Assignment 4

Elliptic Curve Cryptography

Github Link for the project(contributions done by team members):
Encrypting Equations Github Repo

Problem 1 Prove that an elliptic curve $E(\mathbb{R})$ is a group under $\bigoplus$ (focus on closure). Can you do the same for $E(\mathbb{F}_p)$?

Problem 2 (**Coding Question**) Write down the programs for addition of two points on an elliptic curve $y^2 = x^3 + 3x + 120$ over $\mathbb{Q}$ (The inputs can conveniently be integers, it is just that their sum might be in rationals). Take the inputs to be two values of x. To do that, first you need to do fast testing of whether y exists for the given value of x (**Hint**: The set of integers is a sorted array, does that give an advantage in the searching?). If the value of x works (has an corresponding integer value of y), take the second input x; if not, just find a bigger value of x for which it works (do an iterative search starting from x+1. try to take small integer values of x, not more than 5 digits, as the input, with a good amount of gap between the input points, to prevent messing up). Second, generalise this addition to the quotient ring $\mathbb{Z}/p\mathbb{Z}$ for $p = 2^{31} - 1$ (which is a field because $2^{31} - 1$ is a prime), using the fact that if $y^2 = x^3 + ax + b$ over reals, then it also holds modulo p. Can you also try finding the other point for the same value of x (**Hint**: a and $p - a$ have the same square modulo p).

Solution 2 Please make sure to go through the Readme.md file of the github repo before hand.

- Ecc rational addition.c
- Ecc finite.c

Problem 3 (**Coding Question**) Implement the Diffie-Hellman Key exchange and ElGamal public key cryptosystem taking p as $2^{19} - 1$ for $E(\mathbb{F}_p)$. Choose all other parameters as per your convenience, even use an elliptic curve of your choice.

Solution 3

- ECDH.c
- elgamal.c

Problem 4 Read up the Lenstra Elliptic Curve Factorisation Algorithm. Does it present a considerable threat to RSA cryptosystem¿

Solution 4 The lenstra factorisation algorithm has a sub-exponential time complexity. So for small values, the algorithm will be a considerable threat to RSA cryptosystem, and only when we use large values(upwards of 1024 bits), we can consider that lenstra doesn't present any threat to RSA.

OPTIONAL QUESTIONS (Will be much more difficult than the compulsory ones)

Problem 5 Try to implement Lenstra Elliptic curve factorisation algorithm to factor $2^{21}-1$

Problem 6 Read up about Rational functions and divisors, and bilinear pairings. Also read about the Weil Pairing and Tate pairing and efficient ways to compute them (Miller's Algorithm, for one). Is it possible to implement a Tripartite Diffie Hellman Key Exchange?

Problem 7 Find out more about the Pollard's ρ method for DLP.