Homework due Monday, December 2, 11:59pm

This assignment requires some computer use. You may use whatever software you are familiar with, but the computational parts of this assignment can be done with Sage online here: `https://sagecell.sagemath.org/`. All you will need is to write a for loop and perform modular arithmetic operations. If you are unsure about or stuck on any part of the programming, please send me an email.

(1) Use the Euclidean algorithm to compute $e^{-1} \pmod{m}$ (by hand) for each e and m.
   (a) $e = 22, m = 101$
   (b) $e = 31, m = 253$
   (c) $e = 413, m = 619$

(2) Suppose Alice and Bob are doing Diffie-Helman key exchange with the public $p = 104729, g = 12$. Alice sends Bob $A = g^a = 97951$ and Bob sends Alice $B = g^b = 11884$. Show that the prime p is too small to be secure: use a computer to determine their shared secret $s = g^{ab}$.

(3) The *Carmichael totient function* $\lambda(n)$ is the smallest m such that $a^m \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^\times$. We can compute this using the Chinese Remainder Theorem and our knowledge of the structure of $\mathbb{Z}_n^\times$. For example,

$$\begin{aligned} \mathbb{Z}_{105}^\times &\cong \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times \times \mathbb{Z}_7^\times \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \end{aligned}$$

Then $\lambda(105) = \mathrm{lcm}(2, 4, 6) = 12$.
   (a) Determine $\lambda(77)$, $\lambda(162)$ and $\lambda(210)$.
   (b) Show that $\lambda(n) \mid \phi(n)$ for all n. You may need the fact that

$$\mathbb{Z}_{2^\ell}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\ell-2}},$$

   and you may assume this freely.
   (c) Suppose Alice has public key (n, e) where $n = pq$ and Alice receives the $c = m^e \pmod{n}$. Show that Alice can recover m by computing $d = e^{-1} \pmod{\lambda(n)}$ instead of $e^{-1} \pmod{\phi(n)}$.

(4) A *semiprime* is the product of two primes. In RSA, we must choose a large semiprime, but we need to be careful about how we choose the prime factors.
   (a) Show that if $n = pq$ is odd, then n is the difference of two perfect squares. That is, $n = x^2 - y^2$. Recall homework 1, problem 4.
   (b) *Fermat factorization* is a factoring method relying on the above. We guess a value of x, then compute $x^2 - n$. If the result is a perfect square, then we can solve for y and factor n. What is the *smallest* value of x that is possible? That is, what is the first value of x we should check?

(c) Given the semiprime $n = 1940050770913277826811085782601227945929717660407062879$, find its two prime factors using Fermat factorization (use a computer for the calculation). WolframAlpha cannot factor this! (You do not have to prove n is semiprime, only factor it)