Homework 6

Problem 1

In this problem you will carry out a "network attack" against Rabin's cryptosystem. Alice and Bob are members of a network in which all messages are encrypted using Rabin's cryptosystem. The central computer broadcasts a secret message x to each member, separately encrypting the message with the recipient's public key. For example, the central computer sends the ciphertext $C_A = x^2 \bmod n_A$ to Alice, and the ciphertext $C_B = x^2 \bmod n_B$ to Bob.

You observe the resulting ciphertexts $C_A = 7310$ and $C_B = 10087$ going from the central computer to Alice and Bob, respectively. From the public directory, you know that Alice's public key is $n_A = 9991$; Bob's public key is $n_B = 10807$.

a) By hand using the general-purpose method explained in class, find the plaintext x without factoring n_A or n_B. Show all calculations and carefully explain and justify your work. Check your work.

   The purpose of this problem is for you to learn a general-purpose method for carrying out a network attack against Rabin's cryptosystem. Therefore, use the general-purpose method explained in class; *do not use ad-hocs methods* and *do not use any method that depends on factoring any of the moduli.* Although ad-hoc methods and methods based on factoring work for situations with small numbers (including the situation in this problem), such methods will not work well for all large problems.

   optional: In addition to solving this problem by hand, implement a general method for carrying out the network attack.

b) How much time does it take to carry out this network attack against Rabin's cryptosystem? State your answer in terms of all relevant parameters using big-Oh notation. Justify your answer.

Problem 2

Read the draft Chapter on RSA from Stinson's new book *Cryptography: Theory and Practice.* Write a two-page pre-publication book review of this chapter, critically assessing its suitability for use in CMSC-443, and comparing it with Denning's explanation of RSA.