Assignment 2: Entropy Gathering

1 Implementation

Implement an program `egd` that gathers entropy from the Linux operating system. The program is to print a true random sequence of "0" and "1" characters to `stdout` as fast as it can. The program should terminate once the user presses `CTRL-c`.

Make sure that your generator has an equal chance of producing zeros and onces and passes the PRNG tests from the previous assignment. You will be graded on the quality of the generated random number sequence and on how fast your generator can produce random numbers.

2 Hints

The `/proc` filesystem gives you access to various statistics about hardware events. Properly mixing multiple sources of entropy can be used to improve both quality and quantity of the generated random numbers. Writing zeros and ones to `stdout` individually is more expensive then writing blocks of data.

3 Submission

You must submit the implementations to your subversion repository to the directory `courses/comp3704/s2007/$USER/p2/`. Do not include generated files.

- `egd.c`
- `Makefile`

You must check that the submitted code compiles by invoking `make`. Verify that the output of your program matches the expected output using your own testcases.