Math 565, Problem Set 3: *due Wednesday, January 24*

1. Let N be a large integer and let $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}/N\mathbb{Z}$. For each of the functions
$$e\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$
listed in (a), (b), and (c), answer the following questions:

   - Is e an encryption function?
   - If e is an encryption function, what is its associated decryption function d?
   - If e is not an encryption function, can you make it into an encryption function by using some smaller, yet reasonably large, set of keys?

   (a) $e_k(m) \equiv k - m \pmod{N}$

   (b) $e_k(m) \equiv km \pmod{N}$

   (c) $e_k(m) \equiv (k+m)^2 \pmod{N}$.

2. Let p be an odd prime and let g be a primitive root modulo p. Prove that a has a square root modulo p if and only if its discrete logarithm $\log_g(a)$ modulo p is even.

3. Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a 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?

4. Again, 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 chooses $b = 716$ as his private key, so his public key is
   $$B \equiv 2^{716} \equiv 469 \pmod{1373}.$$
   Alice encrypts the message $m = 583$ using the ephemeral key $k = 877$. What is the cipertext (c_1, c_2) that Alice sends to Bob?

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

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

5. Suppose that an oracle offers to solve the Diffie-Hellman problem for you. Explain how you can use the oracle to decrypt messages that have been encrypted using the ElGamal public key cryptosystem.

6. Bob and Alice fix a publicly known prime $p = 32611$; all of the exponents mentioned below are private. Alice takes her secret message $m = 11111$, chooses a random exponent $a = 3589$, and sends the number $u = m^a \pmod{p} = 15950$ to Bob. Bob chooses a random exponent $b = 4037$ and sends $v = u^b \pmod{p} = 15422$ back to Alice. Alice then computes $w = v^{15619} = 27257 \pmod{p}$ and sends w to Bob. Finally, Bob computes $w^{31883} = 11111 \pmod{p}$, and thus recovers Alice's secret message m.

   (a) Explain why this procedure works. In particular, Alice uses the numbers $a = 3589$ and 15619 as exponents. How are they related? What about Bob's exponents?

   (b) Formulate a general version of this cryptosystem, 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?