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

1. [JJJ 3.1] Solve the following congruences.
   (a) $x^{19} \equiv 36 \pmod{97}$.
   (b) $x^{137} \equiv 428 \pmod{541}$.
   (c) $x^{73} \equiv 614 \pmod{1159}$.
   (d) $x^{751} \equiv 677 \pmod{8023}$.
   (e) $x^{38993} \equiv 328047 \pmod{401227}$. *Hint:* $401227 = 607 \cdot 661$.

2. [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.

3. [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.

4. [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 $N' = 111702805302024$.

5. 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 $a \equiv 316955067 \pmod{q}$.

6. Suppose we know $N = pqr$, where p, q, and r are large, distinct, unknown primes. Somehow, we also know $N' = (p-1)(q-1)(r-1)$.

   (a) Use CRT to show that if $\gcd(a, N) = 1$, then $a^{N'} \equiv 1 \pmod{N}$.

   (b) Show that if $z^2 \equiv 1 \pmod{N}$ but $z \not\equiv 1 \pmod{N}$ and $z \not\equiv -1 \pmod{N}$, then either $\gcd(z+1, N)$ or $\gcd(z-1, N)$ equals one of the three prime factors of N.

   Comment: if we pick a random nonzero $a \in \mathbb{Z}_N$, then it is very likely that $a \in \mathbb{Z}_N^*$ (and if not, then $\gcd(a, N)$ will give a nontrivial factor of N, such as p or qr). For $a \in \mathbb{Z}_N^*$, we know $a^{N'} \equiv 1 \pmod{N}$. Consider the sequence $a^{N'}$, $a^{N'/2}$, $\ldots$, $a^{N'/2^t}$, where t is the number of two's in the prime factorization of N'. It can be shown that with probability at least $3/4$, there exists j with $0 \le j < t$ such that $a^{N'/2^j} \equiv 1 \pmod{N}$ but $a^{N'/2^{j+1}} \not\equiv 1 \pmod{N}$ and $a^{N'/2^{j+1}} \not\equiv -1 \pmod{N}$.

7. We are given integers N and N' below, where $N = pqr$ for distinct primes p, q, and r, and $N' = (p-1)(q-1)(r-1)$. Use the technique discussed in the previous problem to factor N into p, q, and r.

$$
\begin{aligned}
N = \; & 725742825587494781218319617775223529799228913737 32 \\
& 5264008188876884904377402290644654280541022108595 3 \\
& 0032075325376583061735775981061610994693799435882 6 \\
& 0698651454669769173922877178980743016174048000845 9 \\
& 9451938857981877709365770088401103514695589151163 2 \\
& 7092987160493189478530181096724357212548958455694 0 \\
& 4547310749373791601000137268301548724007626349575 5 \\
& 4174139156443062049587844820624882439017613249974 3 \\
& 0846472350789665547145078664543729098125406167550 6 \\
& 591968920507
\end{aligned}
$$

$$
\begin{aligned}
N' = \; & 7257428255874947812183196177752235297992289137373 2 \\
& 5264008188876884904377402290644654280541022108595 3 \\
& 0032075325376583061735775981061610994693799435882 6 \\
& 0696215045972653998554650944509103699952303388068 7 \\
& 5864099295706021801337188078563852749083886676619 1 \\
& 7347742491738156885412419567947220633766410428577 2 \\
& 8779242424696798217131372348744385120350939717681 6 \\
& 3943609542086910281157234535395733863709346846958 5 \\
& 2058501331141904514855682261873893235590452971621 2 \\
& 332777917280
\end{aligned}
$$