INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

Random Number Generation: Implementation and Analysis

James Bradley Villinger, School of Computer Science and Mathematics, Victoria University

The summer vacation scholarship went for a duration of six weeks. Initiated in January and concluding in February, the experience was quite fulfilling. Under the supervision of Senior Lecturer Alasdair McAndrew, I was able to ascertain the discrepancies of modern Pseudo Random Number Generation and understand the finer details of Random Number Generation on the whole. For the purpose of implementing the algorithms I used a free program known as Maxima which allowed easy to execute syntax and quick results.

The first week was focussed on reading what was available out there on the internet. The particular area of research can be complicated but luckily the authors of the research had good literacy skills. It was immediately apparent that Pseudo Random Number Generators (PRNG's) are very flawed and unfortunately implemented poorly. PRNG's are broken up into cryptographically secure and non-cryptographically secure, and depending on the context of the security needed, determined what type of PRNG you choose. I also delved into other areas such as the theory behind True Random Number Generation (TRNG) and briefly covered new technologies that will enable much more powerful and efficient generation in the near future.

I found that PRNG's follow standard equations which can be slightly modified by the user. An example of such an equation used by the Linear Congruential Generator (the simplest of generators) which uses the recurrence equation:

$$x_{n+1} \equiv ax_n + b \pmod{m}$$

The research continued until approximately the fourth week when it was ready to be made into an oral presentation for the 'Big Day In' in Sydney. The first segment of the speech was theory based. This was followed by a brief demonstration of how to implement a specific generator. One of the weaker ones was chosen such that the audience could see why it was weak from the follow up analysis.

I would like to thank ICE-EM and AMSI as well as anyone involved for making this opportunity available to me. In the future this experience will help me not just career-wise, but also it has taught me the quintessence of learning. I would like to thank CSIRO. I would also like to thank Yvonne Preston and Jordan Bailing for the efforts to help organize the event. Definitely a worth while experience.

James received an ICE-EM Vacation Scholarship in December 2006.
See http://www.ice-em.org.au/students.html#scholarships2007