HW 7 CMSC 456. DUE Nov 5
Will Be Graded By Nov 12
Regrade Requests Due by Nov 19 NO DEAD CAT POLICY
SOLUTIONS
NOTE- THE HW IS TWO PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly.

2. (30 points) Look up the Euclidean Algorithm to find the Greatest Common Divisor of two numbers.

   (a) (5 points) Write a program to implement the algorithm.

   (b) (5 points) Modify it (actually add to it) so that if it is given (a, b) which are relatively prime it finds the inverse of a mod b.

   (c) (10 points) Use your program to find the GCD of all (a, b) such that $50 \leq a < b \leq 60$, and

   (d) (10 points) Use your program to find, for all $1 \leq x \leq 100$, the inverse of x mod 101.

   SOLUTION TO PROBLEM TWO

   Omitted

3. (30 points) Dr. Batz is trying to factor a large number N using the method that worked on the Jevon's Number. So he wants to find x, y such that $x^2 - y^2 = N$. Instead he finds x, y such that

$$x^2 - y^2 \equiv 0 \pmod{N}$$

   (a) Tell her how she might be able to use this.

   (b) Will there be scenarios where x, y do not help?

   SOLUTION TO PROBLEM THREE

   1) $x^2 - y^2 = N$

   $(x - y)(x + y) = kN$ for some k.

   It is possible that $x - y$ and N share a factor.

It is possible that $x + y$ and N share a factor.

Take $GCD(x - y, N)$ and $GCD(x + y, N)$, hoping to find a factor.

2) It is possible that $x+y = N$ and $x-y = k$ (or the other way around) in whichc case the technique will not get factors.

THERE IS ANOTHER PAGE. GOTO IT!!!!!!!!!

4. (20 points) Read the slides for Misc Crypto where I talk about making the Vig Cipher better. We will be using that method throughout this question. FOR THIS PROBLEM WE USE $A = 1$, $B = 2$, etc, $Z = 26$.

   (a) Alice says to Bob *NSF Good*. Give the resulting key. (It will be a sequence of numbers)

   (b) Alice says to Bob *Problems with a Point*. How long is the resulting key? (You DO NOT need to find the key.)

   (c) Give two phrases p_1 and p_2 (in English) where p_1 has LESS letters than p_2, but using p_1 results in a LONGER key.

SOLUTION TO PROBLEM FOUR

a) We first write down FBI and GOOD in a row

N	S	F	N	S	F	N	S	F	N	S	F
G	O	O	D	G	O	O	D	G	O	O	D

We then translate these letters to numbers and add them up mod 26 column-wise

14	12	6	14	19	6	14	19	6	14	19	6
7	15	15	4	7	15	15	4	7	15	15	4
21	1	21	18	0	21	3	23	13	3	8	10

b)

Problems has 8 letters

with has 4 letters

a has 1 letters

Point has 5 letters

So the answer is the LCM of 8,4,1,5 which is 40.

c) Since the length of the key is the LCM it is short if the numbers share common factors but long if they don't.

Let p_1 be *CMSC ROCKS*

CMSC has 4 letters

ROCKS has 5 letters

Hence p_1 is 9 letters. The LCM of 4 and 5 is 20, so the keylength is 20.

Let p_2 be: *Introduction to Modern Math*

Introduction has 12 letters

to has 2 letters

Modern has 6 letters

Math has 4 letters

The number of letters in $p1$ is 24. The key-length is LCM of 12,2,6,4 which is just 12.

5. (20 points) Alice and Bob are bridge partners. And they cheat! Here is their scheme:

   - If the first card is placed horizontally then the person placing it has 0 or 1 Ace.
   - If the first card is placed Vertically then the person placing it has 2 or 3 or 4 Aces.

   In this problem we will both Alice and Bob and also help the bridge community.

   (a) Alice and Bob will be playing 20 games and are worried that their cheating may be discovered. Show how they can use a 1-time pad to make their cheating harder to discover.

   (b) Change something about how Bridge is played so that Alice and Bob cannot use their method to cheat.