Congressional
Research Service
Informing the legislative debate since 1914

# Encryption: Frequently Asked Questions

**Chris Jaikaran**
Analyst in Cybersecurity Policy

September 28, 2016

**Congressional Research Service**
7-5700
www.crs.gov
R44642

**CRS REPORT**
Prepared for Members and
Committees of Congress

# Summary

Encryption is a process to secure information from unwanted access or use. Encryption uses the art of cryptography to change information which can be read (plaintext) and make it so that it cannot be read (ciphertext). Decryption uses the same art of cryptography to change that ciphertext back to plaintext. Encryption takes five elements to work: plaintexts, keys, encryption methods, decryption methods, and ciphertexts. Data that are in a state of being stored or in a state of being sent are eligible for encryption. However, data that are in a state of being processed—that is being generated, altered, or otherwise used—are unable to be encrypted and remain in plaintext and vulnerable to unauthorized access.

## Purposes of Encryption

Today, encryption is as ubiquitous as the devices that connect to the Internet. Encryption is a tool that information security professionals and end users alike can employ to ensure that the data in their custody remain confidential to only those who are authorized to access the data. It also helps to ensure that data is accessed as the authorized users intend, and not altered by a third party.

Strong encryption helps users around the world trust the systems and data they are using, thereby facilitating the transactions that allow society to operate, such as economic activity, control of utilities, and government. This is important because the world has become more connected, and attackers have become more persistent and pervasive. It is difficult to overemphasize the extent to which Internet-connected systems are under attack. But the frequency with which data breaches are exposed in the news media can act as an indicator of the prevalence of active exploitations. Encryption is a tool used to thwart attempts to compromise legitimate activity and national security.

## Major Issues

However, encryption has posed challenges to law enforcement and elements of national security. Strong encryption sometimes hinders law enforcement's ability to collect digital evidence and investigate crimes in the physical world. As more real world transactions are conducted via digital means and adversaries continue to perpetrate crimes, this problem may become more pronounced. There are multiple sides to the encryption debate, but the sides generally reduce to two main parties: those who favor cryptosystems built as strongly as possible, and those who favor cryptosystems built with the opportunity for access if necessary and approved by a judicial authority.

Encryption has created new issues for end users, as well. The technology was adopted rapidly, and users were not afforded the same opportunities to alter their habits as with the more steady adoption of technologies in the past. With the quick adoption of encryption, users left themselves more vulnerable to being unable to access or share their own data, for instance in the event that they forget the key or lack a way to share that key.

One proposal to alleviate concerns over access to encrypted data by law enforcement includes mandating access for law enforcement while retaining strong encryption. However, this proposal undermines how encryption systems are built by introducing some extraordinary access into the system beyond the direct access of the user. This proposal carries risk as it creates an attack vector which adversaries of all types could seek to exploit. The increased risk raises the possibility that a persistent adversary will be able to circumvent the protections put in place to allow limited access and compromise the data and systems in use. In the 114th Congress, many activities have focused on encryption, including some legislative proposals.

# Contents

## Figures

## Tables

## Contacts

# Introduction

The ready availability and rapid adoption of encryption technologies has ignited a discussion on the applicability of the technology and the conditions under which those technologies should be used and made accessible. Information and communications technology (ICT) manufacturers have implemented strong cryptosystems into their products, which make their users and the devices themselves safer and more trustworthy. But while that happened, law enforcement officers have been increasingly stymied in their efforts to investigate crimes and enforce the rule of law. There are multiple sides to the encryption debate, but the sides generally reduce to two main parties: those who favor cryptosystems built as strongly as possible, and those who favor cryptosystems built with the opportunity for access if necessary and approved by a judicial authority.

Many technology companies, trade associations, security experts, and organizations dedicated to protecting civil liberties and human rights support the first argument.[1] This group argues that our modern economy relies on the trustworthiness of users and devices. They further argue that threats compromise that trustworthiness and put devices and their users under constant attack.[2] They also argue that deliberately weak cryptosystems will place their users and products at an international disadvantage and ultimately make everyone less safe.[3]

Many government agencies, including federal, state, and local law enforcement agencies, fall into the second group.[4] They argue that absolute privacy has never existed because judges could authorize the disclosure of information within their jurisdiction. The recent adoption of encryption technologies hinders the orders of judges to authorize disclosure of information and law enforcement's ability to conduct investigations.[5]

To provide context for this debate, this report will (1) provide a primer on the technology that enables encryption; (2) discuss the uses of encryption; and (3) discuss policy options for future actions on encryption.

# Technology

## What is encryption?

Encryption is a process to secure information from unwanted access or use. Encryption uses the art of cryptography, which comes from the Greek words meaning "secret writing," to change information which can be read (plaintext) and make it so that it cannot be read (ciphertext). Decryption uses the same art of cryptography to change that ciphertext back to plaintext.[6]

[1] Letter from Access et al. to Barack Obama, President of the United States of America, May 19, 2015, https://static.newamerica.org/attachments/3138—113/Encryption_Letter_to_Obama_final_051915.pdf.

[2] Ibid.

[3] Ibid.

[4] Cyrus R. Vance Jr., "Written Testimony" United States Senate Committee on Armed Services, hearing on "Cybersecurity and U.S. National Security," July 14, 2016, at http://www.armed-services.senate.gov/imo/media/doc/Vance_07-14-16.pdf.

[5] James Comey, "Remarks to the 2016 Symantec Government Symposium," August 30, 2016, at https://www.c-span.org/video/?414522-1/fbi-director-james-comey-addresses-concerns-voter-database-breaches.

[6] Matt Bishop, "Chapter 9: Basic Cryptography," in *Computer Security: Art and Science* (Boston, MA: Addison-

(continued...)

## How does encryption work?

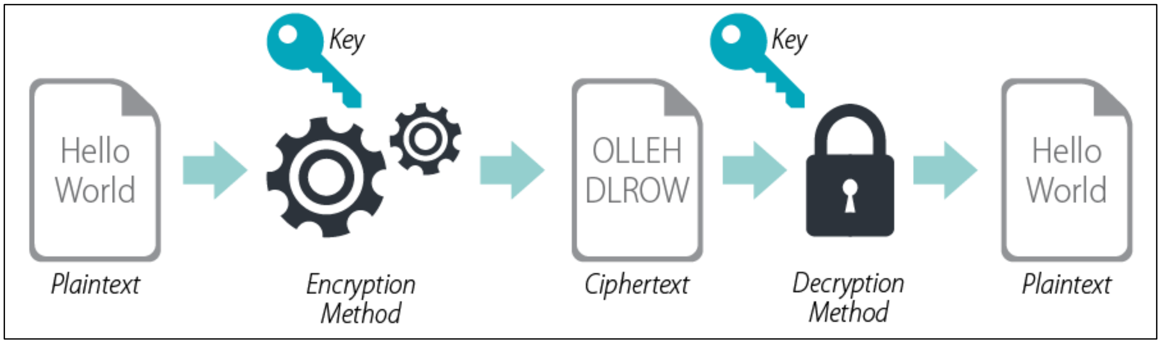
For computer systems, encryption works by applying a cryptosystem to the message, or block of data, that the user seeks to encrypt. A cryptosystem is a five-element system which includes a set of *plaintexts*, *keys*, *encryption methods*, *decryption methods*, and *ciphertexts*. The interaction of these elements is displayed below where $T_P$ is plaintext, $M_E$ is a method of encryption, $K$ is the key, $T_C$ is the cipthertext and $M_D$ is a method of decryption. The encryption and decryption algorithms govern how the cryptosystem substitutes characters in the plaintext and transposes it to a ciphertext, and then back to its original plaintext.

$$T_P + M_E + K = T_C$$

$$T_C + M_D + K = T_P$$

Using a simplified graphical representation, encryption would appear as follows:

**Figure 1. Graphical Representation of a Cryptosystem**



**Source:** CRS analysis.

In some cryptosystems, the key that encrypts the message and decrypts the message is the same—these systems are known as *symmetric.* In other cryptosystems, one key would encrypt a message while it will take another key to decrypt the message—these systems are known as *asymmetric.*

## How can data be encrypted?

To encrypt a message, or block of data, the user would choose an encryption method—in computer security, that is an algorithm—and choose a key.[7] The user would then enter the key into the algorithm with the plaintext to develop a ciphertext.

As shown in **Figure 1**, a plaintext, or the thing that a user seeks to encrypt, would be put through an encryption method and transformed into unintelligible information. This process requires both a key and the encryption method. A user with the key could take that unintelligible information and apply the decryption method, with the key, to transform the information into something intelligible.

There are many encryption methods, also known as standards, available for use by the public, such as the Data Encryption Standard and Blowfish.[8] However, many modern encryption

(...continued)

Wesley, 2003), pp. 217-240.

[7] Here, an "algorithm" means a set of steps which make up a process to execute an operation.

[8] National Institute Of Standards and Technology, "Data Encryption Standard," Federal Information Processing (continued...)

implementations use the Advanced Encryption Standard (AES). AES was developed as a result of a call for proposals from the National Institute of Standards and Technology (NIST), and once publicly scrutinized, it was accepted as a standard by the Department of Commerce in 2001.[9] Many cryptosystems today use AES as the method for how data are substituted and transposed to ensure security.

## What is a "key"?

A key is the input to the encryption and decryption methods (or algorithms, in the case of computer security) that guides the specific substitutions and transpositions the encryption and decryption methods perform.[10] While the same encryption method may be used to secure a wide array of data, each instance of that method being applied with a different key makes that encrypted data unique.

In implementing a cryptosystem, the user generates a key by creating, and continuing to use, a password, passphrase, or passcode. In these cryptosystems, each user has a unique password, or key, but shares the encryption and decryption methods among all users. Alternatively, the system could generate a key for the user. This second technique is common in securing website connections.

Depending on the implementation of the cryptosystem, the key may be the password (or passphrase or passcode). Or, it could be an element necessary to generate the key used in the cryptosystem, as is the case with the iPhone. In the iPhone's cryptosystem, the user generated passcode is combined with the phone's unique identifier to create the key each time the passcode is entered. In this system, the key is not stored on the device.

The secrecy of the key is a crucial element that ensures a cryptosystem is secure. An adversary may intercept the ciphertext and know the encryption standard in use on that system. However, the key will remain a secret, and as a result, so too will the ciphertext.

Another way of thinking about the importance of the key is that those who have access to the key have access to the data. Expanding on this concept, whoever is able to discover the key, can discover the data. That is why the secrecy of a key is so critical to the overall security of a cryptosystem.

It is because the key is so critical to a cryptosystem that keys and data are kept and transmitted separately in secure cryptosystems. If a key was sent along with a ciphertext, an adversary who intercepts that communication would have all elements necessary to decrypt the message.

## What is key escrow?

Key escrow systems propose that an intermediary holds encryption keys so that authorized users may access their data in the event that they lose or forget their password, or in the event that a

(...continued)

Standard 46-3, October 25, 1999, at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf; and B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," paper, 1994, at https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html.

[9] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing standard 197, November 26, 2011, at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[10] Willian Stallings and Lawrie Brown, "Chapter 2: Cryptographic Tools," in *Computer Security: Principles and Practice*, 2nd ed. (Boston, MA: Pearson, 2012), p. 40.

government agency presents the intermediary with a court order to hand over the data. While this appears to be a compromise to the encryption debate, some have argued that key escrows dilute overall security while attempting to strike a balance between individual and national security.[11] Intermediaries may become the target of a variety of attacks. Hackers will seek to circumvent any security put in place to protect the keys, seeking to reap the payload of an unknown trove of users' keys—and data. It is also foreseeable that governments may use the range of tools at their disposal (espionage, legal, economic, etc.) to obtain the keys. The use of an intermediary to reserve encryption keys arguably creates a weakness by which all users may have their data compromised.[12] Current strong cryptosystems limit knowledge of the key to only the creator of the key (and with whomever that user decides to share their key). Creating one or more repositories for keys (the escrow) increases the opportunities for the keys to become known. One way for this to happen is that the repository itself has a weakness which exposes the keys.[13] Another is for an insider or a hacker to expose information held by the repository.[14]

## What is a split key?

A split key scheme is where a key is mathematically split into $N$ pieces, of which only a majority of those pieces is necessary to recreate a usable key to decrypt data. This may be represented as $R$=($N$-$x$), where $R$ is the recovery key and $x$ is some number less than $N$. Proponents of this structure suggest that those holding the pieces of a key must independently agree, and in a majority, to allow access to data. For instance, in this scheme, the user will retain a complete copy of their key, but three organizations (the government, the platform provider, and another party) would also have parts of the key, and two of those three would need agree to recreate the key before someone other than the user could access the encrypted data. However, opponents of this scheme point out that the holders of the pieces of the key will likely become targets for adversarial attacks, increasing the likelihood that entire cryptosystems become compromised.[15]

## What are "public" and "private" keys?

Public keys and private keys are used in an asymmetric cryptosystem. In this system, a public key is a key that is known to anyone, it is not a secret. It may be used by anyone to encrypt data. However, the data can only be decrypted by the user or users with the private key, which is a secret. This system allows many users to submit information to one or more users confidentially and securely.

[11] H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P.G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1998, at https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html.

[12] Bankston, Kevin, "Statement of Kevin S. Bankston during a hearing titled 'Encryption Technology and Possible U.S. Policy Responses,'" U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform, April 29, 2015, at https://oversight.house.gov/wp-content/uploads/2015/05/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston-1.pdf.

[13] Tom Mendelsohn, "Secure Boot Snafu: Microsoft Leaks Backdoor Key, Firmware Flung Wide Open," *Ars Technica,* August 11, 2016, at http://arstechnica.com/security/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/.

[14] Dan Goodin, "Cluster of "Megabreaches" Compromises a Whopping 642 Million Passwords," *Ars Technica,* May 31, 2016, at http://arstechnica.com/security/2016/05/cluster-of-megabreaches-compromise-a-whopping-642-million-passwords/.

[15] Nakashima, Ellen and Gellman, Barton, "As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security," *The Washington Post,* April 10, 2015, at https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

Public and private keys also help address concerns of authentication. If a sender signs an item with their private key, then the recipient may verify the signature with the public key to have a reasonable understanding that the message is authentically from the sender.

Private keys are privately held; that is, held by the user. And public keys are held by trusted third parties which provide access to those keys when requested so that users may use them on demand. An example of this is when a user connects to a website via Hypertext Transfer Protocol-Secure (HTTPS). To enable the secure connection to the website, a user starts the process by sending a request to the site. The site would then send their public key to the user, and the user's computer would then generate a new key (to be used in the HTTPS connection), encrypt it with the website's public key and send that back. The user knows that only the website that has the private key could decrypt the information the user just sent. With the new, user-generated key, the website would create the secure connection with the user, indicated to the user by the HTTPS icon (frequently a lock symbol) in the browser window.

## What is a "backdoor"?

In computer science, the term "backdoor" has many definitions.[16] For the purpose of the encryption debate, a backdoor is a way of bypassing the normal authentication methods of a cryptosystem. In this context, the normal authentication method is that the user enters a key and encrypts or decrypts the data.

There are legitimate and illegitimate ways to access encrypted data. If an authorized user were to provide the password (or key) to another person, then the second person would have access via a normal authentication method and be a legitimate user. If someone were to guess a user's key, that person would access the encrypted data via a legitimate authentication method, but would be an illegitimate user.

Furthermore, any weakness, whether intentionally or unintentionally introduced in the cryptosystem can act as a backdoor. If such a weakness exists, anyone with the capability to exploit the weakness will have access to the information. It is unlikely that any single party will remain the sole user of a backdoor. Because of the increased amount of information generated with computer systems, and the connectedness of those systems, the systems are inherently a target for illegitimate access.[17]

Court-ordered access to encrypted data through the use of a backdoor falls into a grey area. On one hand the access would be beyond the normal authentication of the device, but on the other it would be within an existing legal structure that is deemed legitimate by society at large.[18] Society's current acceptance of that legal structure is evidenced through centuries of court cases which determined an equilibrium between an individual's right to privacy and the state's need to ensure security.

[16] Kim Zetter, "Hacker Lexicon: What is a Backdoor?," *Wired*, December 11, 2014, online at https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

[17] "When Back Doors Backfire," *The Economist*, January 2, 2016, available online at http://www.economist.com/news/leaders/21684783-some-spy-agencies-favour-back-doors-encryption-software-who-will-use-them-when-back.

[18] For more information on this issue, see CRS Report R44396, *Court-Ordered Access to Smart Phones: In Brief*, by Kristin Finklea, Richard M. Thompson II, and Chris Jaikaran.

## What is a "hash?"

A hash is separate from but related to encryption. A hash uses similar mathematical functions as an encryption method to produce a string of characters as an output. This output can only occur one way, so a hash value may be derived from a message, but knowing the hash value will not allow one to know the message.

Hash values are used to validate the integrity of a message. If the hash value for a message changes, then the message itself is altered. This allows a user to determine whether or not they will trust the message.

One may encrypt a message and hash a message, or only do one or the other. Although they use similar mathematical functions, they are not required to be used in tandem. The encryption is a way of achieving confidentiality, while the hash is a way of achieving integrity. See "What is to gain through using encryption?" for more.

## When did encryption begin?

Encryption is not new to human communications. There are examples of Egyptian scribes using transposed hieroglyphs in 1900 BC. Julius Caesar used a simple substitution cipher to send private messages to acquaintances via courier.[19] Thomas Jefferson invented a wheel cipher which was recreated during World War II for communications.[20]

The modern encryption debate ignited in the 1990s during what is often dubbed the "crypto-wars."[21] During this period, the U.S. government proposed the promulgation of encryption with a key-escrow system, known as the "clipper chip." Researcher Matt Blaze found a vulnerability in the security of the clipper chip and the government ended its campaign for key escrow to accompany encryption.

Our current encryption debate began early in the 21st century with the ready availability of encryption platforms which could inhibit government access to electronic evidence. The debate increased in fervor in 2014 when both Apple and Google added full-disk encryption to their mobile operating systems.[22] This by-default encryption exponentially increased the amount of digital evidence that law enforcement was not as easily able to access, and therefore the debate over security of individuals and national security became more prevalent.

## Is building a cryptosystem for encryption difficult?

While the standards for designing and implementing a cryptosystem are published and made publicly available, creating a usable and secure system is a challenging endeavor.[23]

[19] A cipher is a way to write a message as a code, but is not computer code.

[20] SANS Institute. "History of Encryption," InfoSec Reading Room paper, 2001, at https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730.

[21] For more information on the crypto-wars, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea, and CRS Report R44481, *Encryption and the "Going Dark" Debate*, by Kristin Finklea.

[22] Eric Geller, "A Complete Guide to the New 'Crypto Wars,'" *The Daily Dot*, May 5, 2016, at http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/.

[23] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 197 – Announcing the Advanced Encryption Standard (AES)," November 26, 2001, at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

In addition to having a mathematically sound standard to use for the encryption and decryption method, using very large prime numbers (numbers that are divisible only by themselves and one) in the algorithm is necessary to ensure that the secret key remains undiscoverable. If a number other than a prime number is used, the adversary may be able to use factors of that number (a pair of numbers that may be multiplied to generate a new number) to generate a key. That is, if a divisible number is used, the adversary may chance upon the solution by finding two other numbers that are factors of the chosen number. This is otherwise known as a "collision." Such primes are so large that they are not written out in character form but are represented exponentially, such as $2^{44,497}$-1. Additionally, strong ciphers are necessary. Such strong ciphers use 128 bits and 256 bits of data in modern encryption.[24] And finally, large key bit length is necessary to ensure that adversaries cannot compute a key through a brute force attack.[25] A weakness in any one of those elements—the mathematics behind the standard, the key bit length, the key itself, or the prime numbers used—can compromise the cryptosystem, either in its entirety or for a group of users.[26]

In addition to the complexity of implementing a secure cryptosystem, processing the algorithms that enable encryption comes at a cost—time, heat generated from the processing, and energy consumed. Although cryptosystems were around as the Internet was developing, these costs inhibited encryption from becoming ubiquitous, as it would have overly taxed early hardware and led to users abandoning the platform.[27]

## What is the difference between "Cryptanalysis," "Cryptography," and "Cryptology?"

According to the Committee on National Security Systems (CNSSI), the United States intergovernmental agency responsible for the security of information technology systems which are used for national security purposes:

- *Cryptanalysis* is the study of and techniques performed to defeat or otherwise circumvent a cryptosystem. It is the analysis of a cryptosystem to attack it;
- *Cryptography* is the use of a mathematical technique to encrypt or decrypt some data. It is the application of a cryptosystem; and
- *Cryptology* is the mathematical science that deals with cryptanalysis and cryptograph.[28]

## Can we break encryption?

Depending on the implementation, a cryptosystem is crackable. There are attacks against cryptosystems every day. Cryptanalysis contains three main types of attacks.

[24] A bit is the smallest unit of data in computer science. So, 128 bit encryption uses a key of 128 bits of data to encrypt and decrypt texts.

[25] AgileBits, "Guess why we're moving to 256-bit AES keys," press release, March 9, 2013, https://blog.agilebits.com/2013/03/09/guess-why-were-moving-to-256-bit-aes-keys/.

[26] Paul Van De Zande, "The Day DES Died," July 22, 2001, https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722.

[27] Craig Timberg, "Net of Insecurity: The Making of a Vulnerable Internet," *The Washington Post,* May 30, 2015.

[28] Committee on National Security Systems, "National Information Assurance (IA) Glossary," instruction, April 26, 2010, at https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf.

1. *Attacking the ciphertext*. In this type of attack, the adversary has the encrypted data and wants to discover the plaintext, and possibly the key.
2. *Attacking the plaintext*. In this type of attack, the adversary has encrypted data and its corresponding plaintext and tries to determine the key.
3. *Attacking chosen plaintexts*. In this type of attack, the adversary selects plaintexts to be enciphered with a cryptosystem and receives the resulting ciphertexts. Then, using that information, tries to determine the key used in that cryptosystem.[29]

However, cryptographers design cryptosystems to be practically uncrackable. A practically uncrackable system is one in which trying to attack a system using brute force—that is, guessing every possible iteration of the key until the key is discovered—cannot accomplish the goal within any usable amount of time. Cryptosystems are built to require processors to run through multiple instructions and multiple iterations of those instructions before something is encrypted or decrypted. Those iterations require time. Strong cryptosystems, using strong keys, would require multiple times the age of the universe to discover a key with today's computing power.[30]

Because of the large amount of possibilities, those seeking to use a brute-force attack do not just start at zero and add characters until they get to the key. Instead, they attack other elements of the system. For instance, knowing that users choose simple passwords, the attacker could start guessing likely options to greatly reduce the time to find the key.[31]

Or, an attacker could circumvent a cryptosystem entirely and insert themselves between the user and the information they are accessing. Data can only be encrypted while at rest (stored) or in transit (being sent). While a user accesses the data, or is otherwise processing the data, it is in plaintext. So, rather than try to compromise the cryptosystem, an attacker may determine that it is better to compromise the device that is employing the cryptosystem (e.g., the computer or the cell phone). If the attacker puts malicious software on the device that allows them access to what the user is viewing, they could see what the user intends to encrypt before the cryptosystem is activated.

So, although the encryption is still sound, it does not protect against other forms of attack. In this scenario, the attacker would have access to the unencrypted data on the device. So, if the device in question is a corporate laptop that uses full-disk encryption, when the user logs in and connects to a network, the laptop's contents are decrypted and available to the attacker. Such contents may include health records, corporate secrets, or even the activity of the user, such as websites being visited or applications being used.

[29] Matt Bishop, "Chapter 9: Basic Cryptography," in *Computer Security: Art and Science* (Boston, MA: Addison-Wesley, 2003), pp. 217-240.

[30] AgileBits, "Guess Why We're moving to 256-bit AES keys," press release, March 9, 2013, https://blog.agilebits.com/2013/03/09/guess-why-were-moving-to-256-bit-aes-keys/.

[31] Dinei Florencio, Cormac Herley, and Paul C. van Oorschot, "Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts," *USENIX Security 2014,* August 2014, at https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/passwordPortfolios.pdf.

# Uses

## Who uses encryption?

Encryption is used by a variety of users for a variety of purposes. Fundamentally, encryption enables information to remain confidential to a single user or between a user and multiple users. Encryption also enables a level of certainty that who is communicating is who they say they are (as in the case of public-private key encryption) and that the communication is only available to intended recipients.

Individuals use encryption to keep aspects of their lives held on digital platforms private on their devices and among those with which they share information.[32] Businesses use encryption to ensure that their research is kept confidential from their competitors, and to ensure that their transactions with their suppliers and customers are authentic.[33] Governments use encryption to assure their information is kept and handled in confidence.[34] Even without a user's interaction, devices may use encryption when communicating to other devices to ensure that commands received from one device are authentic and safe to execute.[35] However, those seeking to obscure their malicious activities from legal authorities may also employ encryption to thwart opportunities to disable and disband their malicious activity.[36]

## What can be encrypted?

In computer science, data exist in three states.

- Data at rest, or stored data: data resident on a device (e.g., a hard drive or smartphone) that are neither being manipulated nor otherwise processed.
- Data in motion, or data in transit: data being sent between or among various points.
- Data in use, or data in process: data that are being generated, manipulated, or otherwise used by a user or system.

Data that are at rest or in motion can be encrypted. In the case of data in motion, it is encrypted, then sent. However, data that are in use are in a plaintext form to the user or system so that they can manipulate that data, and thus these data cannot be encrypted.

## Where is encryption used?

A cybersystem includes the end terminals in use; the modems and routers used to transmit data; the servers that process the information; the software packages used in sharing that data; other

[32] Bruce Schneier, "Why We Encrypt," *Schneier on Security*, June 23, 2015, at https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html.

[33] Federal Trade Commission, "Start with Security: A Guide for Business," guidance, June 2015, at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[34] Office of Management and Budget, "Protection of Sensitive Agency Information," M-06-16, June 23, 2006, at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf.

[35] U.S. Department of Energy, "Secure Data Transfer Guidnace for Industrial Control and SCADA Systems," PNNL-20776, September 2011, at http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

[36] James Comey, "Remarks to the 2016 Symantec Government Symposium," August 30, 2016, at https://www.c-span.org/video/?414522-1/fbi-director-james-comey-addresses-concerns-voter-database-breaches.

network-connected devices on that network collecting, generating, and processing data; and the user. Encryption is used by all elements in the cybersystem to protect the data in that system, the users of the system, and the system itself.

The influx of new devices to the market (i.e., Internet of Things devices) multiplies cybersystems beyond the end-user terminal and network infrastructure. This expansion amplifies the opportunities for encryption to be applied as a protective measure. As Matt Blaze, a professor of computer science at the University of Pennsylvania, testified before Congress in April 2015:

> It is difficult to overstate the importance of robust and reliable computing and communications to our personal, commercial, and national security today. Virtually every aspect of our lives, from our health records to the critical infrastructure that keeps our society and economy running, is reflected in or supported in some way by increasingly connected digital technology. The influx of new communications and computing devices software over the last few decades has yielded enormous benefit to our economy as well as to our ability to connect with one another. This trend toward digital systems, and the benefits we reap from them, will only accelerate as technology continues to improve. Preventing attacks against our digital infrastructure by criminals and other malicious actors is thus now an essential part of protecting our society itself.[37]

## When is encryption applied?

Encryption can be applied to data at rest on a per file basis (e.g., encrypting a file with a unique password), or on the entire storage device (e.g., encrypting an entire hard drive or smartphone).

Encryption can also be applied before a file is transmitted; for instance, a user may encrypt a file before emailing it to a colleague. Or encryption may be applied to every packet of data in transit between or among points on a network, as in the use of virtual private networks (VPN) or HTTPS.[38]

Data exist as plaintext prior to its encryption. Points at which data is plaintext include when it is being created (e.g., taking a picture or typing a text), processed (e.g., editing a document), or otherwise used (e.g., the system accesses that file for routine maintenance).

## Why would one encrypt data or devices?

As people put more of their data online, and rely on Internet-connected services to conduct their daily business—business which includes health care, power generation and consumption, financial transactions, governance, travel, and relationships, to name a few—the devices people use are generating, collecting, storing and adapting information about them. This information is of value to adversaries of all sorts. If an unauthorized person were able to access these data, they would become aware of the more intimate and sensitive aspects of the data owner's life and business.

[37] Blaze, Matt, "Testimony for Hearing 'Encryption Technology and Possible US Policy Responses,'" House Committee on Government Oversight and Reform Information Technology Subcommittee, April 29, 2015, at https://oversight.house.gov/wp-content/uploads/2015/05/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Blaze.pdf.

[38] A VPN is a secure communications link between two points where all traffic is encrypted. Hypertext Transfer Protocol Secure, or HTTPS is encryption between a specific web service and a host.

Full disk encryption on a device, such as a smartphone, ensures that a person's life is kept confidential in the event that device is stolen or misplaced.[39] Encrypted files ensure that when a data breach occurs, user data are not immediately at the whim of the adversary.[40] Encryption can also curtail nefarious activity. If an adversary knows that a system is secured with strong encryption, that fact may deter the adversary from targeting that user or system.[41]

But encryption occurs beyond an end device or data server. No one has yet built a digital system that is natively and completely secure because cybersystems are large, complex, and contain various elements (e.g., hardware and software) within that system which are updated and replaced at varying intervals. In such a dynamic environment, vulnerabilities present themselves throughout the system. Nevertheless, society relies on these systems. Encryption applied throughout the cybersystem affords its users a level of certainty that their data and service are trustworthy—allowing modern society to remain functioning and productive.[42]

# Policy Discussion

## What is encryption's role in the "going dark" debate?

Simply, "going dark" is a term of art that represents the government's inability to obtain electronic evidence. While encryption has dominated the going dark debate, it is only one element of that debate.

The Federal Bureau of Investigation (FBI) describes going dark with the following scenario: "law enforcement at all levels has the legal authority to intercept and access communications and information pursuant to court orders, but it often lacks the technical ability to carry out those orders because of a fundamental shift in communications services and technologies."[43]

As technology has evolved, some companies have implemented automatic end-to-end encryption on certain communications and data. As a result, law enforcement has reported instances of being stymied from obtaining certain communications as well as stored data that have been encrypted.[44] For instance, of the 4,148 wiretap orders authorized by judges in 2015, there were 13 reported instances in which encrypted communications were encountered, and 11 of these 13 instances involved encryption hindering law enforcement officials.[45]

[39] Mindi McDowell and Matt Lytle, *Protecting Portable Devices: Data Security*, US-CERT, Security Tip (ST04-020_, February 6, 2016, https://www.us-cert.gov/ncas/tips/ST04-020.

[40] Mindi McDowell, *Understanding Encryption*, US-CERT, Security Tip (ST04-019), February 6, 2013, https://www.us-cert.gov/ncas/tips/ST04-019.

[41] National Institute of Standards and Technology, *Advising Users on Information Technology*, Bulletin, November 2007, http://csrc.nist.gov/publications/nistbul/November-2007.pdf.

[42] Blaze, Matt, "Testimony for Hearing 'Encryption Technology and Possible US Policy Responses,'" House Committee on Government Oversight and Reform Information Technology Subcommittee, April 29, 2015, at https://oversight.house.gov/wp-content/uploads/2015/05/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Blaze.pdf.

[43] The Federal Bureau of Investigation, "Going Dark Issue," press release, https://www.fbi.gov/services/operational-technology/going-dark.

[44] See CRS Report R44481, *Encryption and the "Going Dark" Debate*, by Kristin Finklea, as well as the Administrative Office of the U.S. Courts, Wiretap Report 2015.

[45] Ibid.

## What is to gain through using encryption?

Information security, or the security of information in computer systems, is based on a model with three elements.[46]

- *Confidentiality* means "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information." Stated otherwise, confidentiality ensures that when a user sends another user a message, they are certain that only those two users are able to read that message.
- *Integrity* means "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity." Stated otherwise, integrity ensures that when a user sends a message to another user, the message arrives as the sender intends, without alteration.
- *Availability* means "ensuring timely and reliable access to and use of information." Stated otherwise, availability ensures that when a user sends a message to another user, that message is available for the recipient to access when they so choose.

Cybersecurity professionals have tools available to them to help ensure integrity and availability. Hash values allow users to try to ensure the integrity of information, and dynamic routing tries to ensure the availability of information when a user requests it.[47] Ensuring the confidentiality of information had been challenging, until encryption became ubiquitous.

Encryption is a tool that users and cybersecurity professionals can employ to try to ensure that their data and communications remain confidential. As Jay Healey said, "The attackers are beating us in every area. And always have been. The one place that aids the defenders, the one place the mathematics is on our side, is on encryption. In that one area, we are stronger than they are."[48]

Also, by employing strong cryptosystems, users can achieve a level of integrity in their data and communications. Although encryption itself would not stop an adversary from intercepting and manipulating data, the altered data would not be readable by the user since the alteration would change one of the inputs (the ciphertext) in the cryptosystem. As a result, they would be made aware of illegitimate alterations to their data.

This extra layer of security also helps to mitigate the onslaught of attacks users face every day. In the physical world, an attacker would need to be physically near its target to carry out an attack. But online, attackers can automate a coordinated attack against many targets regardless of physical location because of the interconnected nature of the public Internet. Encrypting data mitigates the potential attacks users may face when they connect online.

[46] This model is codified in 44 U.S.C. §3552, from which the definitions are taken.

[47] "Dynamic routing" describes a technique where a network would select the optimal path for data traversing the network to optimize deliver of the data based on real-time network load.

[48] Jason Healey, "Cyber Risk Wednesday: 2016 Threat Landscape," Panel Discussion at the Atlantic Council, Washington, DC, December 9, 2015, http://www.atlanticcouncil.org/events/past-events/cybersecurity-experts-cautiously-optimistic-about-2016.

## What is lost through using encryption?

The spread of ubiquitous encryption occurred faster than many other technologies were adopted. The speed at which encryption was promulgated left many end-users without the time to consider the implications of employing strong encryption for their data.

If a user were to forget or otherwise lose the key, the data would remain in a ciphertext state and stay unreadable to that otherwise legitimate user.

With full-disk encryption by default, users have the opportunity to encrypt data without judging the sensitivity of that data first. A user's data may be sensitive, but not require strong security. In the physical world, a user may keep a diary in a locked desk drawer, but in the digital world, that same diary may be encrypted preventing access by anyone other than that user. The implications for that level of protection are generally not considered by users when they employ encryption.[49]

Strong encryption may deny otherwise-authorized users from accessing shared information, such as family photos and tax records, in the event that the user who maintains the key is not available to decrypt information.[50] This level of security is also a contributing factor to the encryption element of the going dark debate.

## What are the Fourth and Fifth Amendment implications?

Generally, impositions on the Fourth Amendment right to security of papers and effects against unreasonable searches and seizure is considered satisfied upon an independent judge issuing a warrant or other court order to access that information.

Fifth Amendment concerns are more nuanced. The Fifth Amendment protects an individual's right not to be compelled to give incriminating evidence against oneself.[51] Depending on the facts of the case, this might include providing one's passcode to a locked device. In the pre-digital era, the Supreme Court employed a distinction between requiring an individual to disclose a safe combination, which impermissibly required the target to reveal the contents of his mind, and handing over a safe key, which did not. However, the Court has yet to state whether this same dichotomy should apply to passcodes and passwords employed in more modern technology, and the lower courts are only in the early stages of developing case law on this subject.[52]

## What are the trade-offs?

The encryption debate today is a debate of values. On one hand, there is the core value of individual security, and privacy from each other and from the state. On the other hand, there is the core value of national security, that security of the state is necessary to ensure the security of the individual.

[49] Shahani, Aarti, "Mom Asks: Who Will Unlock Murdered Daughter's iPhone?," *National Public Radio*, March 30, 2016, at http://www.npr.org/sections/alltechconsidered/2016/03/30/472302719/mom-asks-who-will-unlock-her-murdered-daughters-iphone.

[50] Kalat, Andrew, "Online, No One Knows You're Dead," ShmooCon 2016 presentation, January 11, 2016, at https://archive.org/details/Online_No_One_Knows_Youre_Dead.

[51] See U.S. Constitution, Amendment V.

[52] See CRS Report R44407, *Encryption: Selected Legal Issues*, by Richard M. Thompson II and Chris Jaikaran, for a more detailed look at this case law.

Evaluation of the individual (or information) security versus national security values is hampered by lack of information. Both sides of the debate have presented general arguments and scenarios about the risks they hope to mitigate. The public debate on encryption has lacked information on the specific threats that strong, end-to-end encryption mitigates and why another form of encryption would put the public at risk. Conversely, the public debate has also lacked specific information on how strong, end-to-end encryption has stymied security activities and put the public at risk. Without this specific information, the public is generally unable to accurately determine the risk presented by encryption, or the lack of it. Instead, the debate is informed by extreme cases which present dire scenarios from which to form a position, but which may not accurately reflect the risk involved.

## Information Security

As discussed above, individual users are under constant attack online from adversaries near and far. The ease with which attacks can be carried out, regardless of geographic location, further exasperates information security professionals. Encryption is a tool information security professionals and end-users can employ to ensure the data under their care remains confidential and its integrity remains intact.

The systems users rely upon are under similar attack. Some of these systems govern life-sustaining and life-saving applications, such as wireless medical devices.[53] Pervasive encryption within these systems helps ensure the trustworthiness of those systems.

Additionally, any system that stores a key would also be vulnerable to an insider threat. An insider, or authorized user or employee, is a threat to such a system because they have legitimate access to the system. Insiders can violate security policies and compromise the security of a system unintentionally or intentionally.[54]

However, information security costs users in both time and computing power. Users also lose opportunities for their information to become available to loved ones or investigators if they are a victim and unable to provide the information.[55] Additionally, users may have a false sense of security through misconfigured cryptosystems which are vulnerable to a variety of attacks.

## National Security

Some have argued that the advances in technology have surpassed the government's ability to keep pace.[56] Without a balance between the advances in technology and government capabilities, some argue that law enforcement agencies at all levels are unable to enforce the rule of law through effective investigations. With this perceived imbalance, crimes online (such as child

[53] Food and Drug Administration, "Radio Frequency Wireless Technology in Medical Devices," Guidance for Industry and Food and Drug Administration Staff, August 14, 2013, at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf.

[54] Insiders could also unknowingly violate security policies; for instance, by clicking on attachments or links in a suspicious email, they could fall prey to a phishing scam and expose their computer and the larger network to exploitation. There are also examples of users knowingly violating their organizations security policies, such as Edward Snowden, Chelsea Manning, and Robert Hastings.

[55] Andrew Kalat, "Online, No One Knows You're Dead," ShmooCon 2016 presentation, January 11, 2016, at https://archive.org/details/Online_No_One_Knows_Youre_Dead.

[56] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," *Prepared Remarks for the Brookings Intuition*, October 16, 2014, at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

pornography and financial thefts) and crimes against online infrastructure (such as ransomware and denial of service attacks) will arguably go un- or under-investigated.

Additionally, encryption technologies help enable criminal associations to persist, such as the indoctrination of a lone wolf terrorist by foreign actors, and limit the ability for law enforcement to intervene for the safety of our communities.

The proposal from those championing national security is based on the premise that law enforcement must investigate criminal activity to maintain rule of law.[57] The discussion has generally not addressed the level of criminal activity that may go un- or under-investigated (through evidence being encrypted or otherwise) for the government to still maintain the rule of law. This is an element of the debate which some hope to entertain in 2017.[58]

## What current legislative proposals exist?

In the second session of the 114th Congress, Members have introduced a variety of legislative proposals to address elements of the encryption issue. **Table 1**, below, highlights bills that address elements of the encryption debate.

**Table 1. Status of Selected Encryption Legislation**

Introduced in the 114th Congress

| Bill Number | Bill Title | Summary | Status |
|---|---|---|---|
| H.R. 4528 | ENCRYPT Act of 2016 | Would prevent states from passing laws mandating decryption or backdoors. | Referred to the House Judiciary, and Energy and Commerce committees |
| H.R. 4839 | Protect Our Devices Act of 2016 | Prohibits the federal government from requiring an entity to break the encryption of a communication. | Referred to the House Intelligence and Judiciary committees. |
| H.R. 4651 | Digital Security Commission Act of 2016 | Would create a commission to study technology challenges and recommend policy solutions to Congress. | Referred to the House Energy and Commerce, Judiciary, and Foreign Affairs committees. |
| S. 2604 | Digital Security Commission Act of 2016 | Would create a commission to study technology challenges and recommend policy solutions to Congress. | Referred to the Committee on Homeland Security and Governmental Affairs |

**Source:** Congress.gov and CRS analysis.

**Notes:** The status of these bills is current as of September 28, 2016.

Additionally, Senators Burr and Feinstein have made a discussion draft of their proposal publicly available, but it has not yet been introduced.[59] The Burr-Feinstein draft, otherwise titled the

[57] James Comey and Sally Quillian, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy," Statement before the Senate Judiciary Committee, July 8, 2015, at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

[58] James Comey, "Remarks to the 2016 Symantec Government Symposium," August 30, 2016, at https://www.c-span.org/video/?414522-1/fbi-director-james-comey-addresses-concerns-voter-database-breaches.

[59] A copy of the draft is available on each Senator's website, at http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf or http://www.feinstein.senate.gov/public/index.cfm?a=files.serve&File_id=5B990532-CC7F-427F-(continued...)

"Compliance with Court Orders Act of 2016," would require a provider of computing services to either decrypt a communication or assist the government in decrypting the message in compliance with a court order. Under this proposal, a judge could issue a court order invoking this act in one or more of the following cases: (a) the crime resulted in or threatened death or serious bodily harm; (b) foreign intelligence, espionage and terrorism; (c) crimes against minors; (d) violent felonies; (e) serious Federal drug crimes; or (f) the state equivalents of any of the above.[60]

## What other policy options have been discussed to address encryption?

- **Continue to allow the courts to develop case law on encryption**. This status quo option would continue to allow cases such as the one concerning the San Bernardino iPhone to come up in courts.[61] But after a few years of this strategy both the government and the technology community are coalescing around a view that Congress legislate on the matter of the availability of encryption and law enforcement's access to encrypted communications, in order to provide uniformity and certainty.[62] Additionally, some have suggested that barring congressional action, market forces and other stakeholders (such as other governments) would be in a position to drive policy.[63]
- **Force platforms to maintain a way to access the plaintext of data.** Rather than focus on the users, this proposal would focus on the platform itself. In this reference, a platform is the suite of hardware, software, or databases that support the service being used (e.g., the Messages application for Apple, Inc. devices). This would allow a solution to arrive at scale, that is, for many users at once, since the providers of the encryption service would build in a mechanism to read plaintexts of data using their platform rather than rely on the individual compliance from users. However, this proposal would, by its nature, introduce a weakness in the security of that platform, one which would likely become the target for adversaries. Although the solution would apply across all users for legitimate access, it would be equivalent to providing adversaries with the opportunity to access the data for all users. One example of this proposal is for platforms to act as administrators of devices or services they provide, and use their administrator access to provide data to law enforcement.[64]

(...continued)

9942-559E73EB8BFB.

[60] For further information and analysis on legislative proposals, see CRS Report R44481, *Encryption and the "Going Dark" Debate*, by Kristin Finklea.

[61] For more information on the San Bernardino iPhone case, please see CRS Report R44407, *Encryption: Selected Legal Issues*, by Richard M. Thompson II and Chris Jaikaran.

[62] Testimonies provided by Bruce Sewell, representing Apple, Inc., and Cyrus Vance, representing the National District Attorney's Association to the House Judiciary Committee on March 1, 2016, at https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/.

[63] Chris Inglis, "Statement Before The Senate Armed Service Committee," Testimony on Cybersecurity and U.S. National Security, July 14, 2016, at http://www.armed-services.senate.gov/imo/media/doc/Inglis_07-14-16.pdf.

[64] Robert Thibadeau, "There Should Be No Encryption Backdoors, Only Front Doors," The Draft Trust Alliance, February 17, 2016, at https://www.drivetrust.com/wp-content/uploads/sites/2/2016/02/No_Encryption_Backdoors_Just_Front_Doors.pdf.

- **Improve the government's ability to investigate and extract digital evidence.** This proposal was offered by Susan Landau, a professor in cybersecurity policy at Worcester Polytechnic Institute, in testimony to the House Judiciary Committee.[65] In this proposal, the U.S. government would invest in research, capabilities, and capacity to continue to carry out investigations despite any technology employed which may act as a hindrance to the investigation. The cost of such an investment is unknown.
- **Create "compelled disclosure" laws.** Otherwise known as "key disclosure laws," this proposal would make it a criminal penalty to fail to produce plaintext versions of documents requested by law enforcement when asked for data held by someone with access. Australia implemented such a law.[66] However, such a law would likely face Constitutional challenges.

## Author Contact Information

Chris Jaikaran
Analyst in Cybersecurity Policy
cjaikaran@crs.loc.gov, 7-0750

[65] Landau, Susan, "Testimony for the hearing titled 'The Encryption Tightrope: Balancing American's Security and Privacy,'" House Judiciary Committee, March, 1, 2016, at https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf.

[66] The Cybercrime Act of 2001 can be read online at https://www.legislation.gov.au/Details/C2004C01213.