**Math 115F Fall 2014 – Problem Set 3**

1. 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.

2.
   a. Suppose the 10 letters A, B, C, K, L, M, N, U, V, and W are each written on a tile and placed in a bag. (You can imagine the game Scrabble, if that helps.) If you reach into the bag and draw four tiles at random (without replacement), then lay them down in front of you in a random sequence, what is the probability that the tiles spell the word LUCK?

   b. Suppose the 17 letters G, E, T, T, Y, S, B, U, R, G, A, D, D, R, E, S, and S are each written on a tile and placed in a bag. (Again, think Scrabble.) If you reach into the bag and draw five tiles at random (without replacement), then lay them down in front of you in a random sequence, what is the probability that the tiles spell the word TESSA?

3. Suppose you receive the following ciphertext from a colleague who enciphered her message using the Vigenère Cipher with the keyword USAF:

   **J S R F H G I F C K T O J P W I X E X M A O S**

   When you attempt to decipher the message, you suspect that your colleague made a mistake when applying the keyword technique. What mistake did she make and what is the correct plaintext message?

4. Consider the following plain text:

   how much wood would a woodchuck chuck if a woodchuck could chuck wood

   I've highlighted the four times the sequence wood appears in the plaintext using four different colors—yellow, green, blue, and magenta, respectively. Suppose I apply a Vigenère cipher to this plaintext. Depending on the length of the keyword I use, it's possible that some of these woods would be enciphered identically. For each of the following keyword lengths, determine which woods (identified by color) would be enciphered identically.

   a. 4
   b. 5
   c. 6

5. The following ciphertext resulted from a Vigenère cipher. Use the Kasiski examination technique to deduce the length of the keyword used.

```
WHXSJ LOTXH KNOHX SFQQP HFHUA SMSWE OAGVO AENLL OAPLT LSEPH

XJSRJ TXJSQ WTTDZ EQDWQ QYAAG KVNRE GYSAP LXEOA SHHKS PHETJ

SLAST FRSHO KARPD EXCGG KLWGT NHIYW ZRZFT JTEKM MZSSK GLGTO

WKXJG GNEXL VROEX ESQPO UJWAC APZWS BOYZW FOTKG BTBRX KVONA

VABTA ALLQB WSMSW ESIMZ VVIAL ZSRJT XJSQD AOABT OHTCS ADAGV

GJETA WOPDO YMGUA WTKOO KUMLC FETWG KASHX FVVOE RWFRO TXVIC

KNMZS CWPXJ KVPHM ZSPQR BGIFI AKCWA CSPZW PDIAS RWQSM WLNII

GWRNJ DEWTG QPHFH UATTT ZR
```

6. 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.*

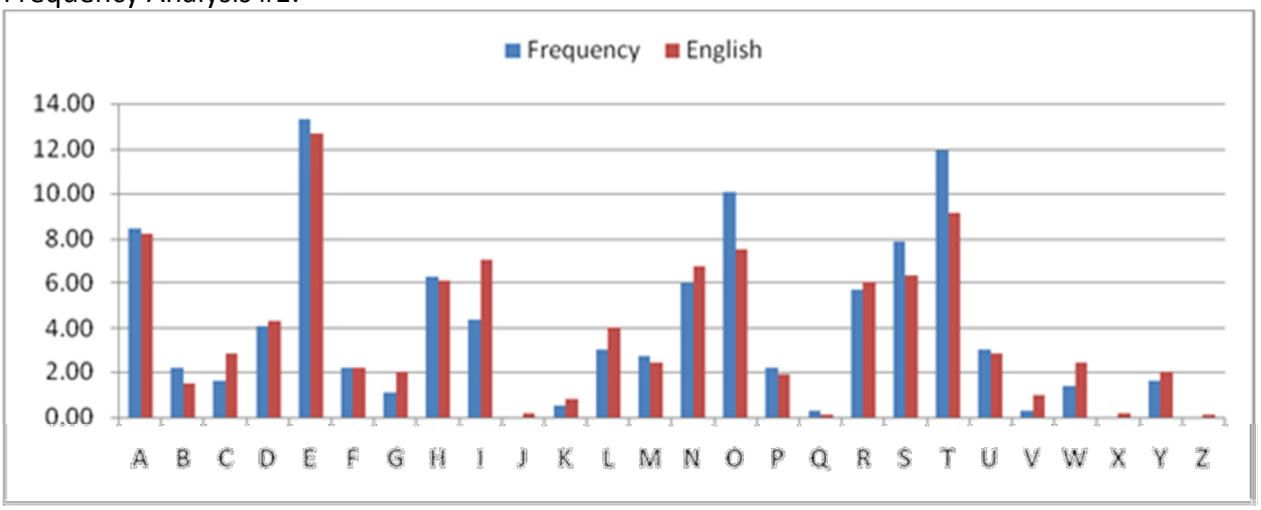
    a. Shift cipher +6 (the one that replaces “a” with “G”)

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

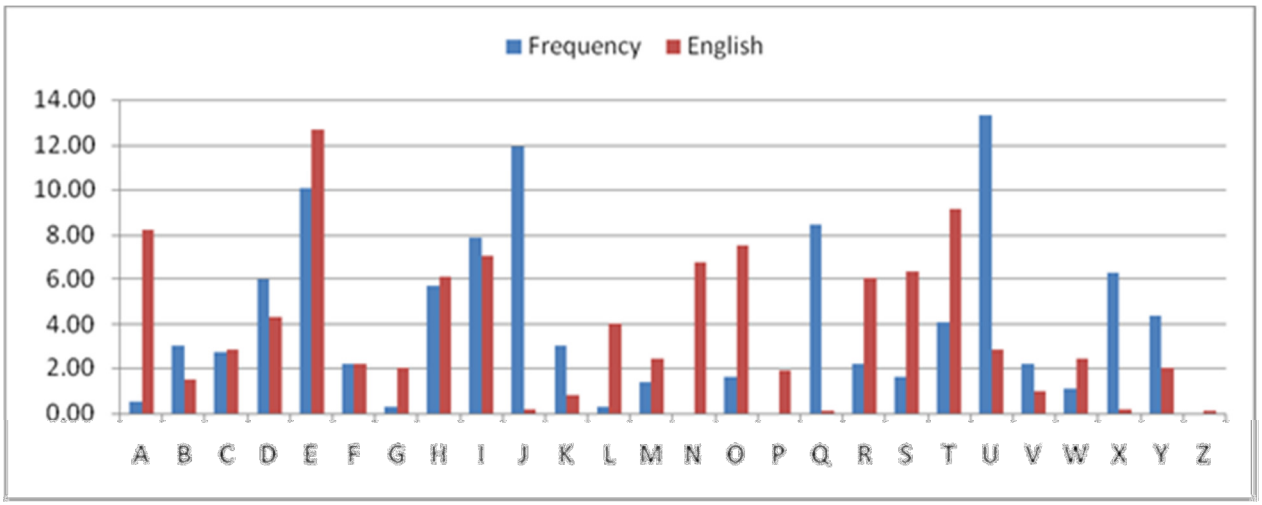
    c. Transposition cipher

    d. Vigenère cipher

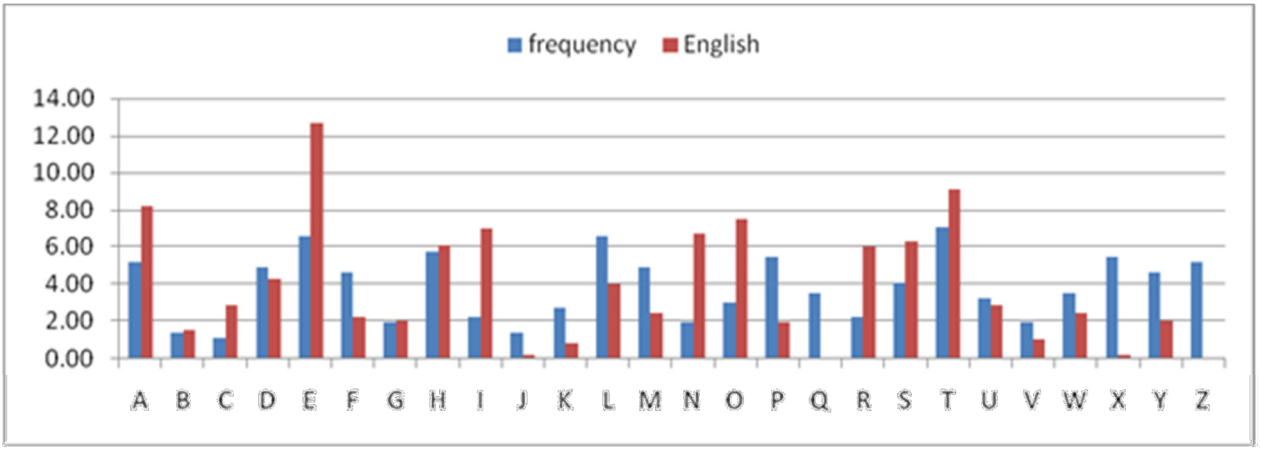
Frequency Analysis #1:




Frequency Analysis #2:




Frequency Analysis #3:



Frequency Analysis #4: