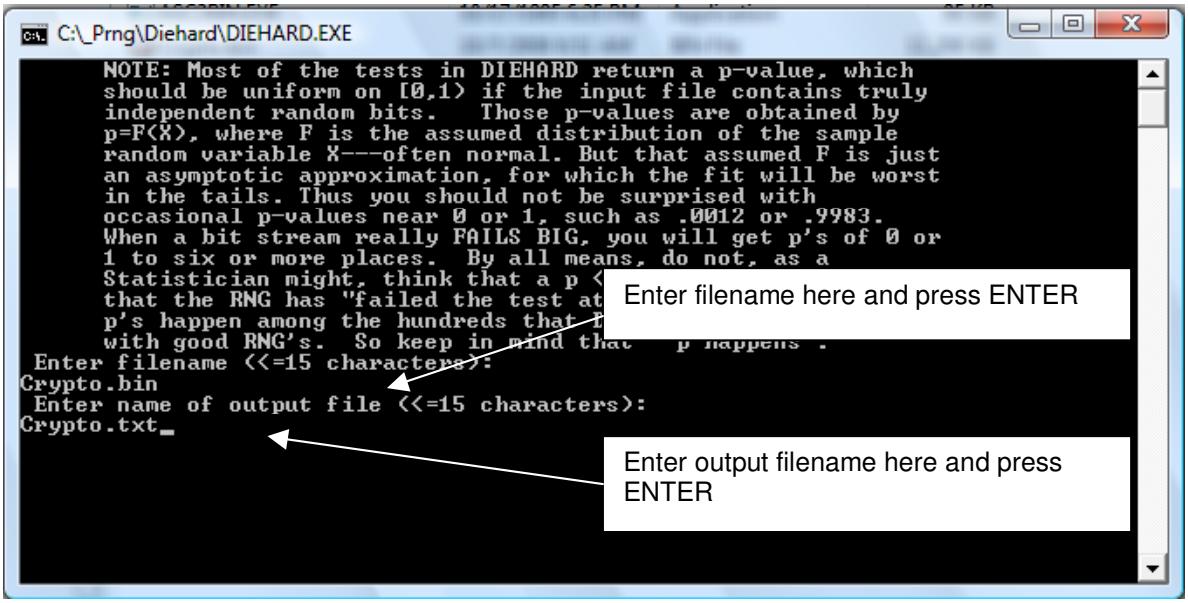
Using Diehard test program by George Marsaglia

Download the Diehard PRNG (Pseudo Random Number Generator) testing software from here: http://stat.fsu.edu/pub/diehard/

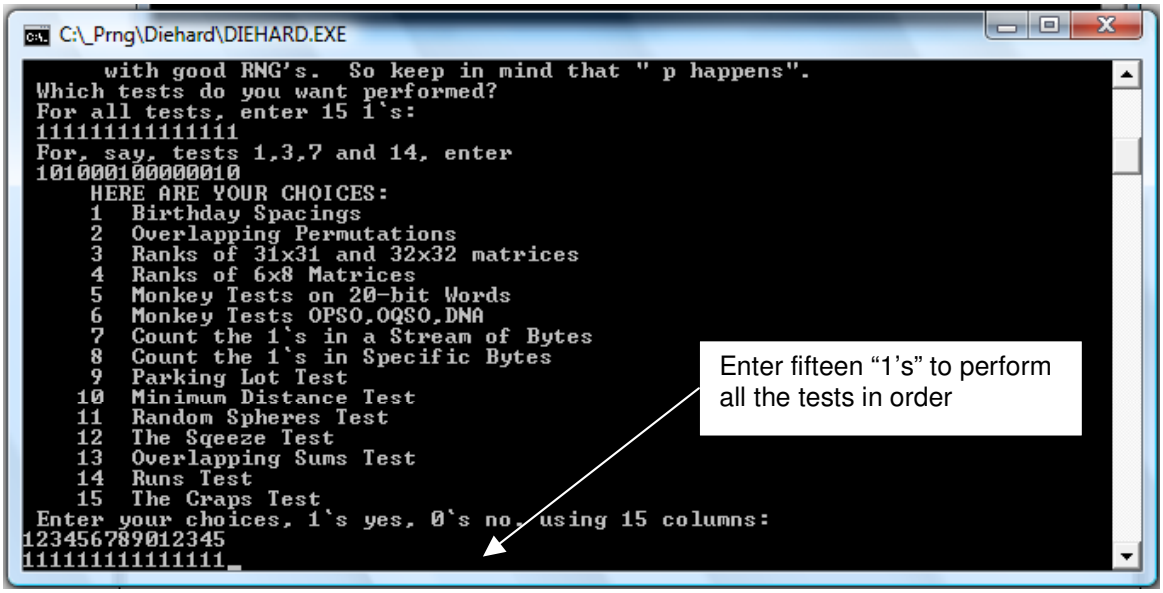
Scroll down and click on the link "Windows software (732kb)"
Create a folder named Diehard and unzip the software to there.

Use the sample application and create a couple of binary test files. It will take a few seconds to create both files approximately 11mb (11,468,800 bytes) in size. The first will be using MS CryptoAPI random number generator (Output: C:\Temp\Crypto.bin). The second will be MS VB Rnd (Output: C:\Temp\VB_Rnd.bin)

1. Copy the newly created ".BIN" files to the Diehard folder
2. In Windows Explorer, navigate to Diehard folder
3. Double click name Diehard.exe to start the application
4. The window below will open.



A lot of data will appear and then another prompt. This will designate which test to run. Enter a "1" for all fifteen tests as shown below. Expand the DOS window to be able to read all the information.



The results of the tests will be written to the associated test file. In this case, Crypto.txt or VB_Rnd.txt.

After the tests have finished running, you will be able to open the test results with notepad or similar editor. A failed test will show in the P-Value as one of the following:

1.0000	Exceeded outer bounds
.9999	Too close to outer bounds
.0000	Too close to inner bounds
*******	Asterisks on the same line as the P-Value (Terrible)

According to theory, Crypto.txt will show good results for all fifteen tests. Visual Basic's results are less than encouraging. VB RND did pass some of the tests but failed miserably on the others.

Here are some examples from the VB_Rnd.txt file.

```
BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
          Results for VB_Rnd.bin
                  For a sample of size 500:     mean
          VB_Rnd.bin      using bits  1 to 24   2.606
 duplicate       number       number
 spacings       observed     expected
       0          28.       67.668
       1         105.      135.335
       2         120.      135.335
       3         110.       90.224
       4          82.       45.112
       5          37.       18.045
 6 to INF         18.        8.282
Chisquare with  6 d.o.f. =    97.61 p-value= 1.000000
 ::::::::::::::::::::::::::::::::::::::::
```

```
OPSO test for generator VB_Rnd.bin
 Output: No. missing words (mw), equiv normal variate (z), p-value (p)
                                                          mw      z      p
   OPSO for VB_Rnd.bin      using bits 23 to 32      331181652.661 1.0000
   OPSO for VB_Rnd.bin      using bits 22 to 31      33246[illegible]57.092 1.0000
   OPSO for VB_Rnd.bin      using bits 21 to 30      574754******* 1.0000
   OPSO for VB_Rnd.bin      using bits 20 to 29      787507******* 1.0000
   OPSO for VB_Rnd.bin      using bits 19 to 28      915777******* 1.0000
```

When you start writing your own PRNG applications, now you know how to test it.