Problem Set #2

Supplemental Problems

You will need to do some research to understand how the ciphers in these problems work. Be sure to give enough explanation so that someone else could understand, and *recreate*, the process you use in encryption and decryption.

1. Use a Vigenère cipher with key $k = TOESOCKS$ for this problem.

   (a) Encrypt the message

   > "In right angled triangles the square on the side opposite the right angle equals"

   FYI, this is beginning of Proposition 47 from Book1 of Euclid's *Elements*. The complete statement is:

   > In right angled triangles the square on the side opposite the right angle equals the sum of the squares on the sides containing the right angle.

   This is how Euclid stated the Pythagorean Theorem, rather than the abbreviated $a^2+b^2 = c^2$ that you may know (implicit in this are that a, b, c are the side lengths of a right triangle where c is the length of the hypotenuse). The ancient Greeks did not have the Arabic numerals or algebraic notation that is familiar to us.

   (b) You receive the encrypted message

   ```
   BVEN SFSK VCZW FGNS MFYD MTOE TFOS PNOH KCSX
   KJSU AHLA GOKJ ZWRA GVYG LAED ZVYU HBXS WP
   ```

   Decrypt the message. Who sent the message?

   Explain the context of the message in a couple of sentences.

2. Use an autokey cipher with key $k = NEZUKO$ for this problem.

   (a) Encrypt the message

   > "I learned that beneath my goody two shoes lie some very dark socks"

   (b) You receive the encrypted message

   ```
   VXRV KBMR GVKA SUWN COOJ MBEI EEIM HLVP HETX FBG
   ```

   Decrypt the message. Who sent the message?