1. Record Nr. UNISA996466094603316

Autore	Greenfield Jonathan S
Titolo	Distributed Programming Paradigms with Cryptography Applications [[electronic resource] /] / by Jonathan S. Greenfield
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1994
ISBN	3-540-49014-0
Edizione	[1st ed. 1994.]
Descrizione fisica	1 online resource (XI, 184 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 870
Disciplina	005.13
Soggetti	Programming languages (Electronic computers) Software engineering Computer programming Data encryption (Computer science) Probabilities Programming Languages, Compilers, Interpreters Software Engineering/Programming and Operating Systems Programming Techniques Software Engineering Cryptology Probability Theory and Stochastic Processes
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Overview -- The RSA public-key cryptosystem -- Notation for distributed algorithms -- The competing servers arrays -- A distributed algorithm to find safe RSA keys -- Distributed factoring with competing servers -- The synchronized servers pipeline -- Message block chaining for distributed RSA enciphering -- Generating deterministically certified primes.
Sommario/riassunto	This monograph describes a programming methodology based upon programming paradigms and generic programs and demonstates how distributed application programs can be developed by simple substitution of data structures and sequential procedures. The author introduces generic programs for two paradigms and shows how to

derive new distributed programs for several applications related to the RSA cryptosystem, including RSA enciphering and deciphering, prime number generation, and factoring. The book is well-written and easily accessible to the non-expert. The work is an appealing combination of the theory and practice of parallel computing and provides a clear introduction to the theory and practice of RSA cryptography.