1.	Record Nr.	UNINA9910298962703321
	Autore	Delfs Hans
	Titolo	Introduction to Cryptography : Principles and Applications / / by Hans Delfs, Helmut Knebl
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
	ISBN	3-662-47974-5
	Edizione	[3rd ed. 2015.]
	Descrizione fisica	1 online resource (XX, 508 p. 5 illus.)
	Collana	Information Security and Cryptography, , 2197-845X
	Disciplina	005.74
	Soggetti	Data structures (Computer science) Information theory Number theory Data protection Computer science - Mathematics Data Structures and Information Theory Number Theory Data and Information Security Mathematics of Computing
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Introduction -- Symmetric-Key Encryption -- Public-Key Cryptography -- Cryptographic Protocols -- Probabilistic Algorithms -- One-Way Functions and the Basic Assumptions -- Bit Security of One-Way Functions -- One-Way Functions and Pseudorandomness -- Provably Secure Encryption -- Unconditional Security of Cryptosystems -- Provably Secure Digital Signatures -- App. A, Algebra and Number Theory -- App. B, Probabilities and Information Theory -- References -- Index.
	Sommario/riassunto	The first part of this book covers the key concepts of cryptography on an undergraduate level, from encryption and digital signatures to cryptographic protocols. Essential techniques are demonstrated in protocols for key exchange, user identification, electronic elections and digital cash. In the second part, more advanced topics are addressed, such as the bit security of one-way functions and computationally

perfect pseudorandom bit generators. The security of cryptographic schemes is a central topic. Typical examples of provably secure encryption and signature schemes and their security proofs are given. Though particular attention is given to the mathematical foundations, no special background in mathematics is presumed. The necessary algebra, number theory and probability theory are included in the appendix. Each chapter closes with a collection of exercises. In the second edition the authors added a complete description of the AES, an extended section on cryptographic hash functions, and new sections on random oracle proofs and public-key encryption schemes that are provably secure against adaptively-chosen-ciphertext attacks. The third edition is a further substantive extension, with new topics added, including: elliptic curve cryptography; Paillier encryption; quantum cryptography; the new SHA-3 standard for cryptographic hash functions; a considerably extended section on electronic elections and Internet voting; mix nets; and zero-knowledge proofs of shuffles. The book is appropriate for undergraduate and graduate students in computer science, mathematics, and engineering.