Cryptography

Lab 6

1 (5 points) Implement Edwards elliptic curve. You may take a look at scripts from [1] but then you need to implement your curves in language that is other than Python. Learn more about dangers of "wrong" elliptic curves [2].

2 (10 points) Implement ElGamal encryption over the curve you implemented.

References

[1] Tanja Lange Daniel J. Bernstein. ECCHacks. `http://ecchacks.cr.yp.to/`.

[2] Tanja Lange Daniel J. Bernstein. Safe curves. `http://safecurves.cr.yp.to/`.