Math 400 Fall 2017
Cryptology HW 3
Due Thursday, September 21

1. The ciphertext `bxo tam det xzx pjl baj lqf asa mde ohy wpc wlb ajl` was encrypted with an autokey cipher. Decrypt it, using the knowledge that the word "the" appears.

2. Let $(1,2,3,4,5) \mapsto (5,3,4,1,2)$ be the key to a permutation block cipher.
   (a) Encrypt the plaintext `california`.
   (b) Decrypt the ciphertext `VENIU TYSIR`.

3. (a) Compute the inverse of 7 modulo 26.
   (b) Is the matrix $\begin{bmatrix} 1 & 5 \\ 3 & 2 \end{bmatrix}$ invertible? Why?
   (c) Find the inverse of $\begin{bmatrix} 4 & 3 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

4. Encrypt the plaintext `random` using a Hill cipher with key $K = \begin{bmatrix} 1 & 4 & 2 \\ 3 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix}$.

5. The ciphertext `YIFZMA` was encrypted by a Hill cipher with key $\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$. What was the plaintext?

6. The ciphertext `GEZXDS` was encrypted by a 2×2 Hill cipher. The plaintext is `solved`. Find the encryption key.

7. Suppose that the matrix $A = \begin{bmatrix} 2 & 3 \\ 4 & 3 \end{bmatrix}$ is used as the encryption key for a Hill cipher. Find two different (two-letter) plaintexts that encrypt to the same ciphertext.
   Why did this happen, and why is it a problem?

8. Suppose I encrypt a message with the Hill cipher, and the ciphertext is a sequence of one hundred `A`s. What can you tell me about the plaintext and the key?
   Does your answer change if the ciphertext is a sequence of one hundred `B`s instead?