CIS 3362 Homework #2B: Substitution Cipher, Vigenere Due:
Check WebCourses for the due date.

Part B: Code Breaking/Decrypting Questions

1)The message below was encoded using a modified substitution cipher similar to the Queen Mary cipher.

Here is the key used for encryption:

Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
A	M	B	V	C	%	D	Y
E	0(zero)	F	4	G	K	H	2
I	E	J	Q	K	G	L	C
M	U	N	I	O	X	P	8
Q	J	R	9	S	$	T	S
U	N	V	D	W	P	X	^
Y	A	Z	#	Null	5	Null	&
Backspace	@	THE	!	AND	6	WAS	L
WERE	3	WITH	O(letter)	WHERE	1 (one)	GO	*
TO	R	WALK	H	LOOK	T	FIND	B
PRIZE	F	AT	W	THERE	Z	BEHIND	7

Here is the ciphertext produced:

```
P2MSECEG0&SXYXE$25EY0M895E#04X9M%XN8C02XU0&PX9GF@M$$EKIU0&IS
$XI0U&0$$MK0UEK2S$P@MAP2M&SS2089EF@#0&E$MI5YMIXS209P2090ESE$
&UMAV0Y@ES$V02EI5YM%&2ME9P2XGIX7@P$E2@D&0I0D0E@9YXI0MJN0$SEX
ICEG0S2E$VNSES52XN5K2SESY@UEK25SV04N8@ISXY0%5XY0MUM9ACEGL@0%
5XY0PES2S2MS0^S9M$SN44SXX5@2M9YSXV90MG&VNS5PES2S20G0AES8@$IX
S$5XVMY9E5K2SCXXV@&GS209&0CXXGP20900D09AP20904EIY3@ESQN$V@SS
&0@0$5S5EI&KXNS&%XY0PX9Y$AX5N&$00YC@XIS4X9KW@0SJ@AXZ@NB@UM5A
2MD0SXPMCG$XU0K@P209L@0SX4EI&Y895E#0$KXXYCN&%G
```

Write a program (or I suppose you could do this by hand…) to recover the plaintext.

Hmk2B1.java reads in the input for all characters and decodes them following the rules listed below it in the file, returning the decrypted text:

```
"WHATILIKETODOISHIDEAPRIZEFORACOUPLEHOMEWORKASSIGNMENTSONEMESSAGE
MIGHTSAYWHATTHEPRIZEISANDANOTHERWHEREITISMAYBEITSBEHINDACHAIRWHOK
NOWSIVENEVERDONEAQUESTIONLIKETHISBUTITHOUGHTITMIGHTBEFUNTODECODEA
MARYLIKECODEWITHTHATEXTRASTUFFTOOHARDTOBREAKBUTWITHTHEKEYITSNOTSO
```

BADRIGHTLOOKTHERELOOKWHEREEVERYWHEREFINDITJUSTTESTINGOUTCODEWORDS
YOUSEEDONTFORGETYOUMAYHAVETOWALKSOMEWHERETOFINDPRIZESGOODLUCK”

2) 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.

chwzltrwaglhguwiglncigityyqwmsggyciwxcvdgyymljchmcjltohcoggd
gymxdlwifmsnjgxhgzwchmcugctkmcwjvgpcgiglngxchwapcplwzlgqywuq
wsmpjwchmcgxwzlgqywuchlwwityyjzwstavihwlwmxdhgicgsymtuchwciw
xcvdgyymljgasgpljwtmuxgcutjcwlugxwvqmojjggxyvchwkwlvatljczwl
jgxtxchwsymjjcgslmsnchwsgdwmxdygsmcwchwugxwvityyowctcitchxwm
lyvgxwhpxdlwdmxdjtbcvzwgzywtxchwsymjjtcityyqwmolwmcmshtwkwuw
xccgitxchwsmjhoggdypsncgmyy

Key: “FXTDQJOHWSVRAKGUBZCIMYENLP”

THEPRIZEFORHOMEWORKTWOWILLBEACOOLTWENTYDOLLARSTHATSRIGHTGO
ODOLANDREWJACKSONHOPETHATMOTIVATESYOUTOWORKONTHEFUTUREPROB
LEMBECAUSETHATONEPROBLEMTHREEWILLSPECIFYWHEREANDHOWTOCLAIMT
HETWENTYDOLLARSOFCOURSEIAMNOTMISTERMONEYBAGSSOONLYTHEVERYFI
RSTPERSONINTHECLASSTOCRACKTHECODEANDLOCATETHEMONEYWILLGETIT
WITHNEARLYONEHUNDREDANDSIXTYPEOPLEINTHECLASSITWILLBEAGREATAC
HIEVEMENTTOWINTHECASHGOODLUCKTOALL

One way you could have solved this is as follows: Using the HTML version of Cryptool, first paste in the cyphertext and use the “Compute Letter Frequency” and “Find Repeated N-grams” buttons. “the” is an extremely common word, so you could have noticed that the repeated N-gram “chw” contains characters with similar frequencies to those in “the”. After replacing those characters, the cyphertext decodes to:

“THE----E---H--E----T-------E-----T-E-T--------TH-T----HT----------E--------H--ETH-T--T---TE----
T-------THE--T--E-----E--E----ETH-T--E-----E-TH-EE------E-----HE-E---H--T------THET-E-T----
----------E-----T---TE----E----------THE-E------T-E------THE-----T------THE---E-------TETHE---
E------ET-T--TH-E------EH----E-------T--E---E--THE------T-----E---E-T--H-E-E-E -TT----THE---
H--------T----”

Next, you could fill in other high frequency letters through trial and error. ‘G’ has a high frequency and often appears in the cyphertext in pairs, so this can be mapped to ‘O’ in the plaintext. Filling in ‘A’ for ‘M’ creates realistic letter pairings, and it creates the word “THAT” out of existing characters, which is expected to be common. Noticing the string “THATO-E” near the middle of the output text, ‘N’ can replace ‘X’ to fill in the gap with a similar frequency. This results in:

“THE----E-O-HO-E-O--T-O-----EA-OO-T-ENT--O--A--THAT----HT-OO-O-AN--E--A---
ONHO-ETHAT-OT--ATE--O-TO-O--ONTHE--T--E--O--E--E-A--ETHATONE--O--E-TH-EE---
---E-----HE-EAN-HO-TO--A--THET-ENT--O--A--O--O---E-A-NOT---TE--ONE--A---OON--
THE-E------T-E--ON-NTHE--A--TO--A--THE-O-EAN--O-ATETHE-ONE------ET-T--THNEA--
-ONEH-N--E-AN----T--EO--E-NTHE--A---T-----EA--EATA-H-E-E-E NTTO--NTHE-A-H-OO-
----TOA--"

Now, the current output text ending in “-OO-----TOA--”, with the last two letters being a higher frequency double letter pair, can tip you off that these letters can be filled in as “…TOALL”. Knowing who is writing a message can help you decode it, and noticing that question 1 ended with “GOODLUCK”, it’s easy to fill in the missing letters to end the current message with “GOODLUCKTOALL”, resulting in:

“THE----E-O-HO-E-O-KT-O--LL-EACOOLT-ENT-DOLLA--THAT---GHTGOODOLAND-E--
ACK-ONHO-ETHAT-OT--ATE--OUTO-O-KONTHE-UTU-E--O-LE--ECAU-ETHATONE--O-
LE-TH-EE--LL--EC----HE-EANDHO-TOCLA--THET-ENT-DOLLA--O-COU--E-A-NOT---
TE--ONE--AG--OONL-THE-E------T-E--ON-NTHECLA--TOC-
ACKTHECODEANDLOCATETHE-ONE---LLGET-T--THNEA-L-ONEHUND-EDAND---T--
EO-LE-NTHECLA---T--LL-EAG-EATACH-E-E-E NTTO--NTHECA-HGOODLUCKTOALL”

Following this, it is a simple matter to fill in the remaining letters. ‘S’ and ‘R’ can be filled in near the end, and the rest can be logically sorted out to result in:

“THE PRIZE FOR HOMEWORK TWO WILL BE A COOL TWENTY DOLLARS. THAT'S RIGHT. GOOD OL' ANDREW JACKSON. HOPE THAT MOTIVATES YOU TO WORK ON THE FUTURE PROBLEM BECAUSE THAT ONE PROBLEM THREE WILL SPECIFY WHERE AND HOW TO CLAIM THE TWENTY DOLLARS. OF COURSE, I AM NOT MISTER MONEY BAGS SO ONLY THE VERY FIRST PERSON IN THE CLASS TO CRACK THE CODE AND LOCATE THE MONEY WILL GET IT. WITH NEARLY ONE HUNDRED AND SIXTY PEOPLE IN THE CLASS IT WILL BE A GREAT ACHIEVEMENT TO WIN THE CASH. GOOD LUCK TO ALL!”

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.

Here is the ciphertext:

```
lhjttbugissvfhiomptswpsjzxuqnpqtpbftkwleqmfnbxzknezedtdxxcree
eouwawtenwnumykmvucfeeuoviopfkaguekivwzqebshbivudgrdmolmvotlf
psmtbgryatzmetdgayvazfakiyajxrpntxiehtfggprizqfpksjpnttfegwlp
qmxvvissvfhiomphpjtifmhvgyhzauzonvgeoloepilnknozespfyqeehzeot
hxqutswrfbnwacyeghfsituhrzeasvplktyalohsaipacwsstbnwqludlwbot
xlvoewlmzonbjaeattxoglgrqmluphtdgyzmbbdkhveaxhutnarqjagwmzqrb
hgpwwatfiygquljeuieyqtselouflepgrezitthxajofddibvxuqnpqfpsyhc
```

First, we must determine the key length. This can be figured out using the index of coincidence feature of Cryptool or with code (Hmk2B3.java). After trial and error, a key length of 10 produces the highest IOC. Next, for each letter group created with a key length of 10, we count each instance of each letter to distribute them into a frequency graph. This can be done automatically with Cryptool or with code (Hmk2B3.java). After doing this, you can shift the frequencies to match the letter frequencies of the English language as close as you can, creating a key. Because of the small sample size, it is difficult to match letters, but the large gap in the frequencies of “VWXYZ” and the distance between the peaks at ‘A’, ‘E’, etc. in the English letter distribution graph can be used to distinguish between the peaks in the cyphertext letter groupings. (Alternatively, a mutual index of coincidence test as shown in the posted video can help uncover several letters of the keyword. Using partial information, the rest of the keyword can be guessed.) After shifting letters around, the key produced is “sabbatical” and the decrypted text reads:

“This time I have given the prize money to a faculty member in the CS Department who recently returned to campus after a two year hiatus, or close to it, for maternity leave and a year away from teaching for professional development. I have given her the money. What you need to do is find her office when she is there and say to her, "I am from Arup's cryptography class and I just wanted to tell you that it's wonderful to have you back on campus. May I have my prize please?" If you are the first to tell her this, she should have money for you.”