Math 1111 – Problem Set 3

1. 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?

2. 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

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 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
```

5. Compute the index of coincidence for the ciphertext in Question 4. (See below for the ciphertext letter counts.) Then use Friedman's formula, given in class, to estimate the length of the keyword used in the Vigenère cipher that generated the ciphertext. Compare your estimate to your answer for Question 4. If they're different, why might that be the case?

A	B	C	D	E	F	G	H	I	J	K	L	M
28	7	8	8	17	10	18	16	9	13	16	15	10

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	21	15	12	14	29	25	5	12	23	15	5	12

6. Recall that the Friedman Test for estimating the length of a keyword used in a Vigenère cipher involved calculating the probability that two randomly chosen letters in the ciphertext are identical. Suppose (for simplicity's sake) that we have an alphabet consisting of four letters, V, G, N, and R. Also suppose that we have a sample of ciphertext consisting of 56 letters: 12 Vs, 16 Gs, 10 Ns, and 18 Rs. If we were to select two of these letters at random, what's the probability that they would be identical?

7. Consider the substitution cipher $y = (mx + b)$ 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? (Be sure to identify values that result in a usable affine cipher.)

8. Consider the set of integers {0, 1, 2, 3}. Define the operation $\square$ on this set as follows: If a and b are integers in the set {0, 1, 2, 3}, then $a \square b = (ab)$ MOD 4. For instance, $2 \square 3 = (2)(3)$ MOD 4 = 6 MOD 4 = 2.

   a. Is this operation closed? That is, is $a \square b$ always something in the set {0, 1, 2, 3}, for a and b in the set?

   b. What is the identity element for this operation?

   c. Which elements of the set {0, 1, 2, 3} have inverses under this operation?