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.

   (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.

   (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 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 $\phi(n)$.

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

   (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:

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