SUBMIT TO: Santa's Crypto Get-Together, Prague 2004

ABSTRACT TITLE: A Concise Introduction to Random Number Generators

AUTHOR LISTING: Peter Hellekalek
Dept. of Mathematics
University of Salzburg
Hellbrunner Straße 34
A-5020 Salzburg, Austria
e-mail: peter.hellekalek@sbg.ac.at
WWW: http://random.mat.sbg.ac.at/

ABSTRACT TEXT

Random number generators (RNGs) are a basic tool in applied cryptography as well as in stochastic simulation (keyword: Monte Carlo Method). Bad RNGs may not only ruin your simulation or your internet casino but also, in some (rare) cases, cost you your life (keyword: Russian one-time pads).

Random number generation has four aspects:

- the design of algorithms;
- theoretical analysis;
- empirical (statistical) testing;
- practical issues.

In this talk, we will mainly discuss the first three points.

Randomness is in the eye of the beholder. Hence, RNGs come in many different flavours. They all have their deficiencies and, in many cases, unwanted side-effects occur.

What is a good random number generator? We will not be able to answer this question, but we will discuss a "checklist" for RNGs. We will present the fundamental concepts for the theoretical assessment of RNGs, and we will also dwell upon empirical testing, in particular upon Maurer's Universal Statistical Test for Random Bit Generators.

Finally, we will discuss the suitability of the Advanced Encryption Standard (AES) for a random number generator. The performance of AES is studied in a series of statistical tests that are related to classical cryptographic notions like confusion and diffusion.