1. Record Nr. UNINA9910437573303321

Autore	Dooley John F
Titolo	A brief history of cryptology and cryptographic algorithms / / John F. Dooley
Pubbl/distr/stampa	New York : , : Springer, , 2013
ISBN	3-319-01628-8
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (xii, 99 pages) : illustrations (some color)
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	004.09 652.8 652.809
Soggetti	Data encryption (Computer science) - History Cryptography - History
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"ISSN: 2191-5768."
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction: A Revolutionary Cipher -- Cryptology Before 1500: A Bit of Magic -- The Black Chambers: 1500 – 1776 -- Crypto goes to War: 1861 – 1865 -- Crypto and the War to End All Wars: 1914 – 1917 -- The Interwar Period: 1919 – 1939 -- The Coming of the Machines: 1918 – 1945 -- The Machines Take Over: Computer Cryptography -- Alice and Bob and Whit and Martin: Public Key Crypto.
Sommario/riassunto	The science of cryptology is made up of two halves. Cryptography is the study of how to create secure systems for communications. Cryptanalysis is the study of how to break those systems. The conflict between these two halves of cryptology is the story of secret writing. For over two thousand years governments, armies, and now individuals have wanted to protect their messages from the “enemy”. This desire to communicate securely and secretly has resulted in the creation of numerous and increasingly complicated systems to protect one's messages. On the other hand, for every new system to protect messages there is a cryptanalyst creating a new technique to break that system. With the advent of computers the cryptographer seems to finally have the upper hand. New mathematically based cryptographic algorithms that use computers for encryption and decryption are so secure that brute-force techniques seem to be the only way to break

them – so far. This work traces the history of the conflict between cryptographer and cryptanalyst, explores in some depth the algorithms created to protect messages, and suggests where the field is going in the future.