HW 08 CMSC/MATH/ENEE 456. Morally DUE Nov 16, 12:30PM

1. (40 points) Write programs for the following:

   (a) (0 points but you will use it later, so you should test it yourself.) Program CRT: Given c_1, N_1, c_2, N_2 find x such that

   $$x \equiv c_1 \pmod{N_1}$$
   $$x \equiv c_2 \pmod{N_2}$$

   (b) (0 points but you will use it later, so you should test it yourself.) Program NATURAL-SQRT: Given $x \in \mathbb{N}$ output

   - 0 if $\sqrt{x} \notin \mathbb{N}$.
   - $\sqrt{x}$ if $\sqrt{x} \in \mathbb{N}$.

   (c) (40 points) Zelda is going to send messages to both Alice and Bob. They are using RSA with $e = 2$ (Why? Because they are dumb as doughnuts.) Write a program to help Eve decode the messages using the low-e attack. More precisely:

   Program LOW-E: Input is c_1, N_1 and c_2, N_2. Eve knows that there exists m such that

   $m^2 \equiv c_1 \pmod{N_1}$ and

   $m^2 \equiv c_2 \pmod{N_2}$.

   Output is either

   - 0 if from this information the low-e attack won't work.
   - m if from this information the low-e attack works.

   Sample input/output:

   - Input: $c_1 = 8, N_1 = 17, c_2 = 25, N_2 = 37$
   - Output: 5

GOTO NEXT PAGE FOR HOW TO SUBMIT

In your main method, you should take as input c_1, N_1, c_2, N_2 and output LOW-E(c_1, N_1, c_2, N_2), which should be m or 0.

(a) Your input (c_1, N_1, c_2, N_2) will be given as command line arguments, in that order. Expect your filename to be the first argument at index 0, c_1 to be the second at index 1, etc.

There is no input read through standard input.

(b) Your output should be printed to standard output. This should be an integer (ex: "5" instead of "5.0"), and this integer should be the ONLY thing printed to stdout.

(c) You should upload a **single** file ending in `.java`, `.py`, `.ml`, `.rb`, `.c`, `.cpp`, or `.scala`, corresponding to Java, Python3, OCaml, Ruby, C, C++, and Scala respectively.

GOTO NEXT PAGE

2. (30 points- 6 points each) Zelda is going to do RSA with both Alice and Bob.

   (a) To set up RSA, Zelda sends Alice $(55, 33)$, so $N = 55$ and $e = 33$. Find the value of d.(YES it does exist.)

   (b) To set up RSA, Zelda sends Bob $(55, 23)$, so $N = 55$, $e = 23$. Find the value of d. (YES it does exist, though this time you probably did not doubt that.)

   (c) Alice is now ready to send Zelda messages! Alice sends Zelda 13. Show what Zelda does to recover the message, and of course show us the message as well. (You can use a calculator.)

   (d) Bob is now ready to send Zelda messages! Bob sends Zelda 2. Show what Zelda does to recover the message, and of course show us the message as well. (You can use a calculator.)

   (e) Eve tries to use the Same-N attack. Show what Eve does to recover the message, and of course show us the message as well. (You can use a calculator.)

GOTO NEXT PAGE

3. (30 points)

Definition A triple of numbers N_1, N_2, N_3 is *pairwise relatively prime* if N_1, N_2 are rel prime AND N_1, N_3 are rel prime AND N_2, N_3 are rel prime. Note that N_1 is rel prime to N_2N_3, N_2 is rel prime to N_1N_3, and N_3 is rel prime to N_1N_2.

And now to our problem.

Prove the following (its the Chinese Remainder theorem for $L = 3$).

Let $a, b, c, N_1, N_2, N_3 \in \mathbb{N}$ such that N_1, N_2, N_3 are pairwise relatively prime. Then there exists x such that the following hold:

$0 \leq x < N_1N_2N_3$

$x \equiv a \pmod{N_1}$

$x \equiv b \pmod{N_2}$

$x \equiv c \pmod{N_3}$.

(You may use that if d, e are rel prime then d has an inverse mod e.)