Exercises 6: homework questions

The following questions should be handed in for marking on Wednesday 3rd November

(1) The following is ciphertext encoded using a Caesar cipher. Find the cleartext.

HWWXEUXWH

(2) The following is ciphertext encoded using a Vigenère cipher with key $SCRAMBLE$. Find the cleartext.

NGEIHJOMNKTI

(3) List the invertible numbers modulo 26 and their inverses.

(4) Show that

$$\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$$

is an encryption matrix and find its inverse.

(5) A Hill cipher encrypts HAND as FUSS. Find the encryption matrix.

(6) Calculate $\phi(257)$ and $\phi(253)$.

The following questions should be handed in for marking on Wednesday 10th November

(1) A cryptosystem has $n = 77$ and $e = 43$. What was the private key?

(2) Let $p = 47$ and $q = 59$. Alice chooses $e = 157$ as her encryption (public) key. Show that this is a valid choice and find the corresponding decryption (secret) key. Alice receives the ciphertext (number) 1044 from Bob. Find the plaintext (number) that corresponds to it.

(3) Show that 5 is a primitive root modulo 23. Find x and y such that $2 = 5^x$ and $3 = 5^y$ modulo 23.