SOEN 321
Exercise 1

(Although these questions will be solved with you during the tutorial, you should try solving them by yourself before the tutorial)

Prob. 1 Consider the affine cipher in which the ciphertext c is given by C= a P + b mod 26. The cryptanalyst observed the following plaintext/ciphertext pairs (p,c): (1,10) and (2,17).

1. Recover the key (a,b) used in the encryption system above.
2. What is the ciphertext corresponding to the plaintext p=3?

Prob. 2 Consider the Hill cipher in which the ciphertext is related to the plaintext using the form

(c1 c2)= (p1 p2) $\begin{pmatrix} k1 & k2 \\ k3 & k4 \end{pmatrix}$. mod 26

The cryptanalyst observed the following plaintext/ciphertext pairs (p1 p2)/(c1 c2): (1 2)/(16 23) and (3 3)/(1 16).

Determine the key corresponding to this system.