Statistical Tests of the SG100 Security Generator.

The simplest statistical test is to check if the SG100 noise strings has about the same number of ones and zeroes.

A test program (N1_TEST.EXE, included in Developer Package) is written that counts bytes and bits. The output is given in absolute and relative frequency.

To make comparison easy the difference between a relative frequency of 50% and observed frequency is computed relative to the standard deviation. These values are seldom higher than three, for random output.

Note, that as the program outputs a large number of sigma values, it sometimes happens that a sigma value higher than three is found. This is normal for random strings. If in doubt, accuracy can be increased by counting a longer noise string.

If we, as an example, count 6,400,000 bytes and find 25,603,990 "one" bits then we have a relative frequency of 0.50007793 Sigma = 1.1 That is 50.008% one bits.

To increase accuracy we count 441,600,000 bytes. We find 1,766,378,269 "one" bits yielding a frequency of 0.49999385 (Sigma = -0.7)

That was very close to 50% "one" bits and 50% "zero" bits. Desperately we can read 1,651,200,000 bytes and count to 6,604,734,712 "one" bits and the frequency is 0.49999506 (Sigma = -1.1)

Download complete test results from http://www.protego.se/doc/n1_test.txt

The SG100 also passes the Diehard test. The Diehard test, by George Marsaglia, consists of several statistical counts that should have a specified distribution if the input string is random. By comparing observed counts to a theoretical count we can see if a string is random or not.

```
For a sample of size 500: mean
SG100.DAT using bits 6 to 29 1.942
 duplicate    number      number
  spacings   observed   expected
0                  70.     67.668
1                 142.    135.335
2                 139.    135.335
3                  86.     90.224
4                  36.     45.112
5                  18.     18.045
6 to INF            9.      8.282

Chisquare with 6 d.o.f. = 2.61 p-value= .143850
```

The observations above are to few to give high accuracy. This problem originates in that the Diehard program do not adjust the sample sizes to a larger test file.
The forthcoming revision of diehard may correct this problem.

Download SG100 Diehard test from http://www.protego.se/doc/diehard.txt.

Go to Diehard site.
http://stat.fsu.edu/~geo/diehard.html

Kelce S. Wilson suggested a statistical test where the longest strings of ones and zeros are measured. A program was written to count the frequency of continuous strings of ones and zeros as a function of string length, and print the results.

Download test results from http://www.protego.se/doc/strings.txt.

Robert Davies have tested hardware random number generators, including the SG100, for a lottery application.
Go to Robert Davies lottery page.
http://nz.com/webnz/robert/recent/lottery.html