Topic Page: data encryption

Definition: **data encryption** from *The Macquarie Dictionary*

1.

the encoding of data so that it cannot be decoded without appropriate software or hardware, so as to prevent unauthorised access or use.

data encryptions

Summary Article: **data encryption**
From *The Columbia Encyclopedia*

the process of scrambling stored or transmitted information so that it is unintelligible until it is unscrambled by the intended recipient. Historically, data encryption has been used primarily to protect diplomatic and military secrets from foreign governments. It is also now used increasingly by the financial industry to protect money transfers, by merchants to protect credit-card information in electronic commerce, and by corporations to secure sensitive communications of proprietary information.

All modern cryptography is based on the use of algorithms to scramble (encrypt) the original message, called *plaintext*, into unintelligible babble, called *ciphertext.* The operation of the algorithm requires the use of a *key.* Until 1976 the algorithms were symmetric, that is, the key used to encrypt the plaintext was the same as the key used to decrypt the ciphertext. In 1977 the asymmetric or public key algorithm was introduced by the American mathematicians W. Diffie and M. E. Hellman. This algorithm requires two keys, an unguarded public key used to encrypt the plaintext and a guarded private key used for decryption of the ciphertext; the two keys are mathematically related but cannot be deduced from one another. The advantages of asymmetric algorithms are that compromising one of the keys is not sufficient for breaking the cipher and fewer unique keys must be generated.

In 1977 the Data Encryption Standard (DES), a symmetric algorithm, was adopted in the United States as a federal standard. DES and the International Data Encryption Algorithm (IDEA) are the two most commonly used symmetric techniques. The most common asymmetric technique is the RSA algorithm, named after Ronald Rivest, Adi Shami, and Len Adleman, who invented it while at the Massachusetts Institute of Technology in 1977. Other commonly used encryption algorithms include Pretty Good Privacy (PGP), Secure Sockets Layer (SSL), and Secure Hypertext Transfer Protocol (S-HTTP). The National Institute of Standards and Technology (NIST) is working with industry and the cryptographic community to develop the Advanced Encryption Standard (AES), a mutually acceptable algorithm that will protect sensitive government information and will be used by industry on a voluntary basis.

Data encryption is regarded by the U.S. government as a national-security issue because it can interfere with intelligence gathering—therefore, it is subject to export controls, which in turn make it difficult for U.S. companies to function competitively in the international marketplace. To resolve this dilemma, the federal government in 1993 proposed *key escrow encryption*, an approach, embodied in an electronic device called a “Clipper chip,” that makes broadly available a purportedly unbreakable encryption technique (although the code was broken by researchers in 1995) with keys to unlock the

information held in escrow for national security and law-enforcement purposes by the federal government. This approach, however, has been unacceptable to civil libertarians and to the international community. In 1994 the Clipper algorithm (called Skipjack) was specified in the Escrow Encryption Standard (EES), a voluntary federal standard for encryption of voice, facsimile (fax), and data communications over ordinary telephone lines. A subsequent compromise escrow scheme intended to create a standard for data encryption that balanced the needs of national security, law enforcement, and personal freedom was rejected in 1995; a compromise proposed in 1999 was also controversial.

The Columbia Encyclopedia, © Columbia University Press 2018

APA

data encryption. (2018). In P. Lagasse, & Columbia University, *The Columbia encyclopedia* (8th ed.). New York, NY: Columbia University Press. Retrieved from https://search.credoreference.com/content/topic/data_encryption

Chicago

"data encryption." In *The Columbia Encyclopedia*, by Paul Lagasse, and Columbia University. 8th ed. Columbia University Press, 2018. https://search.credoreference.com/content/topic/data_encryption

Harvard

data encryption. (2018). In P. Lagasse & Columbia University, *The Columbia encyclopedia*. (8th ed.). [Online]. New York: Columbia University Press. Available from: https://search.credoreference.com/content/topic/data_encryption [Accessed 13 November 2019].

MLA

"data encryption." *The Columbia Encyclopedia*, Paul Lagasse, and Columbia University, Columbia University Press, 8th edition, 2018. *Credo Reference*, https://search.credoreference.com/content/topic/data_encryption. Accessed 13 Nov. 2019.