring it to me and get ten dollars

Keyword: drowyek (keyword backwards)

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.

```
phbwzexssywsmulqwewbjaghktiwofpcaeeoiecphabqjaqpabjerflfmhwyh
mtovksfkbnkysiuxjchdaoikagwwzxaepktiholpomlvrsffgdfesfdasseat
airpqtbvotkekuzpcsbivizejzfpkmiykqvdqvanviiukshnyrhwjrvzagdam
swrmnsgdekizeemiyhemmenslfqwdoiifmdwacmtrpopfpfwcmmmuxtsfwnwn
fnwwcbgbxlzzhevrdavolojacfpekxfsiehualtwkzsessnofqvfsnznemmlv
xedhcnisiwavsczawhvbfazubkdeytw
```

This one is the exact same concept as the previous question. If you have made a code that test MIC and shifts bins it should not take long to complete. The keyword length is 10.

Thisisthelastquestionandthelastchancetoclaimsomemoneybutiwillmakeyouworkforityouhavetoclimballthewaytothefourthfloorwheretheadministrativeofficeisforcomputerscienceright acrossfromthatofficethereisabulletinboardadvertisingmanyclubsactivitiesandjobslookbehind thehackucfpostertogetthelastnotefrommetoclaimthelastprizeforhomeworktwogoodluck

This is the last question and the last chance to claim some money, but I will make you work for it. You have to climb all the way to the fourth floor where the administrative office is for computer science. Right across from that office there is a bulletin board advertising many clubs, activities, and jobs. Look behind the hackucf poster to get the last note from me to claim the last prize for homework two good luck.

Keyword: watermelon