Homework 7, due September 18

(1) Suppose the matrix $\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ is used for an encryption matrix in a Hill cipher. Find two plaintexts that encrypt to the same ciphertext. The plaintexts do not have to be in English.

(2) (Page 57, problem 18) Let a, b, c, d, e, f be integers mod 26. Represent a block of plaintext as a pair (x, y) (mod 26). The corresponding ciphertext (u, v) is

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

Describe how to carry out a chosen plaintext attack on this system and find the key a, b, c, d, e, f. You should state explicitly what plaintexts you choose and how to recover the key.

(3) The following ciphertext was encrypted by a Hill cipher with matrix

$$\begin{bmatrix} 1 & 0 & 5 \\ 7 & -1 & 9 \\ 4 & 6 & 3 \end{bmatrix}.$$

22 15 0 16 22 8 5 22 14 13 20 10 10 6 8 2 4 7 8 16 22

Decrypt.