Math 63: Homework 7

Due: Tuesday, December 6

1. Alice and Bob wish to communicate secretly using the Diffie–Hellman version of the Elgamal encryption system.

a) Alice begins by choosing a "large" prime $p = 14348909$ $(= 27^5 + 2)$ and a random primitive root $g = 7691485$. She also chooses a random private key $a = 919332$. Find Alice's public key (that is, the information she makes public and sends to Bob).

b) Bob now chooses a random private key $b = 197992$. What information does Bob send to Alice to establish their shared secret key? What is that secret key?

Now, suppose Alice and Bob have agreed to send up to five letter messages as follows. First, turn each letter into a number as expected: $A = 1$, $B = 2$, …, $Z = 26$. For a two letter message, multiply the value of the first letter by 27 and add it to the value of the second letter (e.g., HI $\to 8 \cdot 27 + 9 = 225$); for a three letter message, multiply the value of the first letter by 27^2, the second by 27, and then add up all three letters (e.g, ABC $\to 1 \cdot 27^2 + 2 \cdot 27 + 3 = 786$); and for a longer message, keep repeating this process.

c) Suppose that Bob wants to send the message "NMTHY" to Alice.

(i) What is his plaintext message m in the above system? (*Hint:* If you are confused about this system, please ask, or use the message $m = 164423$ in the next part instead).

(ii) What is the encoded cipher text he sends to Alice?

d) Alice responds to Bob with her own encrypted message with cipher text $c = 8730216$. What is her unencoded message? (Ideally in letters, but as a number if you are confused about the above system.)

2. Suppose now that Alice and Bob are tired of Diffie–Hellman and decide to switch to the RSA encryption method.

a) Alice begins by choosing "large" primes $p = 20359$ and $q = 10939$. She chooses a random encrypting exponent $e = 119102437$. What is her public key?

b) Suppose Bob wishes to send the message $m = 12345$. What would be his encrypted cipher text?

c) Bob changes his mind, and instead sends the encrypted message $c = 163527889$ to Alice. What was his original message? (*Hint:* This message is a word encoded using the above scheme, if you want to check your work. It may also be possible to "hack the user" and to guess the word I used here. If you go this route, let me know everything you tried!)

3. Suppose now that you're Eve. Alice and Bob are communicating privately, *yet again*, using RSA. Alice's public key is $(453619540697, 184283032817)$, and Bob just sent the encoded message 294695456230. What is Bob's message? (*Hint:* Even something like Wolfram Alpha can do some pretty impressive things.)

4. Implement by hand, though with the aid of a computer or calculator, the "baby steps/giant steps" algorithm to find the discrete logarithm $\log_2 3$ with $p = 101$.