What Is Encryption?

ITIF Technology Explainer Series • www.itif.org

Encryption describes the process of converting readable data into a scrambled, unreadable format only authorized entities with the right decryption key can decode. Encryption algorithms are mathematical formulas that lay out a set of steps a computer takes to encrypt or decrypt information. Encryption and decryption each require a unique key, or a random string of characters. There are two types of encryption algorithms. The first is symmetric encryption, in which the same cryptographic key is used for both encryption and decryption. The second is asymmetric or public key encryption, which uses two keys: one public and one private. The sender uses the public key, which is shared freely, to encrypt a message only the recipient's private key can decrypt.

Encryption can provide confidentiality, authentication, integrity, and nonrepudiation; in other words, it can encode a message's contents, verify the message's origin, prove that the message hasn't been changed, and prevent senders from denying they sent the message. Advancements in the field of information security, and specifically in the use of encryption to protect the confidentiality of information, have vastly improved security for consumers and businesses. Encryption has become fundamental to security on networks such as the Internet, and is used in nearly every industry to securely store and transmit confidential data. Encryption allows consumers to securely access such popular online services as online shopping and banking, as well as other online service requiring a password, such as web mail, social networks, and patient portals.

Why Now?

As the cost of computing has fallen, so has the cost of encrypting data. As of 2019, 87 percent of all Internet traffic was encrypted to prevent third parties from intercepting this information.[1] Likewise, many devices encrypt the data they store, in part, to remove some of the incentive for thieves to steal them. For example, many companies automatically encrypt data stored on mobile devices so only a properly authenticated device owner can access the information. Finally, a number of online services have begun encrypting communications on their platforms so the content therein is only available to participants in those conversations. While the growing ubiquity of encryption has improved security for consumers and businesses, it has also created challenges for law enforcement, that may not be able to access certain information, such as data on a suspect's phone.

Prospects for Advancement

Companies will continue to integrate encryption into new products and services. Cloud-based services will expand the use of end-to-end encryption to not only protect data in transit, but also ensure stored data is secured such that no third party—not even the Internet service provider (ISP)—can access it.

Technologies such as homomorphic encryption and secure multiparty computation will enable continued improvements to data privacy and security. Homomorphic encryption allows users to analyze, manipulate, and process encrypted data without decrypting the data, ensuring it remains private. Meanwhile, secure multiparty computation allows multiple users with different data inputs to collaboratively analyze that data without revealing their individual inputs to each other, so there is no single point of attack for hackers to target.

Encryption will continue to improve web security through protocols such as Transport Layer Security (TLS), which websites can use to secure communications between their servers and web browsers. TLS protects sensitive data such as logins and payment information, and enables people to carry out sensitive tasks such as filing their taxes and renewing their driver's license online.

Companies will also add biometric authentication to products and services, for example, allowing users to authenticate to their phones using a finger or their face. Biometric authentication can be used alone, or as part of multifactor authentication in conjunction with a password or security token.

The Internet of Things presents some unique challenges because many devices have lower power and computing capabilities, which limits their ability to use best-in-class encryption. But with billions of devices connected to the Internet, and each other, encryption is necessary to secure all of the information these devices collect, store, and transmit.

Quantum computing poses both challenges and opportunities for encryption. On the one hand, it threatens to render some existing forms of encryption obsolete by easily solving the complex calculations encryption algorithms rely on. On the other hand, quantum computing would allow for new forms of encryption that would be even more secure than what is available today.

Applications and Impact

Encryption is a vital component of any modern organization's data security framework. Organizations that handle sensitive information rely on encryption to keep that information from falling into the wrong hands. Governments and militaries use it to protect state secrets, health care providers to safeguard personal health information, educational institutions to secure students' educational records, and companies that handle cardholder payment information use it to prevent fraud. Digital rights management software often relies on encryption to protect intellectual property. Encryption is also an important component of secure communication. Journalists use encrypted messaging services to communicate with confidential sources, and victim advocates use them to communicate with survivors of abuse and get them to safety.

Finally, encryption serves as the basis for innovations such as blockchain technology and virtual private networks (VPNs). Blockchains use encryption to provide anonymity, verify transactions, and prevent tampering, giving users confidence that their transactions are always private and secure. Meanwhile, VPNs encrypt all of the data that passes from users' computers to providers' servers, preventing local ISPs from monitoring users' online activity.

Policy Implications

Encryption plays an important role in improving data protection for businesses and consumers. The U.S. government has long invested in research and development of encryption and set standards for encryption protocols that define best practices for commercial and government use of encryption—and it should continue this role in the future.

More widespread use of encryption has also made it more difficult for law enforcement and national security agencies to access certain information that could help them prevent and investigate crimes and terrorism. Some in the intelligence community and in law enforcement argue governments should enforce mechanisms that would enable companies served with a lawful court order to decrypt information. This could take the form of laws that ban strong encryption or certain types of encryption, weaken encryption standards, call for "backdoors" that allow the law enforcement to circumvent encryption, or mandate key-recovery mechanisms called key escrows.

Each of these methods would reduce overall security for law-abiding citizens and businesses that rely on strong encryption to communicate privately. Should some governments weaken encryption, not only will it give hackers an advantage, but bad actors such as the terrorists and criminals the intelligence community is after would likely seek out foreign tools and services that do not have these weaknesses. Additionally, governments that impose limits on encryption would face economic consequences such as increased costs to consumers as businesses grapple with new requirements and higher security risks, and reduced security features that would damage companies' ability to do business abroad.

The U.S. government should strengthen encryption instead of weaken it, encourage continued innovation in encryption, and defend the right to encrypt around the world. Specific measures can be used to build trust and strengthen data security, such as maintaining robust encryption standards, establishing clear rules for how and when law enforcement can hack into private systems or compel companies to assist in their investigations, and requiring government agencies that discover security flaws to disclose them in a timely and responsible manner and work with private industry to fix them.

Recommended Reading

Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 14, 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

Michael McLaughlin, "Weakening Encryption Would Put Vulnerable Populations at Risk," *Innovation Files*, December 4, 2019, https://itif.org/publications/2019/12/04/weakening-encryption-would-put-vulnerable-populations-risk.

Daniel Castro, "Why FBI is Wrong on Encryption Workaround," *InformationWeek*, December 3, 2014, http://www.informationweek.com/strategic-cio/digital-business/why-fbi-is-wrong-on-encryption-workaround/a/d-id/1317824.

[1] Mary Meeker, "Internet Trends 2019" (Bond, June 11, 2019).