1.

Record Nr.	UNINA9910734837703321
Autore	Banoth Rajkumar
Titolo	Classical and Modern Cryptography for Beginners / / by Rajkumar Banoth, Rekha Regar
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-32959-7
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (230 pages)
Altri autori (Persone)	RegarRekha
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Data protection - Law and legislation Computer networks - Security measures Data protection Cryptology Privacy Mobile and Network Security Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1: An Introduction to Classical And Modern Cryptography -- Chapter 2: Security Standards for Classical and Modern Cryptography -- Chapter-3: Mathematical Foundation for Classical and Modern Cryptography -- Chapter 4: Asymmetric Key Cryptography -- Chapter-5: Modern Cryptanalysis Methods, Advanced Network Attacks and Cloud Security.
Sommario/riassunto	This textbook offers the knowledge and the mathematical background or techniques that are required to implement encryption/decryption algorithms or security techniques. It also provides the information on the cryptography and a cryptosystem used by organizations and applications to protect their data and users can explore classical and modern cryptography. The first two chapters are dedicated to the basics of cryptography and emphasize on modern cryptography concepts and algorithms. Cryptography terminologies such as

encryption, decryption, cryptology, cryptanalysis and keys and key types included at the beginning of this textbook . The subsequent chapters cover basic phenomenon of symmetric and asymmetric cryptography with examples including the function of symmetric key encryption of websites and asymmetric key use cases. This would include security measures for websites, emails, and other types of encryptions that demand key exchange over a public network. Cryptography algorithms (Caesar cipher, Hill cipher, Playfair cipher, Vigenere cipher, DES, AES, IDEA, TEA, CAST, etc.) which are varies on algorithmic criteria like- scalability, flexibility, architecture, security, limitations in terms of attacks of adversary. They are the core consideration on which all algorithms differs and applicable as per application environment. The modern cryptography starts from invent of RSA (Rivest-Shamir-Adleman) which is an asymmetric key algorithm based on prime numbers. Nowadays it is enabled with email and digital transaction over the Internet. This textbook covers Chinese remainder theorem, Legendre, Jacobi symbol, Rabin cryptosystem, generalized ElGamal public key cryptosystem, key management, digital signatures, message authentication, differential cryptanalysis, linear cryptanalysis, time-memory trade-off attack, network security, cloud security, blockchain, bitcoin, etc. as well as accepted phenomenon under modern cryptograph. Advanced level students will find this textbook essential for course work and independent study. Computer scientists and engineers and researchers working within these related fields will also find this textbook useful.