Homework 6

CSC 152 – Cryptography

If anything in this assignment does not make sense, please ask for help.

Quiz: We will have a closed-note 20-30 minute quiz on this homework in class Monday May 6.

Due: You should consider the due date to be when you take the quiz because the quiz may cover anything related to this homework, including programming topics. However, anything submitted before grading occurs will be considered on-time.

Non-submitted work:

Read: Review notes on groups on Piazza.

Written Problems:

There are three steps to follow for the written problems. Step 1: Do them as if they were homework assigned to be graded (ie, take them seriously and try to do a good job). Step 2: Self-assess your work by comparing your solutions to the solutions provided by me. Step 3: Revise your original attempts as little as possible to make them correct. Submit both your original attempt and your revision as separate files.

Submit two files to DBInbox following the procedure documented on Piazza. The first file should be named exactly **hw6.pdf** and should be your homework solutions before looking at my solutions. The second file should be named exactly **hw6revised.pdf** and should be your homework solutions after looking at my solutions and revising your answers.

NOTE: If you wish to handwrite your solutions you may, but only if your handwriting is easy to read and the file you submit is less than 1MB in size.

1) Every element of a group generates a subgroup, and the size of the group is always a multiple of the size of the subgroup. For $\mathbb{Z}_7^*$ and $\mathbb{Z}_8^*$ determine the subgroups generated by each of its elements.

2) Let's say Diffie-Hellman key-exchange is being done with generator $g = 4$ and prime $p = 467$. Note that g generates a subgroup of size 233. What is the key produced when the exponents chosen by the two parties are 400 and 134? What is the key produced when the exponents chosen by the two parties are 167 and 134? Why are the keys identical?

3) Let's say that you capture two ciphertexts encrypted using Elgamal in group $\mathbb{Z}_{31}^*$ using $g = 3$: $(A = 6, y = 17)$ and $(A = 6, y = 25)$. Furthermore, you know that the first ciphertext is of plaintext $x = 21$. What is the second plaintext? *Hint: The two A values can only be the same if the two exponents are the same.*

4) A small elliptic curve group has elements from $\{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + ax + b \bmod p\} \cup \{0\}$ where $a = 1$, $b = 6$ and $p = 11$. Let's say you choose 6 as your multiplier in a Diffie-Hellman key exchange and you receive $(5, 9)$ as your communication partner's contribution. What is the shared key generated?

5) Follow the method seen in class to generate a multiplicative group with a number of elements requiring 10 bits to represent (ie, 1000000000 to 1111111111) and identify a generator of the group. Note: At `http://wolframalpha.com` you can type "11 prime?" to check if 11 is prime and you can check a generator with "order of 11 mod 29".

6) Elliptic curve groups are made from elements of $\{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + ax + b \bmod p\} \cup \{0\}$ where p is prime, a and b are in $\mathbb{Z}_p^*$, and $\{0\}$ is the identity. All of these points do not necessarily make a cyclic group, but it is known that a subset of these points will make a cyclic group. Find an a, b, prime p, and generator (x, y) that generates a group with a prime number of elements (including 0). One way of doing this is by trial and error using your program (below) as a calculator.

7) In Elgamal encryption a public key consists of the specification of a group, a generator, and a Diffie-Helman contribution. Let's say that my public key specifies group $\mathbb{Z}_{11}^*$, generator 2, and DH contribution 5. Tell me what grade you think you should get in this class A, B or C, and then encrypt it using my public key using A=2, B=3, C=4. If you need a random number during encryption, use 4.

Programming:

Read: C program requirements at `http://krovetz.net/152/programs.html`.

A) Submit the following program using DBInbox and name the file `hw6.c`. You are to write a program that reads seven integers $a, b, p, x_1, y_1, x_2, y_2$ from standard input (each value separated by a single space), and prints the result of adding elliptic curve points (x_1, y_1) and (x_2, y_2). If either of the points is not valid, you should output "Error" instead. If the sum is the identity, you should output "0".

For example:

```
>  echo "2 2 17 5 1 5 1" | a.out
(6,3)
>  echo "2 2 17 5 1 5 16" | a.out
0
>  echo "2 2 17 0 0 5 1" | a.out
Error
```

Your program does not need to be robust in the sense that your program may assume the input will be correctly formatted, p will be a prime, and all the inputs will be in $\mathbb{Z}_p$. You do not need to handle the identity "0" as an input. You may also assume $p < 10000$, which means that inverses can be computed using brute force rather than egcd.