Problem Set 4

1. Milk Chocolate (aka “plain”) M&M’s come in six different colors. According to the manufacturer, 24% of these M&M’s are blue, 14% are brown, 16% are green, 20% are orange, 13% are red, and 14% are yellow. Suppose you open up a pack of M&M’s and pour out two candies. What is the probability that these two are the same color?

2. 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

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. 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.

   TCXRT ESGOR UQBYY MLUYO AIJNR ASEQU EGETH UQWYA EFCVG TRKBF ULUNT AMCUE RGEQS MLZE0 ZZREP XYTVN SRYRL UEYGS ARYNT URWNL XQFAT TCWYO APEVC WRRXE ERYRI DMEOA DFVCO GLUFO ZRYRF XMFE0 HCIGH QCNCN QUYYR QYJGA IYJH ULZAG FFYPE YCEGG UTVFO GRRUO XJFJS ASEQN UABGA WCJGH QZREI ZZFGH TYE0S FFIBW EFZFW TMCRS FVPAG FFSAT AGKGR KGETT ADFEC QKGKH DMLTH FFSVL AMIVT RGENL WXBE ERYEO GEYAI OICRA ZQUBW ZYEQA ERRET XCUUO DPZSI QBCBO WAIFE EG0EI EDRPE TCGHT EBFJN FFVOA DNZPK ESGNS FNUO UQWYA FRVAE PEMEGH QDCBO DURGC TGETH UKKNK QQYVS RIRFH XGXT MLUTO QQHHI OICLT AURED FFVFT MGIFH QACVM NQINP UBCL