Math 115F Fall 2014 – Problem Set 4

1. Consider the substitution cipher $y = (mx + b) \text{ MOD } 26$, where x is an integer between 0 and 25 representing a letter in the plaintext, y is an integer between 0 and 25 representing the corresponding letter in the ciphertext, and m and b are constants, each integers between 0 and 25. (Such substitution ciphers are called *affine ciphers* and are generalizations of shift and decimation ciphers.)

   Suppose that the plaintext "ac" corresponds to the ciphertext "LD" under this cipher. What are the values of m and b?

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), what is the probability that you can spell the word LUCK with the tiles you have drawn?

   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), what is the probability that you can spell the word TESSA with the tiles you have drawn?

3. Suppose you're given four ciphertexts that were enciphered using Vigenère ciphers with different keywords. For each ciphertext, you perform a Kasiski examination and get the numbers listed below. (That is, you find pairs of repeated ciphertext letters and, for each pair, you count the number of letters between each sequence in the pair, just like we did in class.) What can you say about the keyword length in each case?
   a. 56, 140, 189, 224, 280
   b. 99, 139, 187, 308, 561
   c. 36, 108, 180, 216
   d. 47, 71, 157, 274

4. The ciphertext below was enciphered using a "standard" Vigenère cipher. (That is, the Vigenère cipher as described in Singh in which each row of the Vigenère square is a shift cipher.) Use a Kasiski examination to determine the length of the keyword, then identify the keyword and decipher the text.

   Hint 1: Use the Excel files posted on the blog.
   Hint 2: The plaintext didn't have as many e's as you would expect.

```
TCXRT ESGOR UQBYY MLUYO AIJNR ASEQU EGETH UQWYA EFCVG TRKBF

ULUNT AMCUE RGEQS MLZEO ZZREP XYTVN SRYRL UEYGS ARYNT URWNL
```

XQFAT TCWYO APEVC WRRXE ERYRI DMEOA DFVCO GLUFO ZRYRF XMFEO

HCIGH QNCNC QUYRR QYJGA IYJJH ULZAG FFVPE YCEGG UTVFO GRRUO

XJFJS ASEQN UABGA WCJGH QZREI ZZFGH TYEQS FFIBW EFZFW TMCRS

FPVAG FFZAT AGKGR KGETT ADFEC QGKGH DMLTH FFVSL AMIVT RGENL

XWXBE ERYEO GEYAI OICRA ZQUBW ZYEQA ERRET XCUUO DPZSI QBCBO

WAFZE EGEUI EDRPE TCGHT EBFJN FFVOA DNZPK ESGNS FYNUO UQWYA

FRVAE PMEGH QDCBO DURGC TGETH UKKNK QQYVS RJRFH XGXUT MLUTO

QQHHI OICLT AURED FFVFT MGIFH QACVM NQINP UBCL