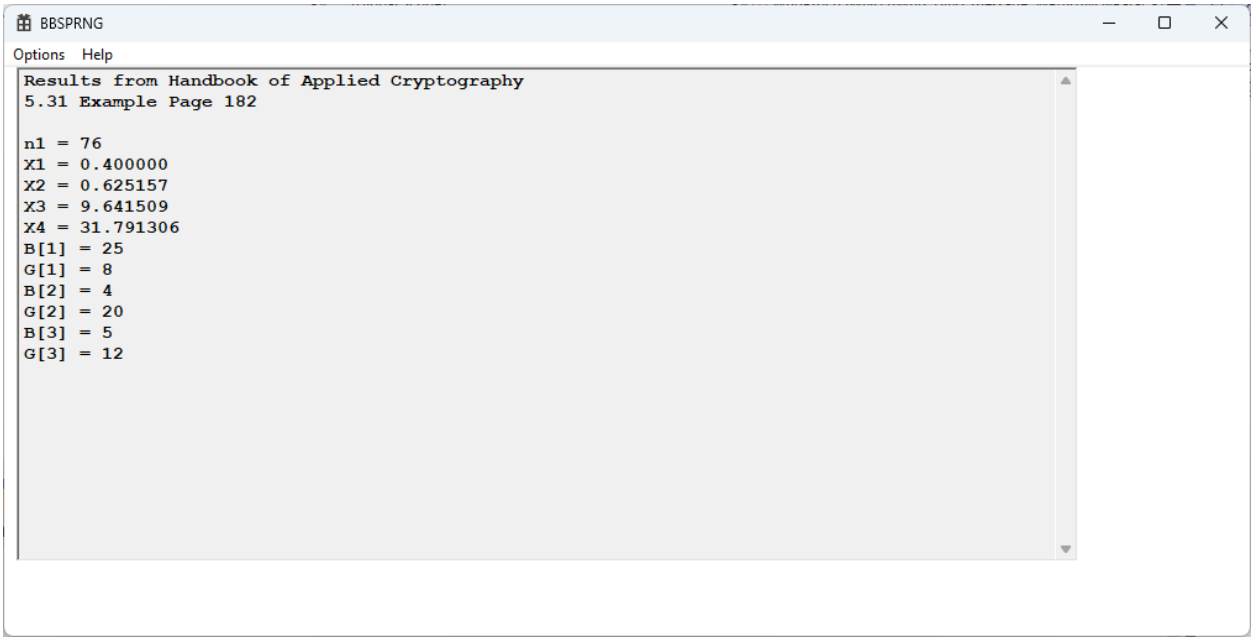
Blog Entry © Friday, February 27, 2026, by James Pate Williams, Jr., C Pseudorandom Bit Generators and Four Statistical Tests

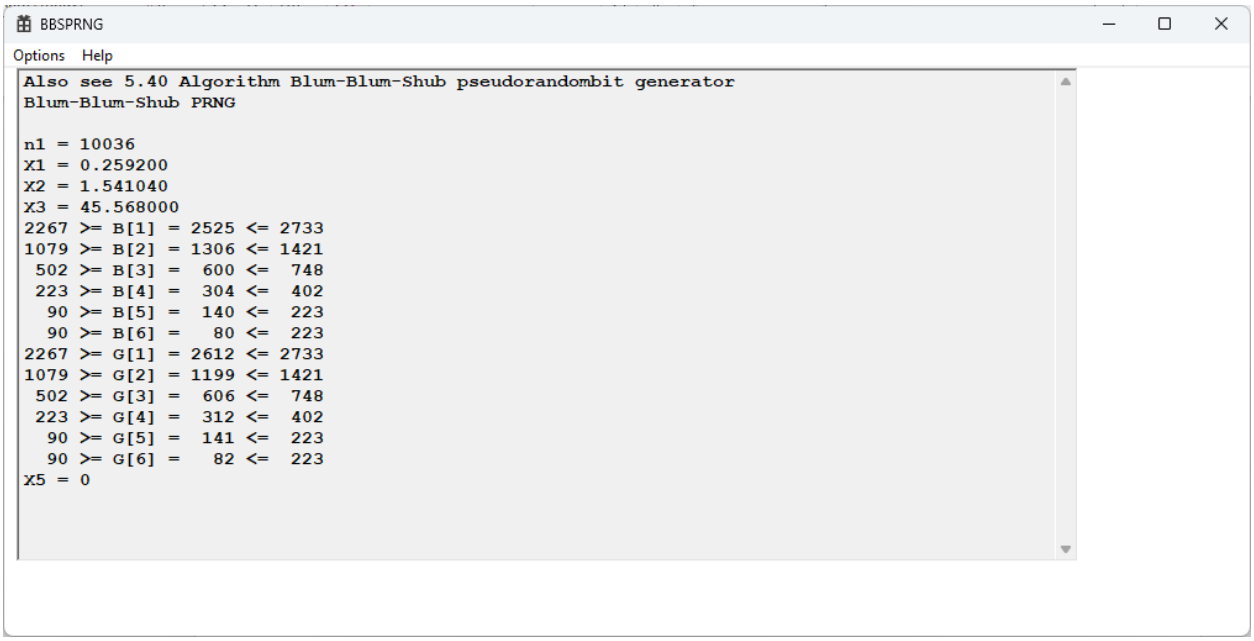
Back on May 22, 2018, I created a C# application to test two test two ANSI X9.17 random bit generators. The generators were based on the cryptographic algorithms triple-AES and triple-DES. Yesterday and today, I created a test program for the two algorithms:

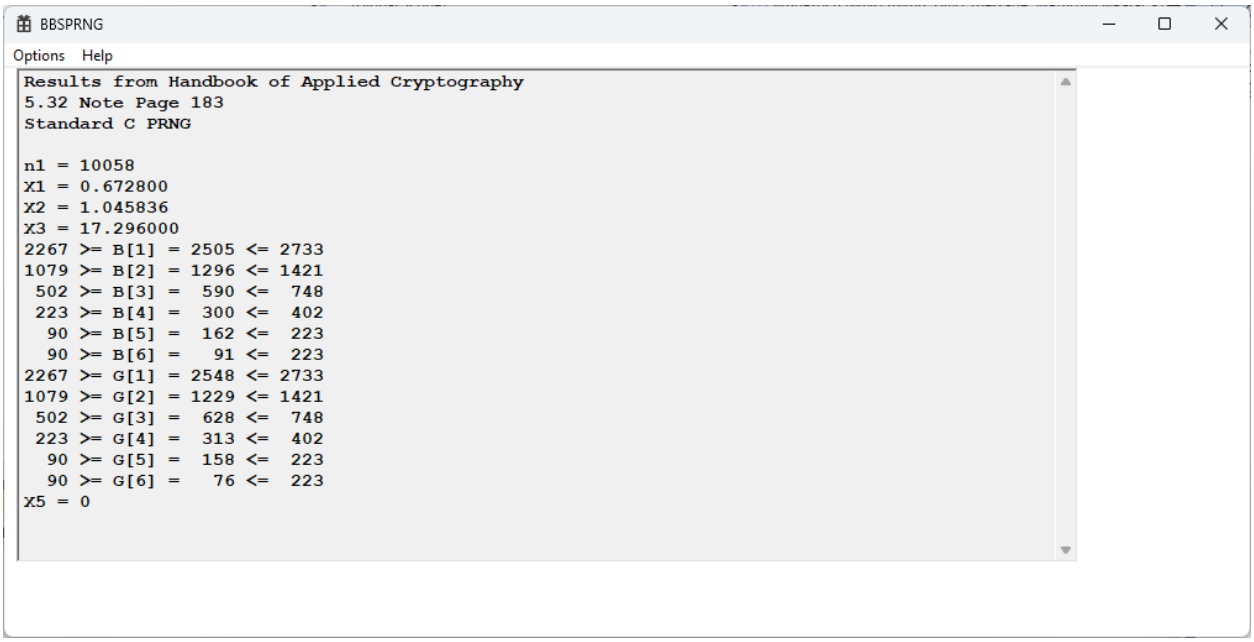
1. The standard C pseudorandom number generator (rand)
2. The Blum-Blum-Shub cryptographic PRNG

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







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).