Julia Sterling **Homework 2** **Due 09-12-2014**

1. Encrypt the message "If at first you don't succeed, failure may be your style." using the mono-alphabetic substitution with keyword "taxes" and key letter "j".

2. You intercept the following message sent by Alice to Bob:

   ```
   QEQU UJMW MICR PMVQ AAQA AQYY QCQB MCJG RPMJ UDMJ CQLO MIRA QFXK UXKT
   RXVX CCXE
   ```

   Through your extensive network of spies you know the following information: Alice always sends Bob messages enciphered with mono-alphabetic substitution with a four-letter keyword. Also you know that tomorrow Alice has decided to have a meeting with Bob by mississippi river. The only problem is that you don't know when.

   (a) Discover when Alice is planning to meet Bob.

   (b) Roughly where are they meeting?

   (c) Discover what her key word was used so that you can break more of her codes.

3. Encrypt the message "These pretzels are making me thirsty" with Vigenere with keyword "five".

4. Break this chiphertext that was enciphered using Vigenere with a two letter keyword (the keyword will not necessarily be a real dictionary word):

   ```
   HQ SV CW YN MM CN GW CC ZR YN PJ BJ BJ G
   ```

   given that "bananas" appears in it.

5. For each of the following decide if $a|c$. Make sure to explain your answer.

   (a) $a = 3564, c = 17285400$

   (b) $a = 1968, c = 14628151$.

6. Use the vigenere applet at

   ```
   http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html.
   ```

   Choose a random ciphertext and try to break it. Write down the keyword. This might not work since they have change Java security. You might look at this and see if you can get it to work:

   ```
   https://www.java.com/en/download/exception_sitelist.jsp.
   ```

   If it doesn't work don't worry about it just write that you couldn't get it to work. I'll continue to work on figuring out a workaround.

7. Suppose you had a computer that could attempted to apply a mono-alphabetic substitution and see if the result was English at the rate of 10,000 per second.
   (a) How long would it take to try all possible mono-alphabetic substitution keys? Convert your answer to a reasonable unit.
   (b) What if the method of a key word (for some dictionary) and key letter were used? How long would it take to try all possibilities in this case? (I will accept any reasonable estimate for the approximate number of words in a dictionary that you can find online.)
   (c) Explain why IT people tell you not to use dictionary words for your password.
8. Find the following places on campus and take a picture of yourself there and send it to me.
   (a) A workout room or swimming pool on campus.
   (b) An advanced mathematics book of your choice in the library.