

Math 401 Fall 2019
 Cryptology HW 3
 Due Thursday, September 19

1. Let $(1, 5, 2, 3, 4)$ be the key to a permutation block cipher.

- (a) Encrypt the plaintext **california**.
- (b) Decrypt the ciphertext **VENIU TYSIR**.

2. (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 $\begin{bmatrix} 4 & 3 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

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

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

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

6. 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?

7. Suppose I encrypt a message with the Hill cipher, and the ciphertext is a sequence of one hundred As:

AA
 AA

What can you tell me about the plaintext and the key?

Does your answer change if the ciphertext is a sequence of one hundred Bs instead?