COMP 133
Assignment 1

The Caesar Shift Cipher

The Key: For my cipher the secret key shared by the sender and the receiver consists of a single number between 1 and 25.

How to Encipher: Given a key k, in order to encipher a message the sender takes each letter of the plaintext and replaces it by the letter that is k positions later in the alphabet. This is done with "wraparound" meaning that if you get to the end of the alphabet when counting up to k positions you continue counting from the beginning. For example, if the key is 3, then plaintext letter A gets replaced by D, B is replaced by E, etc. up to W is replaced by Z, X is replaced by A, Y is replaced by B and Z is replaced by C.

How to Decipher: Given a key k, in order to decipher the receiver takes each letter of the ciphertext and replaces it by the letter that is k positions earlier in the alphabet. Again this is done with wraparound so that when you reach A you continue counting with Z.

A Small Example:

```
Encryption:

Key: 7
Plaintext: cryptography is fun
Ciphertext: jyfwavnyhwof pz mbu
```

Notice that c gets replaced by j which is seven letters later in the alphabet, r by y, etc.

```
Decryption:

Key: 2
Ciphertext: oa hcxqtkvg encuu ku etavqitcrja
Plaintext: my favorite class is cryptography
```

Notice that o gets replaced by m which is two letters before it in the alphabet, a by y, etc.