1. Record Nr. UNINA9910554876603321

Autore	Grimes Roger A.
Titolo	Cryptography apocalypse : preparing for the day when quantum computing breaks today's crypto / / Roger A Grimes
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley, , [2020] ©2020
ISBN	1-119-61822-3 1-119-61823-1 1-119-61821-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (275 pages)
Disciplina	005.82
Soggetti	Data encryption (Computer science) Cryptography Quantum computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	Will your organization be protected the day a quantum computer breaks encryption on the internet? Computer encryption is vital for protecting users, data, and infrastructure in the digital age. Using traditional computing, even common desktop encryption could take decades for specialized ‘crackers’ to break and government and infrastructure-grade encryption would take billions of times longer. In light of these facts, it may seem that today’s computer cryptography is a rock-solid way to safeguard everything from online passwords to the backbone of the entire internet. Unfortunately, many current cryptographic methods will soon be obsolete. In 2016, the National Institute of Standards and Technology (NIST) predicted that quantum computers will soon be able to break the most popular forms of public key cryptography. The encryption technologies we rely on every day—HTTPS, TLS, WiFi protection, VPNs, cryptocurrencies, PKI, digital certificates, smartcards, and most two-factor authentication—will be virtually useless. . . unless you prepare. Cryptography Apocalypse is a crucial resource for every IT and InfoSec professional for preparing for

the coming quantum-computing revolution. Post-quantum crypto algorithms are already a reality, but implementation will take significant time and computing power. This practical guide helps IT leaders and implementers make the appropriate decisions today to meet the challenges of tomorrow. This important book: Gives a simple quantum mechanics primer Explains how quantum computing will break current cryptography Offers practical advice for preparing for a post-quantum world Presents the latest information on new cryptographic methods Describes the appropriate steps leaders must take to implement existing solutions to guard against quantum-computer security threats Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto is a must-have guide for anyone in the InfoSec world who needs to know if their security is ready for the day crypto break and how to fix it.