Project Plan: Elliptic Curve Cryptography

Thomas Butterfield

27-10-20

Description

Much work has been done in the study and implementation of Elliptic Curve Cryptography (ECC). This project aims to implement and test an Elliptic Curve Cryptosystem, as well as compare the efficiency and security of ECC with RSA cryptography. I will also explore attacks on ECC both in theory and in practice.

Preliminary preperation

- A strong understanding of the mathematics behind Elliptic Curve Cryptography, such as point addition and multiplication.
- A familiarity with the common techniques for implementing ECC.
- An understanding of common attacks on real-world ECC.

Objectives

Basic

- Create a working Elliptic Curve Cryptography (ECC) system for computing the essential functions.
- Create client applications that can conduct Elliptic Curve Diffie-Hellman (ECDH) over a network connection.
- Create a User Interface (UI) so that a user can make use of this 'easily' while still seeing what is going on. Allow the user to decide what level of complexity is revealed to them.

Intermediate

- Generate secure random private keys using user delay/input etc.
- Implement the Elliptic Curve Digital Signature Algorithm (ECDSA).
- Add functionality to the User Interface to enable the exchange of secure signed files.

Advanced

- Make the User Interface fancy and show the workings of ECC in a nice and revealing way.
- Analyse the code for efficiency, how does the time required scale with curve/key size. How does this compare with an RSA implementation?
- Analyse the code for vulnerabilities, such as timing attacks on the private key.

Project Plan

The project plan can be broken down fairly simply along the lines of the main objectives, each of which arguably depends on the others. Within each of the objectives however, there is some flexibility for rearrangement/reordering of sub-objectives.
I have chosen to prioritise the mathematical implementation of ECC over the design of the User Interface in this project. I believe that it is more worthwhile to work on the behind-the-scenes aspects of ECC rather than on the front-end design.
The difficulty of these objectives clearly increases as the project progresses, as it should, however there are also some large differences in difficulty between sub-objectives within the same objective, for example, the final advanced objective, analysing the code for vulnerabilities, could easily take the form of an entire project in and of itself. Therefore, for the purposes of this project I must limit the extent to which I explore the security aspects of Elliptic Curve Cryptography and the vulnerabilites of my code, and so I will only look into the vulnerabilites of ECC with respect to a small number of ideas, such as timing attacks.

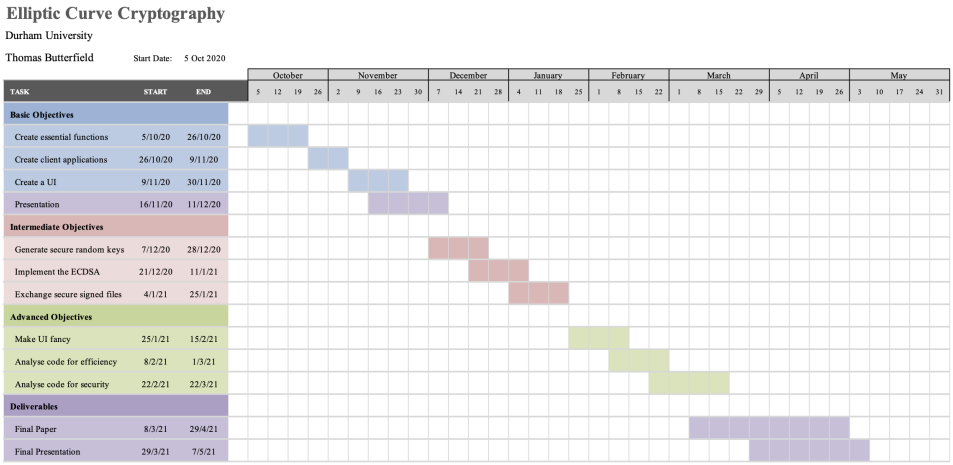

Figure 1: Project Gantt Chart