Reading

Read: Chapter 1 and 2.1-2.4

Problems

1. Eve intercepts the message "NGZZK" encoded using a shift cipher. Can Eve recover the original message? If so what is it, and if not then why can't she?

2. Encrypt the message "helloworld" using an affine cipher sending $x \mapsto 5x + 7 \bmod 26$. What is the function to decipher? Test that it works.

3. In class we learned that the affine cipher $x \mapsto \alpha x + \beta \bmod 26$ only works if $\gcd(\alpha, 26) = 1$. To see why this is true, suppose that $\gcd(\alpha, 26) = d > 1$. Show that if $x_2 = x_1 + \frac{26}{d}$ then x_1 and x_2 encrypt to the same letter. How does this explain why you can't use this α?

4. The ciphertext EDSGICKXHUKLZVEQZVKXWKZUKCVUH was encoded using an affine cipher. Suppose it's known that the the first letter of plaintext is i. What is the deciphered message?

5. The operator of a Vigenère cipher is bored and decides to encrypt plaintext consisting of the same english letter repeated a few hundred times. Suppose the key for this cipher comes from a six letter English word.
   (a) Eve intercepts the ciphertext. What property of the ciphertext will lead Eve to guess the length of the key?
   (b) Now that Eve has the key length, how can she find the English word used to create the key? (Frequency can't help here since the original message only has one type of letter. One may check that there are no two six letter English words which are shifts of one another)

6. The cipher in the file Vigenere.txt contains a message which has been encoded using a Vigenere cipher. Figure out the key and decode the message. What is it?

7. **For Fun:** Newspapers commonly have a cryptoquip puzzle, which is a famous quote which has undergone a substitution cipher. To make the puzzle more manageable, spaces and punctuation and left in and one substitution is given. Try to decode the following quote:

   "ENBCNJZGE U OGB G ZYI. CYZGE U'T G ZYI. CYTYJJYO U'FF HJYMGMFE BCUFF MN G ZYI. BUIK! CKNJN'B BY FUCCFN KYHN QYJ GZDGRANTNRC" - BRYYHE

   given that Y = O.