HOMEWORK 5

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (2.6) Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for the Diffie-Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks your assistance, so you tell him to use the secret exponent $b = 871$. What value B should Bob send to Alice, and what is their secret shared value? Can you figure out Alice's secret exponent?

(2) (2.7) Let p be a prime and let g be an integer. The *Decision Diffie-Hellman Problem* is as follows. Suppose that you are given three numbers A, B, and C, and suppose that A and B are equalt to

$$A = g^a \mod p,\ B = g^b \mod p$$

but that you do not necessarily know the exponents a and b. Determine whether C is equal to $g^{ab} \mod p$. Notice that this is different from the Diffie-Hellman problem itself.

(a) Prove that an algorithm that solves the Diffie- Hellman problem can be used to solve the decision Diffie-Hellman problem.

(b) Do you think that the decision Diffie-Hellman problem is hard or easy? Why?

(3) (2.8) Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the Elgamal public key cryptosystem.

(a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

(b) Bob choose $b = 716$ as his private key, so his public key is

$$B = 2^{716} = 469 \mod 1373$$

Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with associated public key $A = 2^{299} = 34 \mod 1373$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt this message.

(d) Now Bob choose a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using the this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by the solving the discrete logarithm problem $2^b = 893 \mod 1373$ and using the value of b to decrypt the message.

(4) (2.9) Suppose Eve is able to solve the Diffie-Hellman problem. More precisely, assume that Eve is given two powers g^u and $g^v \mod p$, then she is able to compute $g^{uv} \mod p$. Show that Eve can break the Elgamal PKC.

(5) (2.10) This exercise describes a public key cryptosystem that requires Bob and Alice to exchange several messages. We illustrate the system with an example.

Bob and Alice fix a publicly known prime $p = 32611$, and all of the other numbers are private. Alice takes her message $m = 11111$, choose a random exponent $a = 3589$, and sends the number $u = m^a \mod p = 15950$ to Bob. Bob chooses a random

exponent $b = 4037$ and sends $v = u^b \mod p = 15422$ back to Alice. Alice then computes $w = v^{15619} = 27257 \mod 32611$ and sends $w = 27257$ to Bob. Finally, Bob computes $w^{31883} mod 32611$ and recovers the value 11111 of Alice's message.

(a) Explain why this algorithm works. In particular, Alice uses the numbers $a = 3589$ and 15619 as exponents. How are they related? Similarly, how are Bob's exponents $b = 4037$ and 31883 relates?

(b) Formulate a general version of this cryptosystem, i.e. using variables, and show that it works in general.

(c) What is the disadvantage of this cryptosystem over Elgamal? (Hint: How many times must Alice and Bob exchange data?)

(d) Are there any advantages of this cryptosystem over Elgamal? In particular, can Eve break it if she can solve the discrete logarithm problem? Can Eve break it if she can solve the Diffie-Hellman problem?