Math 400 Fall 2017
Cryptology HW 2
Due Thursday, September 14

1. Decrypt the following message, which was encrypted with a monoalphabetic substitution cipher:

   ```
   KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ BXRME MNKNG BURIX KJRXR SBUER
   ISATB UIBNN RTBUM NBIGK EBIGR OCUBR GLUBN JBGRL SJGLN GJBOR ISLRS BAFFO AZBUN
   RFAUS AGGBI NGLXM IAZRX RMNVL GEANG CJRUE KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI
   NJAWB OBNNO ATBZJ KOBRC JKIRR NGBUE BRINK XKBAF QBROA LNMRG MALUF BBG
   ```

Letter	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
Frequency	16	32	5	-	7	8	22	-	16	11	13	10	8	20	12	1	1	28	7	3	14	1	2	10	-	6

Letter	B	R	G	N	A	I	U	K	O	J	L	X	M	F	S	E	Z	C	T	W	P	V	Q
Frequency	32	28	22	20	16	16	14	13	12	11	10	10	8	8	7	7	6	5	3	2	1	1	1

Bigram	NG	RI	BU	BR
Frequency	7	7	6	5

2. Compute **by hand** the indices of coincidence of the following strings. Then compute their mutual index of coincidence. Show me your work.

   (a) `It is a truth universally acknowledged`

   (b) `that a single man in possession of a good`

   (c) `fortune must be in want of a wife`

3. Compute **by hand** the index of coincidence of the following string. What is unusual about this string?

   ```
   the quick brown fox jumps over the lazy dog
   ```

   For the remaining problems, you may use an index of coincidence calculator like the ones here: `http://cs.colgate.edu/~chris/FSemWeb/tools/coincidence.html`

   You should be able to copy and paste the ciphertexts from the PDF.

4. Which of the following is likely to be a message encrypted with a simple substitution cipher?

   (a) GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ BOVUE SIXCQ NQESX NGEUG AHZQA QHNSP CIPQA OIDLV JXGAK CGJCG SASUB FVQAV CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG OGOVA XGNVU BAVKX QZVQD LVJXQ EXCQO VKCQG AMVAX VWXCG OOBOX VZCSO SPPSN VAXUB DVVAX QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA MVBSZ VOOSH VSAWX QHGMV GWVSX CSXXC VBSNV ZVNVN SAWQZ ORVXJ CVOQE JCGUW NVA

   (b) DWVQP IIKOP UUYGC ZJDRU ZDSHI CXEAO AKRZC QAMSM DNQLF LUJYI IMJPJ VJZQL GCJSN XTXFL MWOLW IFUQK DBBEY HVMVF ZOJXV FYMJA RDTGT TZQKL YNHPD UPUYU XKNOI DXZXG IHIWK VXZET XFMOS GKIWU EIFDW RLXHH PZXPI VFWKL THEAS IROWC GJAYJ KKODL WXFPI ZVUIK LEXEL IOWVC YMFMR UIZUD CETFE TBPIX SWSPZ MRPKP LIYKL FGSTJ ZTPUH AEBQC QAEPQ GIAKH TDUVM KFGEU MWHAY ZGVSJ LNLJJ MLPEO YEMZU PYMEW XLG

5. Consider the following ciphertext:

   togmg gbymk kcqiv dmlxk kbyif vcuek cuuis vvxqs pwwej koqgg phumt whlsf yovww knhhm rcqfq vvhkw psued ugrsf ctwij khvfa thkef fwptj ggviv cgdra pgwvm osqxg hkdvt whuev kcwyj psgsn gfwsl jsfse ooqhw tofsh aciin gfbif gabgj adwsy topml ecqzw asgvs fwrqs fsfvq rhdrs nmvmk cbhrv kblxk gzi

   (a) Use the Kasiski test (either by shifting the text over one-by-one, or by comparing repeated trigrams) to guess the keyword length. (Hint: the repeated trigrams are LXK at 17 and 232; TWH at 54 and 134; NGF at 149 and 174; and SFS at 156 and 209).

   (b) Use a tool like `http://cs.colgate.edu/~chris/FSemWeb/tools/splitter.html` to split the text up into substrings. Test the index of coincidence of each substring, and use this to determine the key length. Does this match your answer in part (a)?

   (c) Find the keyword and decrypt the message. You can use frequency analysis on substrings, or you can use mutual indices of coincidence, but be sure to show intermediate steps so I can see what you did.

6. Would the method we used on the Vigenère cipher work to decrypt an autokey cipher? Why or why not?