Alexis Schloetter **Homework 2** **Due 09-13-2013**

1. Encrypt the message "If your parents never had children, chances are you won't, either." using the mono-alphabetic substitution with keyword "right" and key letter "w".

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

   ```
   XSPS VVSH PFFX PFQF BVXK FCOY FCVL EJFS ZFVX KFPL WWLW WLTT LVLZ FVBX
   XHSS DOSD N
   ```

   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 "rice".

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

   ```
   AB LE PH NC ZA VC UA IU UU UU ZN LF SH VI UY
   ```

   given that "bananas" appears in it.

5. Find q, r with $0 \leq r < a$, so that $b = a \cdot q + r$ with:

   (a) $a = 42830, b = 1191054$

   (b) $a = 188554, b = -1640195$.

   (c) $a = 34523, b = 21840$.

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.

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.