1. Record Nr. UNINA9910465187503321

Autore	Rass Stefan
Titolo	Cryptography for Security and Privacy in Cloud Computing
Pubbl/distr/stampa	Norwood : , : Artech House, , 2013 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2013]
ISBN	1-60807-576-1
Descrizione fisica	1 online resource (264 p.)
Collana	Artech House information security and privacy series
Altri autori (Persone)	SlamanigDaniel
Disciplina	005.8/2
Soggetti	Computer networks - Security measures Cloud computing Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cryptography for Security and Privacy in Cloud Computing; Contents; Chapter 1 Introduction; 1.1 MODERN CRYPTOGRAPHY; 1.2 CLOUD COMPUTING; 1.3 DIGITAL IDENTITY, AUTHENTICATION, AND ACCESS CONTROL; 1.4 PRIVACY-ENHANCING TECHNOLOGIES; 1.5 OUTLINE; References; Chapter 2 Fundamentals; 2.1 NUMBER THEORY; 2.1.1 Drawing Random Coprime Elements; 2.1.2 Computing Inverse Elements Modulo a Prime; 2.1.3 Computing Negative Powers Modulo a Prime; 2.1.4 Getting (Large) Primes; 2.1.5 Quadratic Residues, Legendre Symbol, and Jacobi Symbol; 2.2 RINGS, GROUPS, FIELDS, AND LATTICES. 2.2.1 Finding a Generating Element2.2.2 Groups of Quadratic Residues; 2.2.3 Constructing a Subgroup; 2.2.4 Constructing General Finite Fields; 2.2.5 Homomorphy and Isomorphy; 2.2.6 Elliptic Curves; 2.2.7 Pairings; 2.2.8 Lattices; 2.3 CODING; 2.4 COMPUTATIONAL COMPLEXITY; 2.4.1 Computational Intractability; 2.4.2 Factorization-Related Assumptions; 2.4.3 Discrete-Logar.
Sommario/riassunto	As is common practice in research, many new cryptographic techniques have been developed to tackle either a theoretical question or foreseeing a soon to become reality application. Cloud computing is one of these new areas, where cryptography is expected to unveil its power by bringing striking new features to the cloud. Cloud computing is an evolving paradigm, whose basic attempt is to shift computing and

storage capabilities to external service providers. This resource offers an overview of the possibilities of cryptography for protecting data and identity information, much beyond well-known cryptographic primitives such as encryption or digital signatures. This book represents a compilation of various recent cryptographic primitives, providing readers with the features and limitations of each.