Assignment 8

RWH

due November 3 2015

Another encryption assignment

1. **Vernam Encryption** Write a program in C that will encrypt a file use XOR and a Vernam key. A Vernam key is a short string. (The real system used a much longer random sequence.) Read the input at low level, as binary data (hint unsigned char is useful here.) Then xor each character in the binary data with the character in the key. When you get to the end of the key reuse the key from the beginning.

   The program should take command line arguments for the key, input and output.

   ```
   ./vern abc input.clear output.encrypted
   ```

   Note that the cipher should decrypt its own output. The command:

   ```
   ./vern abc output.encrypted input.clear
   ```

   should recover the original input. If you use open to create the output file, you may want to also set O_RDWR or O_WRONLY as well as O_CREAT. You could also use fread and fwrite for this problem.

2. **Finding the period**

   This cipher is vulnerable if the key repeats, and with a short key, like abc above, it will repeat many times for any reasonably sized input.

   The incidence of coincidence slides the cipher along itself and counts the number of times the same symbol is seen.

   ```
   ABCABCABC    count is 9
   ABCABCABC
   then shift 1
   ABCABCABC    count is 0
    ABCABCABC
   then shift 2
   ABCABCABC    count is 0
     ABCABCABC
   then shift 3
   ```

```
ABCABCABC    count is 6
   ABCABCABC

Clearly the period is 3.
```

Write the code to do that. The file classcipher.vrn is in my directory for this.

3. **EXTRA CREDIT** The character ' ' (space) is most common in English text. After finding the period count the most common character for each period and recover the key by XOR'ing it with ' '.