Cryptology
Assignment

Due Friday, March 23, 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 23. 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. You may use Maple for the calculations.

1. Do problems 4.8 and 4.9 in the textbook.

2. 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.

3. Suppose that RSA is implemented using the public keys, $N = 221$ and $e = 77$.

a. While encrypting the plaintext 160, repeated squaring was used, and the following results were obtained:

$$\begin{array}{lll}
160^2 & \bmod 221 & = & 185 \\
160^4 & \bmod 221 & = & 191 \\
160^8 & \bmod 221 & = & 16 \\
160^{16} & \bmod 221 & = & 35 \\
160^{32} & \bmod 221 & = & 120 \\
160^{64} & \bmod 221 & = & 35 \\
160^{72} & \bmod 221 & = & 118 \\
160^{76} & \bmod 221 & = & 217 \\
160^{77} & \bmod 221 & = & 23
\end{array}$$

The intermediate results which were obtained give a cryptanalyst some very useful information for factoring the modulus. What was so interesting?

(Hint: Look at the results of the different squarings.) Show how to use this information to factor 221.

b. What is the decryption exponent d?

Problems

To be discussed Wednesday, March 14, 2001.

1. Do problems 4.4, 4.7, 4.11, 4.14 in the textbook. (For 4.14, skip part (b), but assume the result there for the later subquestions.)

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