

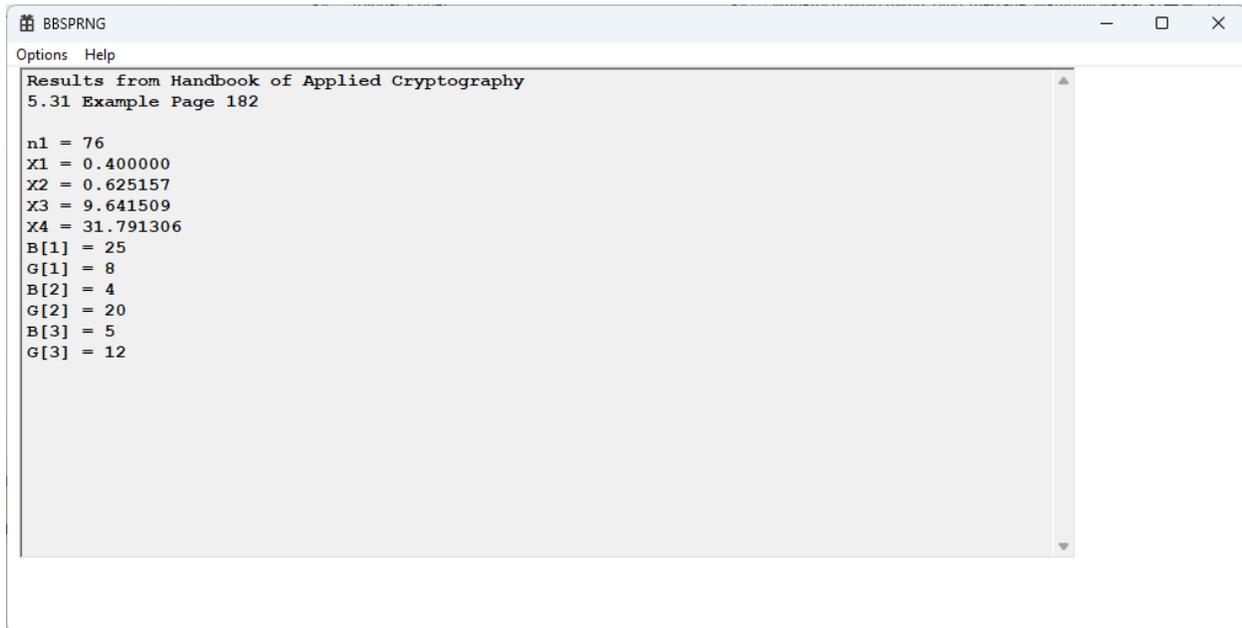
Blog Entry © Friday, February 27, 2026, by James Pate Williams, Jr., C Pseudorandom Bit Generators and Four Statistical Tests

Back on May 22, 2018, I created a C# application to test two test two ANSI X9.17 random bit generators. The generators were based on the cryptographic algorithms triple-AES and triple-DES. Yesterday and today, I created a test program for the two algorithms:

1. The standard C pseudorandom number generator (rand)
2. The Blum-Blum-Shub cryptographic PRNG

References:

1. ***Handbook of Applied Cryptography*** by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Chapter 5.
2. [Runs Test – Numerical Explorations](#)



```
BBSPRNG
Options Help
Results from Handbook of Applied Cryptography
5.31 Example Page 182
n1 = 76
X1 = 0.400000
X2 = 0.625157
X3 = 9.641509
X4 = 31.791306
B[1] = 25
G[1] = 8
B[2] = 4
G[2] = 20
B[3] = 5
G[3] = 12
```

```
BBSPRNG
Options Help
Also see 5.40 Algorithm Blum-Blum-Shub pseudorandombit generator
Blum-Blum-Shub PRNG

n1 = 10036
X1 = 0.259200
X2 = 1.541040
X3 = 45.568000
2267 >= B[1] = 2525 <= 2733
1079 >= B[2] = 1306 <= 1421
 502 >= B[3] = 600 <= 748
 223 >= B[4] = 304 <= 402
  90 >= B[5] = 140 <= 223
  90 >= B[6] = 80 <= 223
2267 >= G[1] = 2612 <= 2733
1079 >= G[2] = 1199 <= 1421
 502 >= G[3] = 606 <= 748
 223 >= G[4] = 312 <= 402
  90 >= G[5] = 141 <= 223
  90 >= G[6] = 82 <= 223
X5 = 0
```

```
BBSPRNG
Options Help
Results from Handbook of Applied Cryptography
5.32 Note Page 183
Standard C PRNG

n1 = 10058
X1 = 0.672800
X2 = 1.045836
X3 = 17.296000
2267 >= B[1] = 2505 <= 2733
1079 >= B[2] = 1296 <= 1421
 502 >= B[3] = 590 <= 748
 223 >= B[4] = 300 <= 402
  90 >= B[5] = 162 <= 223
  90 >= B[6] = 91 <= 223
2267 >= G[1] = 2548 <= 2733
1079 >= G[2] = 1229 <= 1421
 502 >= G[3] = 628 <= 748
 223 >= G[4] = 313 <= 402
  90 >= G[5] = 158 <= 223
  90 >= G[6] = 76 <= 223
X5 = 0
```

Note that the Blum-Blum-Shub PRNG failed on the Blk[6] and Gap[6] tests. Also note that the Standard C program failed the Gap[6] test and just barely passed the Blk[6] test. X5 is the long runs test (blocks or gaps with a run of 34 or greater).