Cryptology
Problems

To be discussed Monday, May 1, 2000.

1. Do problems 6.1.a, 6.1.b, and all of 6.5 in the textbook.

2. (From Salomaa's textbook) In the ElGamal Signature Scheme, what is the effect on ecryption, verification, and security if α is not primitive element? (Note that α should be a primitive element, so this would change the scheme somewhat.)

3. In the discussion of DSS on page 210, it says that to find a qth root of 1 modulo p, one should begin with a primitive element α_0 of Z_p and compute $\alpha_0^{(p-1)/q}$.

   a. Why is this correct? What subgroup does the result generate?

   b. How long does it take to do this computation?

   c. Is it necessary that α_0 be a primitive element?

4. In the verification protocol for undeniable signatures, the verifier chooses randomly two values e_1 and e_2. Why are there two values? Why not just let $e_2 = 0$ always?