Name: _____

Read and take notes on the introduction to Chapter 13, Section 13.1 Fermat Pseudoprimes, and Section 13.2 Non-Prime Pseudoprimes.

Reading Questions

1. Make sure you are familiar with the following terminology: pseudoprime, witness, false witness/liar, Fermat pseudoprime, Fermat pseudoprime base b, Fermat witness, Fermat false witness/liar, Carmichael number.

2. What can we gain by 'sacrificing' certainty in primality testing? Why does this matter for modern cryptosystems?

3. What does Fermat's Little Theorem say? Give two equivalent ways of stating the result. (Make sure to include the quantifiers at the beginning of the sentences!)

4. True or false, with explanations.

   (a) If an odd integer n is prime, then $2^{n-1} = 1 \bmod n$.

   (b) An odd integer n is prime if $2^{n-1} = 1 \bmod n$.

(c) If $b^{n-1} = 1 \bmod n$ for all b relatively prime to n, then n is prime.

5. (a) Give an example of a non-prime Fermat pseudoprime. (There are eight listed in Section 13.1.)

(b) Use the first proposition in Section 13.2 to generate another non-prime Fermat pseudoprime from the one you gave in (a). (Give a formula for this number rather than trying to write out all the digits.)

(c) Use the second proposition in Section 13.2 to generate another non-prime Fermat pseudoprime.

6. What struck you in this reading? What is still unclear? What remaining questions do you have?