PROBABILITY
AND
MATHEMATICAL STATISTICS
Vol. 15 (1995), pp. 101–114

CRYPTOGRAPHY, STATISTICS AND PSEUDORANDOMNESS. I

Stefan Brands
Richard Gill

Abstract: In the classical approach to pseudorandom number generators, a generator is considered to perform well if its output sequences pass a battery of statistical tests that has become standard. In recent years, it has turned out that this approach is not satisfactory. Many generators have turned out to seriously bias the outcome of some simulation experiments in which they were put to use. From a theoretical point of view, the classical approach does not at all explain in what way a completely deterministic algorithm can be said to simulate randomness.

Much less known is that cryptographers, who have a need for pseudorandom numbers of very high quality, have developed a theory that actually explains why a pseudorandom number generator can simulate randomness. Our aim in this two-part paper is to make this theory more accessible for mathematical statisticians and probabilists.

2000 AMS Mathematics Subject Classification: Primary: -; Secondary: -;

Key words and phrases: -