# D

## DATA ENCRYPTION

Data encryption refers to the process of transforming electronic information into a scrambled form that can only be read by someone who knows how to translate the code. Encryption is not a new idea; it was used by Julius Caesar in the days of the Roman Empire to preserve secrecy in letters and messages. Encryption has played played a major role in many wars and in military circles generally; today, it is very important in the business world as well.

Encryption has turned electronic in modern times. It is the easiest and most practical method of protecting data stored, processed, or transmitted. It is commonly used to scramble the contents of contracts, sensitive documents, and personal messages sent over the Internet. More and more institutions, including small businesses with data to protect, also use encryption to protect data on their computer in-house.

### HOW ENCRYPTION WORKS

Encryption comes from the science of cryptography, which involves the coding and decoding of messages in order to protect their contents. One of the most ancient forms of it is letter substitution—thus, for instance, sending the next letter in the alphabet instead of the actual letter in the text. *Ifmmp xpsme* thus spells out *Hello world.*. In the electronic environment, every symbol has a numerical value expressible in binary notation. Thus the letter *A* is 01000001 and the letter *a* is 01100001. Humans cannot make out a vast stream of zeroes and ones, but it is child's play for a computer. Patterns of letters are therefore transformed before transmission by using an arbitrary key; the key may be used in arithmetic, logical, or other ways to make the underlying meaning inaccessible to anyone who does not know the key. The more binary digits the key has, the more difficult the code is to crack—meaning that the longer it takes a computer system, attempting to break the code, to find the key by trial and error.

### TYPES OF ENCRYPTION PROGRAMS

There are two main types of encryption programs, single key and public key.

**Single Key.** Single key encryption is also known as private key, secret key, or symmetric encryption. It means that the sender and the recipient of the data both hold the same key for translation. This single key is used both to code and to decode information exchanged between two parties. Since the same key is used to encrypt and decrypt messages, the parties involved must exchange the key secretly and keep it secure from outsiders. Private key encryption systems are usually faster than other types but they can be cumbersome when more than two parties need to exchange information.

**Public Key.** The second, and more commonly used, type of data encryption system is known as a public key system. This approach involves two separate keys: a public key for encoding information and a private key for decoding information. The public key can be held and used by any number of individuals and businesses, whereas only one party holds the private key. The system is particularly useful in electronic commerce: the merchant holds the private key and all customers have access to the public key. The public key can be posted on a Web page or stored in an easily accessible key repository. Public key encryption systems are widely available on the Internet and heavily used by large companies.

The best-known data encryption program is called RSA. It was developed in the late 1970s by three graduates of the Massachusetts Institute of Technology—Ronald Rivest, Adi Shamir, and Leonard Adleman. In the first decade of the twenty-first century, there were more than a billion installations of RSA encryption programs on computer systems worldwide. RSA scrambles data based on the product of two prime numbers, each of which is 100 digits long. RSA is known as a public key encryption system because many people can use it to encode information, but only the person who holds the key (or knows the value of the two prime numbers) can decode it. RSA is embedded in hundreds of popular software products. It is also available on the Internet as a free download.

A number of other data encryption programs enjoy wide use as well. Examples include Pretty Good Privacy (PGP), which is considered easy to use; Secure Sockets Layer (SSL) now referred to as Transport Layer Security (TLS), which is used by many companies that process health care data or that accept online credit card orders; and Data Encryption Standard (DES), which was invented by IBM in the mid-1970s and was the U.S. government standard for security until 2002 when Advanced Encryption Standard (AES) officially became the new standard. Triple DES, an advanced version of DES, is still used in some areas of the U.S. government.

## MOTIVATION FOR ENCRYPTION

Encryption systems cost money in the form of software and greater computer capacity. Processing of encrypted data in and out also adds time to all procedures. But the money is well spent. Betsy Spethmann, writing in 2005 for *Promo* magazine, reports that security breaches of systems holding customer data cost their owners on average $14 million per incident. In addition, once such breaches become known, the database owner typically loses at least 20 percent of its customers. The loss of troubled customers in large numbers is likely to increase. The National Conference of State Legislatures (NCSL) reported in December 2009 that forty-five U.S. states have passed laws requiring companies to notify employees or customers when their personal information has been compromised.

## TRENDS IN ENCRYPTION PRACTICES

In the early twenty-first century, many corporations materially strengthened their defenses against the interception of transmitted data by encryption; they also fortified their information systems with ever better firewalls against intruders. Companies have also focused more on *internal* security. In many companies data are routinely encrypted before transmission to another site—but remain in clear, unencrypted language on the computer itself, protected only by a system of passwords.

More and more companies in consequence are extending encryption to information backup. They are also exploring off-site storage of backup data on distant computers where they reside in encrypted form. Even such methods are not sufficient to protect data from individuals who, by the very nature of their jobs, have access to the sensitive data. Thus, at the boundaries of encryption other techniques of supervision and control must be devised to protect information.

Dave Raffo wrote in 2010 that, "Data backup security is a rapidly evolving—if not rapidly adopted—piece of the enterprise data storage world. It largely revolves around encryption, and has spread in the past few years from tape to host to disk, and is now an issue for the young cloud storage market." Cloud computing is the newest way for companies to manage, store, and secure data without the expense of additional hardware and software. Some experts question the security of cloud computing while others consider it the wave of the future. Carefully researching a potential cloud computing company before using it is one way to get the benefits of cloud computing with the least security risk.

As technology evolves, so will data encryption techniques. Staying up to date on the newest developments and being willing to adapt business's information storage systems as necessary is the only way to ensure that data will remain secure.

**SEE ALSO** *Biometrics; Internet Security.*

## BIBLIOGRAPHY

Angwin, Julia. "Internet Encryption's Password is 'Slow.'" *Wall Street Journal*. 28 March 2000.

Britt, Phillip. "Encryption Key to Data Security." *Information Today*. November 2005.

Brotby, W. Krag. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Boca Raton, Fla.: CRC Press, 2009.

"Internet Security Gateway Targets Small Network Environments." *Product News Network*. 16 December 2005.

Komiega, Kevin. "Tape Encryption Not a Security Cure-All." *InfoStor*. January 2006.

Korper, Steffano, and Juanita Ellis. *The E-Commerce Book: Building the E-Empire*. 2d ed. San Diego, Calif.: Academic Press, 2001.

MacVittie, Don. "Don't Be the Next Data Debacle—Implement Tape Encryption Now, Before You Find Yourself in the White-hot Spotlight for All the Wrong Reasons." *Network Computing*. 24 November 2005.

National Conference of State Legislatures. "State Security Breach Notification Laws." Available from: http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx. Retrieved February 2, 2010.

National Institute of Standards and Technology. "Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)." Available from:

http://csrc.nist.gov/archive/aes/frn-fips197.pdf. Retrieved February 2, 2010.

"No One-Stop Shopping to Stop Database Pilferages." *eWeek*. 21 December 2005.

Raffo, Dave. "Secure Your Backups: Six Ways to Make Your Data More Secure." *Security Search*. 2 February 2010. Available from: http://searchsecurity.techtarget.com.au/articles/38410-Secure-your-backups-Six-ways-to-make-your-data-more-secure. Retrieved February 2, 2010.

Spethmann, Betsy. "Data Security Mistakes Cost an Average $14 Million." *Promo*. 23 November 2005.

Swann, James. "Preparing for Triple DES Security." *Community Banker*. December 2005.

"You Know These Security Threats—You Hired Them: New Products Are Designed to Stop Threats that Come from the Inside." *Information Week*. 31 October 2005.

***Hillstrom, Northern Lights; Darnay, ECDI updated by Miller, Anaxos***

# DATABASE ADMINISTRATION

Database administration is the maintenance of records of any type—for example, customer lists, vendor histories, or addresses. Database management involves transferring the contents of an electronic filing cabinet to an electronic file using computer software known as a database management system (DBMS). Accoring to *WiseGeek.com*, "As one of the oldest components associated with computers, the database management system, or DBMS, is a computer software program that is designed as the means of managing all databases that are currently installed on a system hard drive or network." The need for database administration now occupies nearly every corner of the business world. This need has led to the development of a multibillion dollar software industry and a thriving database administration consulting niche. Almost every company has records of one type or another to maintain, which means that almost every company is affected by DBMS in some way or another.

Databases can range in size from a few hundred addresses maintained on a user's hard drive to hundreds of terabytes of data maintained on massive servers. One of the benefits of using a database management system is that even if the data is vast and is stored on a remote mainframe, end-users throughout a company can all access the data from their desktop using computer networking technology. With the spread of wireless networking in the twenty-first century, employees can even access databases when not physically linked to the company's network. Reports that in the past had to be requested days or even weeks in advance and created by computer technicians can be generated in minutes by the average user.

The most common type of system is the relational database management system (RDBMS). An RDBMS sorts data into unique fields and allows users to retrieve that data by each field and by linking fields between related records. Relational databases can sort the fielded data any number of ways and generate reports in a matter of minutes. Data can often be output in any form the end-user desires. In addition, a RDBMS can serve as the front-end program that brings data together from several individual databases and produces data tables that combine the information from the various databases. Without an RDBMS, a database is a "flat-file" system—that is, one in which each database is self-contained in a single table. Only very small database systems use this method, and they sacrifice flexibility in the posing of queries and the sorting of data.

Database management technology is a rapidly advancing field, and relational databases are starting to be replaced by more sophisticated database management systems such as object-oriented database management systems (OODBMS) and object-relational database management systems (ORDBMS). The development of these new types of database systems was spurred in large part by the explosion of multimedia files during the first decade of the twenty-first century. During this period, companies realized that they had more than simple records to maintain—they had complicated files with sounds and images; they had brochures, photographs, time-series inputs, and 3-D coordinates—all of which could be more easily maintained if they were organized and stored in a database.

ORDBMS have become more popular because of the growing need to store disparate types of information. An example of the type of data that might be stored in an object-relation system is a human resources file on an employee. In the past, the database record might have only included text information about the employee, such as birth date, address, and starting date. With an object-relational system, the record could also include the employee's photo or voice sample. Or, a company could maintain geospatial information that would allow it to query the database to locate all customers who made more than $50,000 and lived within 10 miles of the company's location.

## SELECTING A SYSTEM FOR A SMALL BUSINESS

Relational and object-oriented databases each have both strengths and weaknesses, and the weaknesses of one type is generally a strength of the other. For small-business owners who are considering purchasing a database management system, experts say that the first thing they need to do is determine what they hope to get out of the system—what type of reports they need, for example. Once the output is known, it is easier to know what type of database is needed,