Problem Set 4

Due on Thursday, October 26, 2006.

Problem 17: Diffie-Hellman Key Exchange

Alice and Bob use the Diffie-Hellman key exchange protocol (section 58, lecture notes 11) with prime $p = 29$ and primitive root $g = 2$. Alice chooses $x = 5$, Bob chooses $y = 3$.

(a) Use the Lucas test (section 56, lecture notes 11) to show that 2 is a primitive root of 29.

(b) What are the public numbers a and b that Alice and Bob compute, and what is the resulting shared secret key?

Problem 18: ElGamal Cryptosystem

A public key cryptosystem can be built from the ElGamal variant of Diffie-Hellman Key Exchange (section 59, lecture notes 11) together with a symmetric cryptosystem such as AES. Using the same parameters as in problem 17 above, what are Bob's public and private keys?

Problem 19: Square Roots with Composite Moduli

(a) How big is $\mathbf{Z}_{105}^*$?

(b) Find all square roots of 1 modulo 105.

(c) How many quadratic residues are there modulo 105? Find them.

Problem 20: Computing Square Roots Modulo a Prime

(a) Show that 2 is a quadratic residue modulo 103.

(b) Find a square root of 2 modulo 103 using the method of section 64 (lecture notes 12).

Problem 21: Quadratic Residues

Let p be an odd prime. Let $a, b \in \mathrm{QNR}_p$ be quadratic non-residues modulo p. Show that ab is a quadratic residue modulo p.