Cryptology
Problems

To be discussed Monday, March 13, 2000.

1. First, we will discuss the problems from the first assignment.

2. Do problems 3.2 and 4.4 in the textbook.

3. Look at problems 4.1, 4.2, and 4.3 in the textbook, plus the problem listed below. If you are at all unsure of how to do them, please do them. Even if you are not unsure, you might consider this an opportunity to try using Mathematica (which is even more useful for problem 4.4 above). To do this, you can login to wagner and type "math" or "mathematica" (with "mathematica", in order to get it to perform a calculation, you can do "shift return"). To find out how to use a function such as "PowerMod", you can type "?PowerMod". If you want a list of all functions which contain a string such as "Mod", you can type "?*Mod*". Some relevant functions for this course are "Mod", "PowerMod", and "ExtendedGCD". To get out of Mathematica in "math", you type "Quit".

Another easy problem. Let $n = 143$ be a modulus for use in RSA. Choose a public encryption exponent e and a private decryption exponent d which can be used with this modulus. Try encrypting and decrypting some value to see that the exponents you have chosen work.

4. Do problems 4.11, 4.14, and 4.15 in the textbook. (For 4.14, skip part (b), but assume the result there for the later subquestions.)
In problem 4.11, it should say "having success probability", rather than "having failure probability". In 4.15c, the floor symbol should be a ceiling.

5. Calculate the Jacobi symbols $\left(\frac{16}{57}\right)$, $\left(\frac{20}{59}\right)$, and $\left(\frac{23}{59}\right)$.