Comparison of two pseudorandom number generators

Objective:

To gain an understanding of pseudorandom number generators and their statistical properties.

Due Date:
20 April 2010 (issued on 23 March 2010).

Marks:

This assignment represents 12.5% of the total marks for this module.

Description of Assignment:

This assignment will require you to test two simple pseudorandom number generators and compare them in terms of the statistical properties of their outputs (i.e. their ability to produce numbers that appear random). The algorithms themselves can be found on the website and are written in C although you may rewrite them in any language you wish for testing purposes.

The tests you choose to determine the statistical properties of each generator should be well known (you will need to read up on the types of tests normally carried out)[1]. You may use any programming language you wish to implement the tests and you may borrow code where possible as long as it is referenced clearly and explained clearly[2].

The assignment report should contain the following:

- A description of the operation of each random number generator.
- Explanations of the tests you have chosen to implement and why.
- Graphs and tables which draw clear comparisons between the outputs of the two algorithms.
- A discussion on which one might be considered a better algorithm in terms of its randomness properties.
- A brief discussion as to whether or not either of these pseudorandom number generators are suitable for cryptographic purposes.
- Bibliography of information (where you got any code used, information etc. with the relevant sections referenced to the bibliography).

---

[1] I will not be specifying any test for you to choose this is entirely up to you (there are many resources available with the relevant information - don't limit yourselves to the Internet).

[2] Reams of code which make no sense to me will generally get no marks.

Reports will only be accepted by e-mail and should be sent to the following **three** email addresses before 5 pm on the due date.

xiaojun.wang@dcu.ie; amitabha@eeng.dcu.ie; insky.bj@gmail.com

Each email lab report submission should contain the following:

- The subject heading formatted exactly as follows:
  Student ID Number - Full Name - EE548 Assignment2

- It should contain
  1. Your report, including the scanned, signed cover sheet (the latter you may also fax to me if you wish - Fax: +353-1-7005508).
  2. Your code and details on how to compile it.

Copying of any form will not be accepted. This includes copying and pasting information from the Internet. All code must be your own. Any reports with copied text will get zero.