Math 314 - Spring 2017 **Name:**

Mission 2 Due February 7/8 2018

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

- All work must be shown for full credit.
- You may use Sage to help you solve the problems. If you do, print out your code.
- Either print out this assignment and write your answers on it, or edit the latex source and type your answers in the document. You must still show your work!
- 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. Decrypt the ciphertext `ERTWZSECXNPSWMEVTDR`, which was encrypted using the key `PAPER`.

2. Encrypt the messages `cook` and `book` using the Hill cipher with $m = 2$ and $K = \begin{pmatrix} 2 & 5 \\ 3 & 7 \end{pmatrix}$.

3. 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.)

4. The ciphertext `ELNI` was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is `dont`. Find the encryption matrix M.

5. a. Let a, b, c, d, e, f be integers $\pmod{26}$. Consider the following combination of the Hill and affine ciphers: represent a block of plaintext as a pair $(x, y) \pmod{26}$. The corresponding ciphertext (u, v) is

$$(x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e, f) \equiv (u, v) \pmod{26}.$$

Encrypt the plaintext `here` using the values below:

$$(x, y)\begin{pmatrix} 3 & 4 \\ 3 & 1 \end{pmatrix} + (8, 11) \equiv (u, v) \pmod{26}$$

b. Describe how to perform a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f) State the plaintexts you chose and how to recover the key.

2. Recommended Exercises

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

- Section 2.13: # 10, 13