1.	Record Nr.	UNINA9910796805703321
	Titolo	Decrypting the encryption debate : a framework for decision makers
	Pubbl/distr/stampa	Washington, DC : , : The National Academies Press, , [2018] 2018
	ISBN	0-309-47156-7 0-309-47154-0
	Descrizione fisica	1 online resource (xiv, 104 pages)
	Collana	Consensus study report
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Computer networks - Security measures - Social aspects Privacy, Right of - United States Civil rights - United States
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Sommario/riassunto	Encryption protects information stored on smartphones, laptops, and other devices - in some cases by default. Encrypted communications are provided by widely used computing devices and services - such as smartphones, laptops, and messaging applications - that are used by hundreds of millions of users. Individuals, organizations, and governments rely on encryption to counter threats from a wide range of actors, including unsophisticated and sophisticated criminals, foreign intelligence agencies, and repressive governments. Encryption on its own does not solve the challenge of providing effective security for data and systems, but it is an important tool.At the same time, encryption is relied on by criminals to avoid investigation and prosecution, including criminals who may unknowingly benefit from default settings as well as those who deliberately use encryption. Thus, encryption complicates law enforcement and intelligence investigations. When communications are encrypted "end-to-end," intercepted messages cannot be understood. When a smartphone is locked and encrypted, the contents cannot be read if the phone is seized by investigators.Decrypting the Encryption Debate reviews how encryption

is used, including its applications to cybersecurity; its role in protecting privacy and civil liberties; the needs of law enforcement and the intelligence community for information; technical and policy options for accessing plaintext; and the international landscape. This book describes the context in which decisions about providing authorized government agencies access to the plaintext version of encrypted information would be made and identifies and characterizes possible mechanisms and alternative means of obtaining information.