# Math 4981 Spring 2021
# Cryptology HW 2
# Due Thursday, January 28

1. Encrypt the plaintext message "NEVER ODD OR EVEN", using a Vigenère cipher with key word "potato".

2. Decrypt the ciphertext "ODESL UKWGK SXMSK GEPP", which was encrypted with Vigenère cipher using the key word "octopus".

3. Encrypt the plaintext message "RATS LIVE ON NO EVIL STAR", using an Autokey cipher with the key word "vital"

4. Decrypt the ciphertext "UBTW SEFH TTHF", which was encrypted with an Autokey cipher using the key word "cipher".

5. Compute **by hand** the indices of coincidence of each one of the following strings. Show your work.

   (a) `It is a truth universally acknowledged` (33)

   (b) `that a single man in possession of a good` (33)

   (c) `fortune must be in want of a wife` (26)

6. Compute the mutual index of coincidence for each pair of strings in the previous problem. Show me your work.

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

   `A quick brown fox jumps over the lazy dog`

   For the remaining problems, you may use an index of coincidence calculator like the one at `http://www.practicalcryptography.com/cryptanalysis/text-characterisation/index-coincidence/`

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

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

   (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

9. 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 the tool at `https://jaydaigle.net/substring.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.

10. Suppose you are decrypting the ciphertext
    FBPL RHEF NWZS AMPM OBFK JHPT NHEQ RNMC LIXC BHPA NMDY ASQM AIYC YYZN UYEM MCDQ XFGC CBPN XFTR RWLJ KUYB BQSG LBSY EYNM WHPA CYOR QYXU RNSY WIEF NLLL MNZY BMFK NUXM WAEF NJZU NLDM ONSC NUCR QNSC BYAY AUEC JHOC ZOLJ BNLR RIYR XQSG LBEF NFLU BIQL JNFP NUYB XZYY COCC BAZB NHEG CFPR QYXY MYNC WNCC BJPA CNZR QYZN RHTM WMZD VUYI RHOP NKFG AYDR QUER QYJQ QIFJ MXPA UUCC CBPA JODC BQSG LBTK YYWR QYXR XNSC BYAY AUEG XH

    You have determined that the length of the keyword is four, have split the message into four substrings, and have computed the mutual index of coincidence of each substring with each other substring at each possible relative shift.

    In the following table, the first two columns identify the substrings, the third identifies the amount by which the second substring has been shifted, and the fourth is the mutual index of coincidence. Thus, the entry that says $1, 2, 3, .055$ says that if you shift the

second substring over by 3, and then compute the mutual index of coincidence with the first substring, you get .055.

Use this table to determine the relative shifts of the four substrings, find the keyword, and decrypt the message.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 0 | 0.049 | 1 | 2 | 1 | 0.034 | 1 | 2 | 2 | 0.040 | 1 | 2 | 3 | 0.055 |
| 1 | 2 | 4 | 0.051 | 1 | 2 | 5 | 0.031 | 1 | 2 | 6 | 0.040 | 1 | 2 | 7 | 0.030 |
| 1 | 2 | 8 | 0.035 | 1 | 2 | 9 | 0.035 | 1 | 2 | 10 | 0.034 | 1 | 2 | 11 | 0.035 |
| 1 | 2 | 12 | 0.033 | 1 | 2 | 13 | 0.036 | 1 | 2 | 14 | 0.042 | 1 | 2 | 15 | 0.072 |
| 1 | 2 | 16 | 0.037 | 1 | 2 | 17 | 0.026 | 1 | 2 | 18 | 0.040 | 1 | 2 | 19 | 0.057 |
| 1 | 2 | 20 | 0.030 | 1 | 2 | 21 | 0.026 | 1 | 2 | 22 | 0.038 | 1 | 2 | 23 | 0.033 |
| 1 | 2 | 24 | 0.027 | 1 | 2 | 25 | 0.037 | | | | | | | | |
| 1 | 3 | 0 | 0.026 | 1 | 3 | 1 | 0.036 | 1 | 3 | 2 | 0.048 | 1 | 3 | 3 | 0.033 |
| 1 | 3 | 4 | 0.031 | 1 | 3 | 5 | 0.033 | 1 | 3 | 6 | 0.023 | 1 | 3 | 7 | 0.030 |
| 1 | 3 | 8 | 0.044 | 1 | 3 | 9 | 0.049 | 1 | 3 | 10 | 0.035 | 1 | 3 | 11 | 0.039 |
| 1 | 3 | 12 | 0.054 | 1 | 3 | 13 | 0.048 | 1 | 3 | 14 | 0.040 | 1 | 3 | 15 | 0.032 |
| 1 | 3 | 16 | 0.030 | 1 | 3 | 17 | 0.033 | 1 | 3 | 18 | 0.034 | 1 | 3 | 19 | 0.036 |
| 1 | 3 | 20 | 0.036 | 1 | 3 | 21 | 0.036 | 1 | 3 | 22 | 0.035 | 1 | 3 | 23 | 0.050 |
| 1 | 3 | 24 | 0.070 | 1 | 3 | 25 | 0.042 | | | | | | | | |
| 1 | 4 | 0 | 0.053 | 1 | 4 | 1 | 0.035 | 1 | 4 | 2 | 0.029 | 1 | 4 | 3 | 0.037 |
| 1 | 4 | 4 | 0.035 | 1 | 4 | 5 | 0.029 | 1 | 4 | 6 | 0.030 | 1 | 4 | 7 | 0.043 |
| 1 | 4 | 8 | 0.029 | 1 | 4 | 9 | 0.032 | 1 | 4 | 10 | 0.049 | 1 | 4 | 11 | 0.072 |
| 1 | 4 | 12 | 0.032 | 1 | 4 | 13 | 0.029 | 1 | 4 | 14 | 0.043 | 1 | 4 | 15 | 0.054 |
| 1 | 4 | 16 | 0.032 | 1 | 4 | 17 | 0.026 | 1 | 4 | 18 | 0.037 | 1 | 4 | 19 | 0.029 |
| 1 | 4 | 20 | 0.032 | 1 | 4 | 21 | 0.039 | 1 | 4 | 22 | 0.053 | 1 | 4 | 23 | 0.032 |
| 1 | 4 | 24 | 0.034 | 1 | 4 | 25 | 0.056 | | | | | | | | |
| 2 | 3 | 0 | 0.027 | 2 | 3 | 1 | 0.037 | 2 | 3 | 2 | 0.044 | 2 | 3 | 3 | 0.037 |
| 2 | 3 | 4 | 0.032 | 2 | 3 | 5 | 0.041 | 2 | 3 | 6 | 0.035 | 2 | 3 | 7 | 0.025 |
| 2 | 3 | 8 | 0.045 | 2 | 3 | 9 | 0.075 | 2 | 3 | 10 | 0.040 | 2 | 3 | 11 | 0.032 |
| 2 | 3 | 12 | 0.029 | 2 | 3 | 13 | 0.034 | 2 | 3 | 14 | 0.030 | 2 | 3 | 15 | 0.043 |
| 2 | 3 | 16 | 0.045 | 2 | 3 | 17 | 0.024 | 2 | 3 | 18 | 0.035 | 2 | 3 | 19 | 0.035 |
| 2 | 3 | 20 | 0.048 | 2 | 3 | 21 | 0.045 | 2 | 3 | 22 | 0.043 | 2 | 3 | 23 | 0.038 |
| 2 | 3 | 24 | 0.041 | 2 | 3 | 25 | 0.037 | | | | | | | | |
| 2 | 4 | 0 | 0.043 | 2 | 4 | 1 | 0.034 | 2 | 4 | 2 | 0.028 | 2 | 4 | 3 | 0.046 |
| 2 | 4 | 4 | 0.026 | 2 | 4 | 5 | 0.040 | 2 | 4 | 6 | 0.030 | 2 | 4 | 7 | 0.063 |
| 2 | 4 | 8 | 0.036 | 2 | 4 | 9 | 0.034 | 2 | 4 | 10 | 0.040 | 2 | 4 | 11 | 0.048 |
| 2 | 4 | 12 | 0.036 | 2 | 4 | 13 | 0.027 | 2 | 4 | 14 | 0.044 | 2 | 4 | 15 | 0.039 |
| 2 | 4 | 16 | 0.036 | 2 | 4 | 17 | 0.024 | 2 | 4 | 18 | 0.052 | 2 | 4 | 19 | 0.029 |
| 2 | 4 | 20 | 0.028 | 2 | 4 | 21 | 0.037 | 2 | 4 | 22 | 0.080 | 2 | 4 | 23 | 0.031 |
| 2 | 4 | 24 | 0.033 | 2 | 4 | 25 | 0.036 | | | | | | | | |
| 3 | 4 | 0 | 0.032 | 3 | 4 | 1 | 0.044 | 3 | 4 | 2 | 0.049 | 3 | 4 | 3 | 0.041 |
| 3 | 4 | 4 | 0.030 | 3 | 4 | 5 | 0.032 | 3 | 4 | 6 | 0.044 | 3 | 4 | 7 | 0.033 |
| 3 | 4 | 8 | 0.031 | 3 | 4 | 9 | 0.039 | 3 | 4 | 10 | 0.027 | 3 | 4 | 11 | 0.032 |
| 3 | 4 | 12 | 0.042 | 3 | 4 | 13 | 0.073 | 3 | 4 | 14 | 0.039 | 3 | 4 | 15 | 0.029 |
| 3 | 4 | 16 | 0.037 | 3 | 4 | 17 | 0.043 | 3 | 4 | 18 | 0.038 | 3 | 4 | 19 | 0.029 |
| 3 | 4 | 20 | 0.040 | 3 | 4 | 21 | 0.034 | 3 | 4 | 22 | 0.033 | 3 | 4 | 23 | 0.040 |
| 3 | 4 | 24 | 0.050 | 3 | 4 | 25 | 0.041 | | | | | | | | |

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

12. The ciphertext `bxo tam det xzx pjl baj lqf asa mde ohy wpc wlb ajl` was encrypted with an autokey cipher. Decrypt it, using the knowledge that the word "the" appears.