CS 402 Cryptography

Problem Sheet 2

Note: in all questions below, messages are split up into single-symbol units.

(1) You intercept the following ciphertext:

PXPXKXENVDRUXVTNLXHYMXGMAXYKXJN
XGVRFXMAHWGXXWLEHGZXKVBIAXKMXQM

which comes from shift encryption of a message composed of symbols from the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Use frequency analysis to recover the plaintext.

(2) In the 27-symbol alphabet consisting of a space (1 symbol) and the 26 letters

ABCDEFGHIJKLMNOPQRSTUVWXYZ

use the affine encryption function $f(n) \equiv 13n + 9 \mod 27$ to encrypt the message HELP ME

(3) An affine encryption function $f(n) \equiv an + b \mod 41$ has been used on plaintext composed of symbols from the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZØ123456789;,.?!

to produce the following ciphertext:

7NIIXI9ONPEBX,BG7QP7IULVQEOE7I9

Use frequency analysis to determine the encryption key (a, b) (assume that after "E", "T" is the most frequently occurring letter in plaintext messages of reasonable length written in English). Hence determine the decryption function and the plaintext.

(4) Consider the affine encryption function $f(n) \equiv an + b \mod p$, where p is prime and $a \not\equiv 1$. Show that there is always a symbol in the message alphabet that is the same when encrypted. What is that symbol in the previous question?