T-79.5501 Cryptology
Homework 11
April 17, 2007

1. In Step 4 of Rabin's Oblivious Transfer protocol (see Lecture 10 Notes) Alice may try to cheat by sending a random number z. What will then happen in Step 5? What Bob should do to detect if Alice is trying to cheat.

2. Suppose that (y_1, y_2) is an encryption of message m and $(\hat{y}_1, \hat{y}_2)$ is an encryption of message $\hat{m}$ using ElGamal public key encryption system with the same public key. Show how, given these two encryptions, one can compute encryptions of messages $m\hat{m} \bmod p$ and $m/\hat{m} \bmod p$ even without knowledge of the public key.

3. Using Shanks' algorithm attempt to determine x such that

   $$4815^x \equiv 48794 \pmod{50101}.$$

   Hint: See Problem 4 in Homework 10.

4. Element $\alpha = 202$ is of order 16 in the multiplicative group $\mathbb{Z}^*_{2005}$. It is given that element $\beta = 133$ is in the subgroup generated by α. Using Shanks' algorithm compute the discrete logarithm x of $\beta = 133$ to the base $\alpha = 202$, that is, solve the congruence

   $$202^x \equiv 133 \pmod{2005}.$$

5. Solve the congruence

   $$3^x \equiv 24 \pmod{31}$$

   using

   a) Shanks' algorithm; and
   b) the Pohlig-Hellman algorithm.

6. Solve the congruence

   $$3^x \equiv 135 \pmod{353}$$

   using the Pohlig-Hellman algorithm.