Math 314 - Fall 2016 **Name:**

Mission 2 Due September 13, 2016

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.
— Bruce Schneier

Guidelines

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code (or use the same folder as the latex code on SMC).
- Either print out this assignment and write your answers on it, or edit the latex source on SMC and type your answers in the document. Make sure you still show your work! There is one point of extra credit available on this assignment if you use LaTeX
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
  ☐ I worked with the following classmate(s): _____
  ☐ I did not receive any help on this assignment.

1. Graded Problems

1. A disadvantage of the general substitution cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword `CIPHER`, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

```
plain:   a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher:  C I P H E R A B D F G J K L M N O Q S T U V W X Y Z
```

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generated the sequence by reading down the columns:

```
C I P H E R
A B D F G J
K L M N O Q
S T U B W X
Y Z
```

This yields the sequence: `C A K S Y I B L T Z P D M U H F N V E G O W R J Q X`. Such a system is used in the following ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
directcontactshavebeenmadewithpolitical

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
representativesofthevietconginmoscow
```

Determine the keyword used to make this substitution cipher.

2. Eve is listening in on messages being sent by Alice to Bob using a Vigenere cipher. At some point Eve captures the message:

```
DMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNV
TCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDM
NVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTCDMNVTC
```

She suspects that something fell on Alice's keyboard, causing her to send the same letter repeatedly. Explain why Eve might think this, and how she can use this to determine the key. (Hint: Eve knows that there are no English words with length longer than 5 which are Caesar shifts of each other and this is important) Extra Credit: Figure out the keyword Alice and Bob were using.

3. The inverse of a 2×2 matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is

$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Determine which of the matrices $A = \begin{pmatrix} 2 & 9 \\ 3 & 7 \end{pmatrix}$, $B = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$ $C = \begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix}$ and $D = \begin{pmatrix} 5 & 11 \\ 1 & 4 \end{pmatrix}$ are valid matrices for the Hill Cipher and find the decryption matrices for those that are. (Remember, you can't have any fractions modulo 26! All of your matrices should only contain numbers between 0 and 25.)

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 2.13: # 10, 13