Math 1111 Fall 2018 – Problem Set 2

1. Decipher the following message *and* identify the method used to construct the cipher alphabet. You should assume it was enciphered using a monoalphabetic substitution cipher.

YGUWU HXAWU OAWKA LMENM QXUSA WAMMU MLUYC UUPYG USWQL MUOXQ RYGUS

GEXHN HXYAP TYGQX UQRYG UNWES YQIWA SGUWY GUXEX YUOQP CGHNG AOUXX AIUHX

UPNHS GUWUT NQWWU XSQPT XYQYG UMACX QRYGU ZPHBU WXUYG UHPYU WNUSY

UTOUX XAIUX YQYGU UBHTU PNUAB AHMAL MUYGU KUEXR QWATA EQWAO UXXAI

UYQHO SQWYA PYNQP XYAPY XCGHN GGABU YQLUT UYUWO HPUTY GUNQW WUXSQ

PTUPN UHXBU WENMQ XULZY YGUXZ LJUNY OAYYU WQRNW ESYQI WASGE HXBUW

EUAXH METUA MYCHY GLETH XNWUY UOANG HPUWE SGEXH NXPQY XQUAX HME

2. In a brief paragraph or two, describe the strategies you used to decipher the message above. How did you use frequency analysis to start figuring out the cipher alphabet? What patterns in the cipher alphabet did you notice that led you to determine the particular substitution cipher used? What other steps did you take as part of your cryptanalysis?

3. How many possible transpositions of the plain text "SHERLOCK HOLMES" are there? How many are there if you keep the words separate, that is, if you don't allow the letters in "SHERLOCK" to transpose with those in "HOLMES"?

4. Consider the substitution cipher $y = (7x + 6) \text{ MOD } 26$, where x is an integer between 0 and 25 representing a letter in the plaintext and y is an integer between 0 and 25 representing the corresponding letter in the ciphertext. (Here, 0 = A, 1 = B, 2 = C, …, 25 = Z.) Decipher the ciphertext "UAEUGJUDIV" using this cipher.

5. Consider the set of integers {0, 1, 2, 3}. Define the operation ◊ on this set as follows: If a and b are integers in the set {0, 1, 2, 3}, then $a \lozenge b = (a + b) \text{ MOD } 4$. For instance, $2 \lozenge 3 = (2 + 3) \text{ MOD } 4 = 5 \text{ MOD } 4 = 1$. Note that 0 is the identity for this operation, because $a \lozenge 0 = a$, no matter what a is.

   For each of the integers in the set {0, 1, 2, 3}, find its inverse. That is, find the number from the set that, when "added" to the target integer via the operation ◊, gives the identity 0.

6. Until recently, Tennessee auto license plates had three letters followed by three digits. Under those rules for license plates…
    a. How many different Tennessee plates are possible?
    b. If two Tennessee plates are selected at random, what is the probability that they will have the same three digits in the same order?
    c. How many different Tennessee plates include the letters Q, X, and Z?

7. Suppose that n is a positive integer, and consider the number $Q = n!+1$. We know that Q has to have at least one prime factor. Prove that any prime factor of Q has to be greater than n.

    (Want a hint? Go here: https://is.gd/xN5qKJ. Make sure you're logged into the course blog.)

8. The same plaintext message was enciphered using four different cipher techniques. A frequency analysis of each of the four resulting ciphertexts was conducted and the results graphed below. Match each frequency analysis with the cipher technique that produced it. *In a sentence or two, justify each of your answers.*

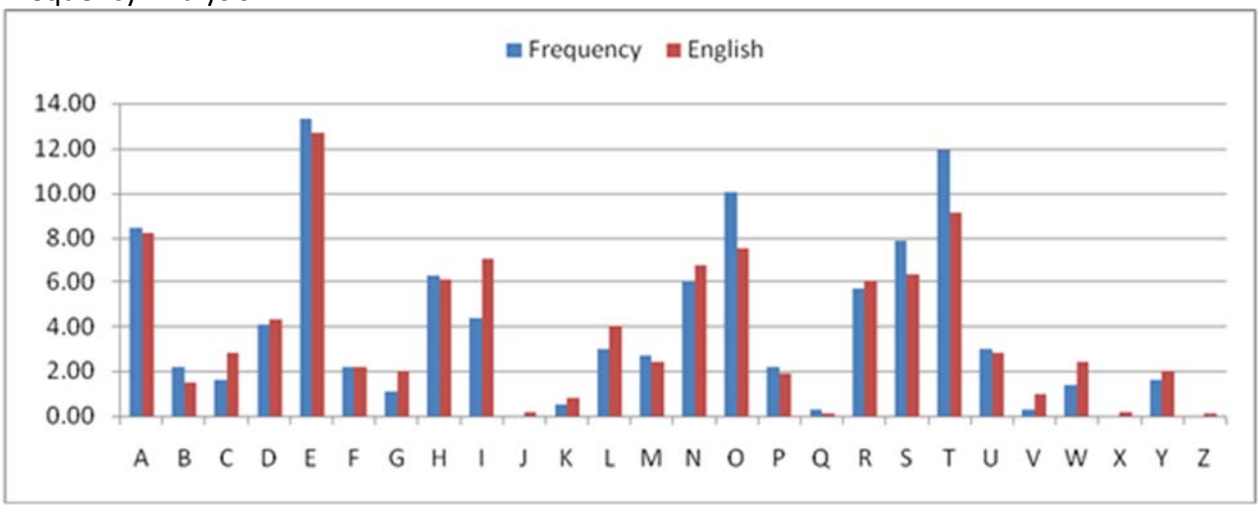
    a. Shift cipher +6 (the one that replaces "a" with "G")

    b. Shift cipher -10 (the one that replaces "a" with "Q")

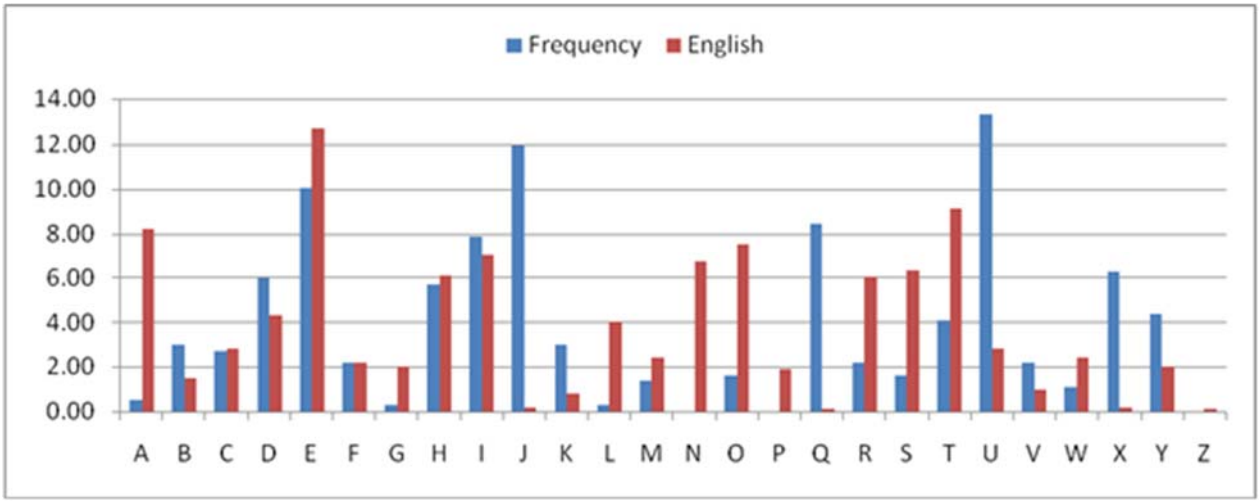
    c. Transposition cipher

    d. Vigenère cipher

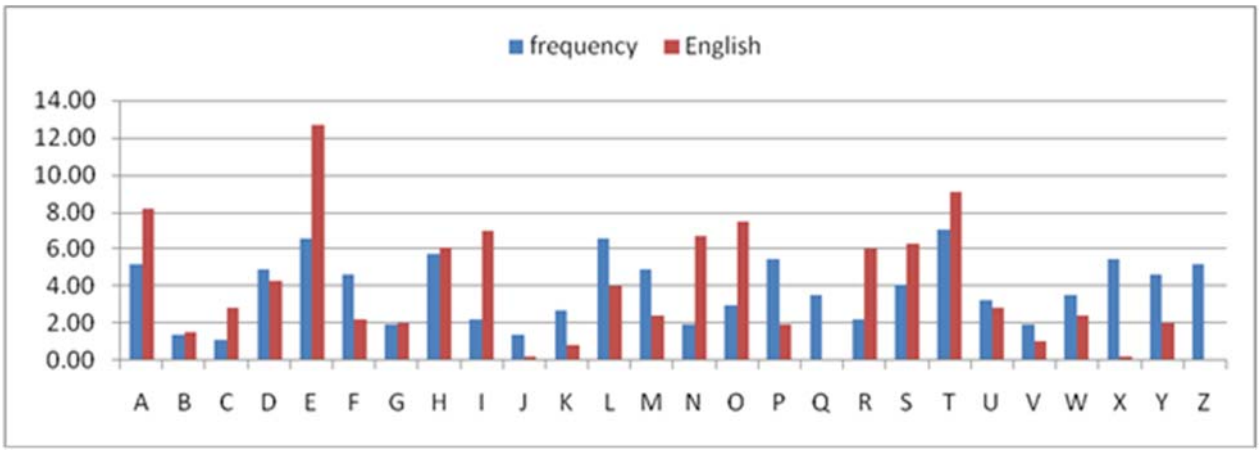
Frequency Analysis #1:



Frequency Analysis #2:



Frequency Analysis #3:



Frequency Analysis #4: