Cryptology
Assignment

Due Friday, March 24, at 10:15.

Note that this is an actual assignment which must be approved in order to take the exam in June. You may not work with others on the assignment. It must be turned in by 10:15 on Friday, March 24. If it is late, it will not be accepted. There will be no chance to redo the assignment if it is not acceptable the first time.

1. Do problem 4.7 in the textbook.
For 4.7b, I recommend using the PowerMod function in Mathematica.
2. Do problem 4.13 in the textbook. Explain why you get the answers you do and how you could figure these out simply by factoring the n and $n-1$. (You can check your answer by writing a short program. The numbers are small enough that you can use simple int variables in C.)
3. Do problem 4.18 in the textbook.
You may use either the defintion of the Rabin Cryptosystem used in the textbook or the one I gave in class, but make it clear which one you are using. Explain what calculations you did; a correct result alone is insufficient.