**MSc Project Description**

**Project Title:** Discrete Logarithm problem in Finite fields and applications to Cryptography

**Student:** Divyesh Bhagwanji Chudasama (A817622)

**Programme:** MSc Internet Computing and Network Security

**Aim & Objective of Project:** The aim of this project is to collect current algorithms for solving the finite field problem and then select one or a few of these algorithms to implement in the programming language C. The Discrete Logarithm Algorithms are:

1. **Trial Exponentiation** – *There exists a deterministic algorithm which solves the Discrete Logarithm Problem (DLP) in a finite field in time O(*
2. **Shanks’ “Baby-Step Giant-Step” Method** – *There exists a deterministic algorithm which solves the DLP in in time O( using space O(.*
3. **Pollard’s ρ-method** (1978) – *There exists a probabilistic algorithm which solves the DLP in with time complexity O( and space complexity O(*log*(q)).*
4. **Pollard’s λ-method “Kangaroo Method”** (1978)- *There exists a deterministic algorithm, which, given as input a finite field , a primitive element α of , where β is an element of and two integers a, b are elements of , computes ≤ b, in time O( and space O.*
5. **The Pohlig-Hellman Method** (1978) – *There exists a deterministic algorithm which solves the DLP in in time O(, where p is the greatest prime divisor of q-1.*

Sources and materials will include: The Internet, An IDE for C language – XCode (Mac) or Notepad++ (Windows), Thesis (Public Key Cryptography Using Discrete Logarithms in Finite Fields) – L.Maurits

**Long Term Aim:** The long-term aim with this project is to look at computing the discrete logarithms for some very specific inputs, namely, if the primitive element

is defined by the equation:

then compute the discrete logarithms of the elements:

, for i = 1,2,…,n-1

Further, if possible, a further long-term aim is to see if any of the above of the above algorithms listed above would be suitable for the specific input.

**Equipment:** A Computer

**Training needed to achieve aims/objectives:** No physical training is needed for this project, however mental preparation is required through:

* Understanding very well what finite fields are
* Understanding what discrete logarithms are in finite fields
* Understanding the discrete logarithm algorithms
* Having a strong mathematical background
* Having good C/C++ programming skills

***Prerequisites:*** *Good C/C++ programming abilities & a high level of mathematical understanding*

**Risk Assessment:** The key underlying risk for this project is failing to implement the chosen algorithm(s) in an efficient manner, which could lead to the failure of the project. Hence, a well thought out structure and organised model is required for the timeline of the project for a successful finish. This is outlined below in the table, however, alongside this, it is essential to gain a very good understanding not only of the mathematical content and processes but also of the project requirements. This is a key element to grasp upon, and some questions to guide me include: What are the project requirements? How can this be accomplished? What is the anticipated outcome?

* **What are the project requirements?** – Background reading about the Discrete Logarithm Problem is required. Not only what the problem is and potential acceptable solutions, but it is also to be considered what past work has been carried out on this problem and what current work is being done. This could have a diverse effect on the lifetime of the project, because previous work could be a tool from which I could continue this project and also understand how to go about dealing with what is required from me. Nevertheless, the project asks for implementation of either one or more of the Discrete Logarithm Algorithms. Consider which approach to take and how to best implement to the level of standard required.
* **How can this be accomplished?** - As stated above through thorough research, reflection upon past works and current works. In addition analysing the results to then take forward and implement in C.
* **What is the anticipated outcome?** – The anticipated outcome is the successful implementation of one or more of the Discrete Logarithm Algorithms, in the most efficient manner possible. A dissertation reflecting my findings, problems faced, literature review and the general project experience will be produced for submission, alongside a disc consisting of my source files and an electronic copy of my report.

**Work Plan**

Below is a plan for the schedule of my project:

|  |  |
| --- | --- |
| **Date** | **Task** |
| 14th May 2012 – 3rd June 2012 | * Read up about finite fields and understand what they are * Study and analyse the discrete logarithm algorithms * Decide which algorithm(s) to choose for the project and implement |
| 4th June 2012 - 4th July 2012 | * Plan and implement algorithms in C |
| 5nd July 2012 – 14th July 2012 | * Test code/Make corrections if errors |
| 16th July 2012 – 13th September 2012 | * Write up Dissertation |
| 14th September 2012 | * Submit Dissertation |
| 17th/18th September 2012 | * Project Demonstration |

Throughout the schedule of the project I shall aim to arrange meetings with my supervisor on a weekly basis to discuss progress or issues.