Problem Set 6

Due before midnight on Wednesday, December 3, 2008.

In the problems below, "textbook" refers to Douglas R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, 2006.

Problem 1: ElGamal Ciphertext Decryption

Textbook, problem 6.9. An electronic copy of Table 6.3 has been placed on the Zoo in file /c/cs467/assignments/ps6/stinson_table_6.3.txt so that you don't have to type in all of this input data. Although you will have to implement ElGamal decryption in order to solve this problem, the numbers are all small enough so that you can get by with 32-bit arithmetic rather than using one of the big number packages.

Problem 2: ElGamal Signatures

Textbook, problem 7.3(a).

Problem 3: Simplified Feige-Fiat Authentication Protocol

Bob is using 20 rounds of the simplified Feige-Fiat authentication protocol presented in section 95 in Lecture Notes 20, thinking that the chance of an impostor successfully impersonating the legitimate Alice is only 2^{-20}. Unbeknownst to him, there is a bug in the random number generator that he is using to generate b, so $\mathrm{prob}[b = 1] = 0.9$ and $\mathrm{prob}[b = 0] = 0.1$.

(a) What is the probability that an impostor can successfully fool Bob? Argue why your answer is correct.

(b) Describe how the attack works that achieves the probability of part (a) above.