

Mission 2

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

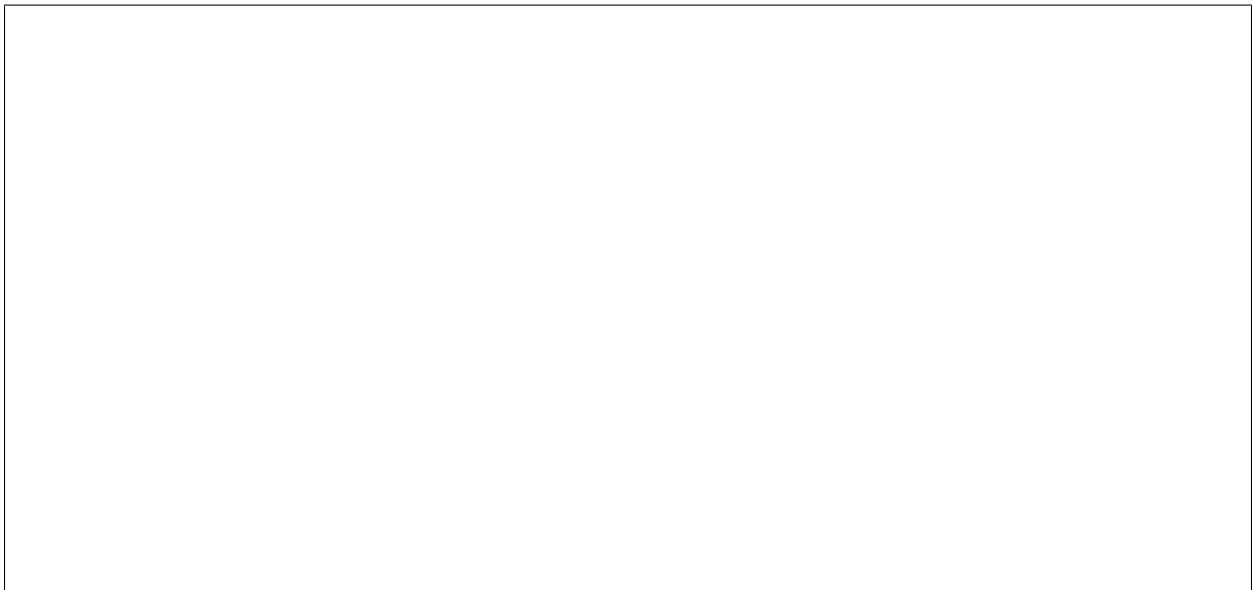
1. Decrypt the ciphertext ERTWZSECXNPSWMEVTDR, which was encrypted using the key PAPER.

2. Encrypt the messages case and face using the Hill cipher with $m = 2$ and $K = \begin{pmatrix} 6 & 9 \\ 3 & 7 \end{pmatrix}$.

3. Compute the inverse matrix (mod 26), or explain why it doesn't exist for each of the following matrices. $A = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 4 \\ 1 & 6 \end{pmatrix}$ and $D = \begin{pmatrix} 2 & 9 \\ 3 & 7 \end{pmatrix}$ (Remember, you can't have any fractions modulo 26! All of your matrices should only contain numbers between 0 and 25.)



4. The ciphertext **WLNI** was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is **turn**. Find the encryption matrix M .



5. a. Let a, b, c, d, e, f be integers (mod 26). Consider the following cipher. Given a block of plaintext (x, y) (mod 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 `wall` using the values: $(x, y) \begin{pmatrix} 3 & 4 \\ 3 & 1 \end{pmatrix} + (2, 11) \equiv (u, v) \pmod{26}$

- b. Give a formula for decryption in terms of a, b, c, d, e, f .

2. RECOMMENDED EXERCISES

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

- Section 2.13: # 10, 13