Minutes of Review Meeting 1

Project Lima

29th January 2003 3:00 - 4:00 pm

Attendance: Dr Ross Anderson, all group memebers present

Presentation:

- Presented required deliverables to Dr Anderson.
- Run through of algorithms, implementation and distribution method proposed.
- Discussed project and group organisation and role delegation.

Feedback and suggestions:

0.1 Program Implementation

- Dr Anderson suggested that we could consider the use of the Eliptic Curve Method as an optimisation later on. This is a random implementation of Pollard Rho and an extension of the $P(P-1)$ method. This method can allow for easy distribution. However, we did not intend to distribute the Pollard Rho method, and from our research, the Quadratic Sieve method (Self-initialising Hyper Cube) is the most efficient for dealing with "large" numbers as defined in our specified range.
- We should treat all distributed jobs as individual separate tasks. The notion of factoring several numbers simultaneously should only be considered in an organisational sense rather than in implementation.
- It is possible to encounter raw or buggy clients who may return wrong answers. However this problem can be largely ignored. We will assume that the clients are trustworthy to avoid "feature creep" in our implementation.
- Relying on the Java BigInteger package may dramatically slow down performance.

0.2 Project Management

- Plan out time scale. Good management strategies are essential in determining the success of a project.
- Draw out Pert Chart and Gant Chart.
- Set concrete milestones. Ensure good communication within the group and sub-groups so that problems can be discovered and resolved early.

0.3 Final Project Presentation

- Presentation is to last for no more than 4 minutes 50 seconds. 5 OHP slides are allowed.
- Know our audience – Half of the department members have strong mathematical backgrounds, others may be experts in distributed system engineering.
- On the presentation day, a random selection of the faculty members may turn up. Each faculty memeber has 3 votes.
- Making the presentation stimulating, enjoyable and memorable are as important as the content of the presentation itself.
- We need to start gathering material and search for ideas for the presentation from now on. Perhaps we could apply an element of our project to talk about a topical issue, which will add relevance and interest to the otherwise 'dry' subject of factorisation of prime numbers. (eg how could Saddam's PCs be used to crack NSA keys; Security issues concerning the X-Box)