Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. [JJJ 3.6] Alice publishes her RSA public key $(N, e) = (2038667, 103)$.
   (a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?
   (b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.
   (c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.
2. [JJJ 3.7] Bob's RSA public key has modulus $N = 12191$ and exponent $e = 37$. Alice sends Bob the ciphertext $c = 587$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. *Hint:* N has a factor that is less than 100.
3. [JJJ 3.8] For each of the given values $N = pq$ and $N' = (p-1)(q-1)$, use the method in the proof that **FactorN** is at least as easy as **ComputeN'** to find p and q.
   (a) $N = 352717$ and $N' = 351520$
   (b) $N = 28424293$ and $N' = 28411488$
   (c) $N = 111702827046011$ and $N' = 111702805302024$.
4. Consider the following two problems.

   FactorN Given an integer N that is the product of distinct, unknown primes p and q, output p and q.

   Reduce Given an integer a and an integer N that is the product of distinct, unknown primes p and q with $p < q$, output $b \in \mathbb{Z}_p$ and $c \in \mathbb{Z}_q$ such that $a \equiv b \pmod{p}$ and $a \equiv c \pmod{q}$.

   (a) Prove that **Reduce** $\leq$ **FactorN**.
   (b) Prove that **FactorN** $\leq$ **Reduce**.
   (c) Illustrate part (b) by factoring $N = 446846784807308867$. Given $a = 723728945230$ and N, your black box for **Reduce** reports that $a \equiv 299450419 \pmod{p}$ and $a \equiv 316955067 \pmod{q}$.