MAT 258 - CODING ASSIGNMENT #2
due Friday, November 10, 2017 at 11:50PM.

OBJECTIVE: Students will implement simple algorithms used in secret sharing problems.

GRADING: The assignment is worth 5% of your course grade.

INSTRUCTIONS:

- Students may work individually or in pairs. Each team must submit their own code, but they may ask questions and clarification from classmates and the instructor.
- Students may use algorithms discussed in class, in the textbook or from other resources.
- Students must submit their projects on Moodle.

PROJECT:

1. **Shift Cipher:** I used a shift cipher $f(x) = x + a \pmod{26}$ to encode the message M.
   - Write a program to find the shift a and decode the message: decode the message using all 26 possible shift values and the user will pick the one that makes sense.
   - Test your program for the encoded message "$DOFKVFVBSPRLNHTLZ$". Include a and M in your *Answer Sheet*.

2. **Smart Shift Cipher Decoder:** I used a shift cipher $f(x) = x + a \pmod{26}$ to encode a message.
   - Write a program to find the shift a, by looking at frequencies of letters. A table of letter frequencies for English can be found here:
     `http://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html`
     (a) User will input a (long) encoded text c.
     (b) Your program will compute letter frequencies for the text c.
     (c) Use the most frequent letter to find the shift a. (Hint: what letter does it encode?)
     (d) Decode c, using the shift a you found in (c).
   - Test you program with the following c. Once decoded, the text should make sense.
     ZNGURZNGVPFNFNARKCERFFVBABSGURUHZNAZVAQERSYRPGFGUR
     NPGVIRJVYYGURPBAGRZCYNGVIRERNFBANAQGURQRFVERSBENRF
     GURGVPCRESRPGVBAVGFONFVPRYRZRAGFNERYBTVPNAQVAGHVGV
     BANANYLFVFNAQPBAFGEHPGVBATRARENYVGLNAQVAQVIVQHNYVGL
   - Include the frequency table, the shift a, and the decoded message in your *Answer Sheet*.

3. **Extended Euclidean Algorithm:** Find $\gcd(a, b)$ and the inverse of a modulo b, if it exists.

   - Write a program that does the following:
     (a) Input positive integers a and b

     (b) Find $\gcd(a, b)$.

     (c) If $gcd(a, b) = 1$, find the inverse of a modulo b, otherwise state "inverse does not exist".
   - Test your program with $a = 1234567$ and $b = 1333331$. Include output in the *Answer Sheet*.

4. **Chinese Remainder Theorem:** k friends will collectively open a safe. What they know:

   (i) Each friend knows a *different* pair of integers (d_i, r_i), $1 \leq i \leq k$.

   (ii) When the code to the safe is divided by d_i, the remainder is r_i.

   (iii) The code is the smallest non-negative integer that works for all k friends.

   - Write a program to find the secret code:
     (a) Input the number of people k

     (b) Input k pairs of integers, making sure the divisors are relatively prime.

     (c) Use the Chinese Remainder Theorem to solve the system of congruences.
   - Test your program with pairs $(27, 16), (16, 3), (35, 6), (59, 2)$ and include it in your *Answer Sheet*.

SUBMIT THE FOLLOWING:

- An executable. This should be able to run on a clean machine, please compile it accordingly.
- A read-me file explaining how to run your code.
- *Answer Sheet* with answers to the specific problems.