Name: ______________________ Score (Out of 9 points):

A non-programmable, non-scientific calculator may be used.

1. This question concerns the uses of Fermat's Little Theorem in primality testing.

   We recall that Fermat's Little Theorem states the following: If $p > 0$ is a prime integer, and a is any unit modulo p, then $a^{p-1} \equiv 1 \pmod{p}$.

   (a) [2 points] Suppose that you compute $2^{589,312} \equiv 111,577 \pmod{589,313}$. What can you conclude, if anything, about whether $589,313$ is prime? Briefly explain.

   The number $n = 589,313$ is not prime. If it were, then Fermat's Little Theorem would imply that $a^{n-1} \equiv 1 \pmod{589,313}$ for any unit a modulo $589,313$, including $a = 2$. Since 2^{n-1} is not congruent to 1, n cannot be prime.

   (b) [2 points] Suppose that you compute $2^{78,552} \equiv 1 \pmod{78,553}$. What can you conclude, if anything, about whether $78,553$ is prime? Briefly explain.

   The number $n = 78,553$ may or may not be prime. Because $2^{n-1} \equiv 1 \pmod{n}$, it is consistent with the conclusion of Fermat's Little Theorem. In fact, it is rare that $2^{n-1} \equiv 1 \pmod{n}$ for composite numbers n, so the result strongly suggests that the number n is prime, but ultimately the test is inconclusive.

 The quiz continues on the back of the page.

2. You are communicating privately with a colleague using RSA.
   You publish modulus $n = 133 = (7)(19)$ and the encryption exponent $e = 7$.

   (a) [1 point] Find $\phi(n)$.

   $$\phi(n) = (7-1)(19-1) = 108$$

   (b) [2 points] Find a decryption exponent d.

   We run the Euclidean algorithm on 7 and 108 to find a multiplicative inverse to 7 modulo 108:

   $$\begin{aligned} 108 &= 15(7) + 3 \\ 7 &= 2(3) + 1 \end{aligned}$$

   $$\begin{aligned} 1 &= 7 - 2(3) \\ 1 &= 7 - 2(108 - 15(7)) \\ 1 &= 31(7) - 2(108) \end{aligned}$$

   And so $d = 31$ is a suitable decryption exponent.

   (c) [2 points] Your colleague sends you the message $5 \pmod{n}$. Decrypt it.
   If you don't have a calculator, you can leave your answer as an umsimplified product.

   You may find the following helpful:

   $5^2 \equiv 25 \pmod{n}$, $25^2 \equiv 93 \pmod{n}$, $93^2 \equiv 4 \pmod{n}$, $4^2 \equiv 16 \pmod{n}$, $16^2 \equiv 123 \pmod{n}$

   We need to compute $5^d \pmod{n}$. First, we write d as a sum of powers of 2:

   $$d = 16 + 8 + 4 + 2 + 1$$

   $$\text{Then} \qquad \begin{aligned} 5^d &= 5^{16+8+4+2+1} \\ &= 5^{16}5^{8}5^{4}5^{2}5^{1} \\ &\equiv (16)(4)(93)(25)(5) \pmod{n} \\ &\equiv 744,000 \pmod{n} \\ &\equiv 131 \pmod{n} \end{aligned}$$

   We conclude that the decrypted message is 131.