Homework 1, Due Tue July 14, 2015

NOTE- THIS HW IS TWO PAGES LONG. DO NOT IGNORE THE SECOND PAGE.

NOTE- FOR THE AFFINE CIPHER *the multiplier* MEANS WHAT I CALLED a AND *the additive term* MEANS WHAT I CALLED b

1. (10 points) What is your name? Write it clearly. Staple your HW. What High School are you from? If you have never gotten an email from me then email me.

2. (10 point AND this will help you with the next two problems) Assume Alice and Bob use a shift cipher with shift 5. Write down the correspondence table for both encoding and decoding.

3. (10 points) Assume Alice and Bob are using shift cipher with shift 5. If Alice wants to send *Computer Science is a Great Major* what does she send (remember that she before coding she breaks the message into blocks of five and only uses capitol letters).

4. (10 points) Assume Alice and Bob are using shift cipher with shift 5. If Alice receives the message *MNQFW DFSIO DGBNQ GJKWN JSIX* then what did Bob send?

5. (10 points and this will help you with the next two problems) Assume Alice and Bob use an affine cipher with multiplier 5 and additive term 2. Write down the correspondence table for both encoding and decoding.

6. (10 points) Assume Alice and Bob are using an affine cipher with multiplier 5 and additive term 2. If Alice wants to send *Computer Science is a Great Major* what does she send (remember that she before coding she breaks the message into blocks of five and only uses capitol letters).

7. (10 points) Assume Alice and Bob are using an affine cipher with multiplier 5 and additive term 2. If Alice receives the message *MLCFF WOHCH HCGWI COCLW CRUBL QOTQK W* then what did Bob send.

8. (10 points) For this problem we are operating mod 7.

   (a) For each number in $x \in \{0, 1, 2, \ldots, 6\}$ find $-x$, that is find a number y such that $x + y \equiv 0 \pmod 7$.

   (b) For each number in $x \in \{1, 2, \ldots, 6\}$ find $1/x$, that is find a number y such that $xy \equiv 1 \pmod 7$.

9. (20 points) In Fredonia they have 18 letters in their alphabet They want to use an affine cipher, that is, we want to code the number $x \in \{0, 1, \ldots, 17\}$ by the number $ax + b \pmod{17} \in \{0, 1, \ldots, 17\}$. List all the numbers that CAN be used for a. List all the numbers that CAN be used for b.

10. (OPTIONAL) Write a program that will, given a text and a number s, produce the output of the Shift Cipher when shifted by s. Also write a program that will, given an s and given a message that was coded by a shift cipher with shift s, decodes it. Test both of them with each other.