2009/2010 Seminar Series

www.cs.unb.ca

Faculty of Computer Science UNB

"PSEUDO-RANDOM NUMBERS" BY Prof. Bill Knight

Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. — John von Neumann

1 Grandparents -- Two Early Methods
2 Three Ideas of What Random Means
   i. Kolmogorov
   ii. Unpredictable
   iii. Computational Complexity
3 (Empirical) Tests of Generators
4 Real Random Numbers Are Not Really Safe
5 Matrix Generators -- A Large Class Which Includes
   i. Linear Congruential
   ii. Shift Registers
   iii. The Mersenne Monster
6 Make It Better
   i. Combine Two or More Generators
   ii. Shuffle the Sequence
7 Monte Carlo and Parallel Computing
8 The Paranoid World of
   Games, Gambling, Commerce, Military, & Spies
9 End

Wednesday, February 17th @ 3:40pm
Information Technology Center, C-317