Cryptology
Problems

To be discussed Wednesday, March 21, 2001.

1. Do problems 4.10, 4.17 and 4.14b in the textbook.
(The last one was skipped earlier because it is hard. Try it now.)

2. With RSA, there are often recommendations to use a public exponent $e = 3$.

a. What would the advanatage to this be?

b. If $e = 3$, the two prime factors dividing the modulus, p and q, must be such that $p \equiv q \equiv 2 \pmod 3$. Why is it impossible to have one or both of p and q congruent to 0 or 1 modulo 3?

c. Suppose that $e = 3$, $p = 3r+2$ and $q = 3s+2$. What would the decryption exponent d be?