CSci 4554 Assignment 8

Due Monday, April 26th in class

Problem 1 (8 points). Consider a Diffie-Hellman key exchange protocol with two different prime values of p, both on the order of 200 bits:

- with the largest prime factor of $p-1$ on the order of 2^{160}
- with the largest prime factor of $p-1$ on the order of 2^{40}

Compare the number of tries needed to solve the discrete logarithm problem in these two cases. Explain what these tries consist of and how the solution will be constructed.

Problem 2 (6 points). Suppose an RSA public key N is a 1024-bit integer. Mallory knows that the message m is less than $1,000,000$. Describe how Mallory can use the Meet-in-the-Middle attack to find m given its ciphertext c. How much memory would the attack require? Is this a realistic requirement?

Problem 3 (12 points). For each of the following pairs (p, a) please say whether $a \in QR_p$ and if it is then find its square root. Note that p is not necessarily prime. Show all your computations (including those to figure out if a is in QR_p).

- $p = 19, a = 11$.
- $p = 19, a = 12$.
- $p = 83, a = 77$.
- $p = 89, a = 35$.
- $p = 57, a = 43$.
- $p = 57, a = 50$.

Problem 4 (7 points). Find all square roots of 43 modulo 57. Show a pair of the square roots that add up to 0 modulo 57 and a pair that allows you to factor 57.

Problem 5 (5 points). Exercise 6.9 p. 201. You may assume that the composite is a product of just two primes.