1.	Record Nr.	UNINA9910254087203321
	Autore	Meijer Alko R
	Titolo	Algebra for Cryptologists / / by Alko R. Meijer
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
	ISBN	3-319-30396-1
	Edizione	[1st ed. 2016.]
	Descrizione fisica	1 online resource (XIV, 301 p. 6 illus.)
	Collana	Springer Undergraduate Texts in Mathematics and Technology, , 1867-5506
	Disciplina	005.82
	Soggetti	Algebra Data structures (Computer science) Computer science—Mathematics Data Structures and Information Theory Discrete Mathematics in Computer Science
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Prerequisites and Notation -- Basic Properties of the Integers -- Groups, Rings and Ideals -- Applications to Public Key Cryptography -- Fields -- Properties of Finite Fields -- Applications to Stream Ciphers -- Boolean Functions -- Applications to Block Ciphers -- Number Theory in Public Key Cryptography -- Where do we go from here? -- Probability. .
	Sommario/riassunto	This textbook provides an introduction to the mathematics on which modern cryptology is based. It covers not only public key cryptography, the glamorous component of modern cryptology, but also pays considerable attention to secret key cryptography, its workhorse in practice. Modern cryptology has been described as the science of the integrity of information, covering all aspects like confidentiality, authenticity and non-repudiation and also including the protocols required for achieving these aims. In both theory and practice it requires notions and constructions from three major disciplines: computer science, electronic engineering and mathematics. Within mathematics, group theory, the theory of finite fields, and elementary number theory as well as some topics not normally covered in courses

in algebra, such as the theory of Boolean functions and Shannon theory, are involved. Although essentially self-contained, a degree of mathematical maturity on the part of the reader is assumed, corresponding to his or her background in computer science or engineering. Algebra for Cryptologists is a textbook for an introductory course in cryptography or an upper undergraduate course in algebra, or for self-study in preparation for postgraduate study in cryptology.