1. Record Nr. UNINA9910695299803321

Autore	Rukhin Andrew L
Titolo	A statistical test suite for random and pseudorandom number generators for cryptographic applications [[electronic resource] /] / Andrew Rukhin ... [and others]
Pubbl/distr/stampa	[Gaithersburg, MD] : , : [U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology], , [2001]
Edizione	[Rev.]
Descrizione fisica	xi, 153 pages : digital, PDF file
Collana	NIST special publication ; ; 800-22
Altri autori (Persone)	RukhinAndrew L BasshamLawrence E
Soggetti	Random number generators Statistical hypothesis testing Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from title screen (viewed on July 24, 2006). "With revisions dated May 15, 2001."
Nota di bibliografia	Includes bibliographical references (page G-1).
Sommario/riassunto	This paper discusses some aspects of selecting and testing random and pseudorandom number generators. The outputs of such generators may be used in many cryptographic applications, such as the generation of key material. Generators suitable for use in cryptographic applications may need to meet stronger requirements than for other applications. In particular, their outputs must be unpredictable in the absence of knowledge of the inputs. Some criteria for characterizing and selecting appropriate generators are discussed in this document. The subject of statistical testing and its relation to cryptanalysis is also discussed, and some recommended statistical tests are provided. These tests may be useful as a first step in determining whether or not a generator is suitable for a particular cryptographic application. However, no set of statistical tests can absolutely certify a generator as appropriate for usage in a particular application, i.e., statistical testing

cannot serve as a substitute for cryptanalysis. The design and cryptanalysis of generators is outside the scope of this paper.