

Encryption & Cryptography 101

1. History and theory of cryptography

To quote Wikipedia; Encryption is the process of transforming information (referred to as plaintext) using a mathematical algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

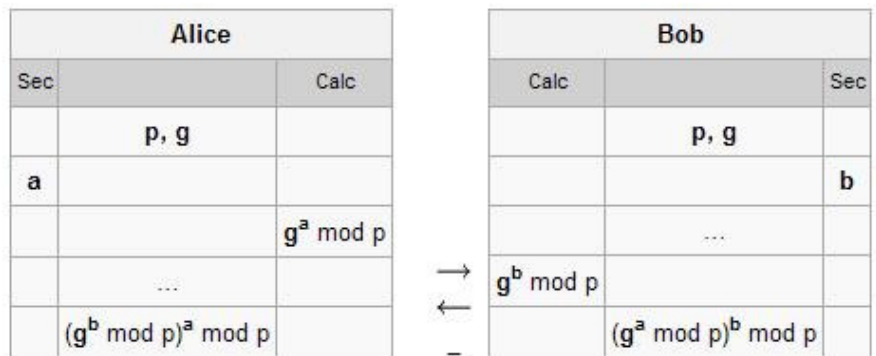
Encryption has been used to protect communications since ancient times, but only organizations and individuals with extraordinary need for confidentiality had bothered to exert the effort required to implement it. Al-Kindi was a pioneer in cryptanalysis and cryptology. He gave the first known recorded explanation of cryptanalysis in approx. 850 AD. Encryption, and successful attacks on it, played a vital role in World War II. Many of the encryption techniques developed then were closely-guarded secrets (Kahn). In the mid-1970s, with the introduction of the U.S. Data Encryption Standard and public key cryptography, strong encryption emerged from the preserve of secretive government agencies into the public domain. Cryptography has since become a renowned and respected scientific field.

2. Encryption in modern technology

Encryption is used in protecting information within many kinds of civilian systems, such as the Internet & e-commerce systems, mobile telephones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

Encryption is used to secure data end-to-end, meaning only the original sender and intended recipient of the encrypted data will be able to access it, and anyone monitoring a computer or router in the route between the end points will not be able to read the data. The machines (for instance, your PC and a server out on the Web somewhere) must first agree on a key. This is done by a special process designed to prevent others from being privy to the key. One such process is called the “Diffie-Hellman key exchange”. Here is a brief example of how a simple key exchange using this method would work:

1. Alice and Bob first agree to use a prime number $p=23$ and base $g=5$.
2. Alice chooses a secret integer $a=6$, then sends Bob $(g^a \bmod p)$
 - o $5^6 \bmod 23 = 8$.
3. Bob chooses a secret integer $b=15$, then sends Alice $(g^b \bmod p)$
 - o $5^{15} \bmod 23 = 19$.
4. Alice computes $(g^b \bmod p)^a \bmod p$
 - o $19^6 \bmod 23 = 2$.
5. Bob computes $(g^a \bmod p)^b \bmod p$
 - o $8^{15} \bmod 23 = 2$.



Both Alice and Bob have arrived at the same value, because g^{ab} and g^{ba} are equal. Note that only a , b and $g^{ab} = g^{ba}$ are kept secret. All the other values are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel. Of course, much larger values of a , b , and p would be needed to make this example secure, since it is easy to try all the possible values of $g^{ab} \bmod 23$ (there will be, at most, 22 such values, even if a and b are large). If p were a prime of at least 300 digits, and a and b were at least 100 digits long, then even the best algorithms known today could not find a given only g , p , and $g^a \bmod p$, even using all of mankind's computing power. For more on this, see <http://en.wikipedia.org/wiki/Diffie-Hellman>.

2. Terminology and common ciphers

In cryptography, a cipher (or cypher) is an algorithm for performing encryption and decryption — a series of well-defined steps that can be followed as a procedure.

The encryption “key” is the password used to encrypt or decrypt (lock or unlock) the secure data. Key size (alternatively key length) is the size of the digits used to create an encrypted text; it is therefore also a measure of the number of possible keys which can be used in a cipher, and the number of keys which must be tested to 'break' the encryption if no faster means is available. In an ideal encryption system, the key length is therefore a measure of how secure the data is, and the effort and time needed to decrypt it by force. The length of a key is therefore critical in determining the susceptibility of a cipher to exhaustive search attacks. Because modern cryptography uses binary keys, the length is usually specified in bits. The time and effort needed to break a cipher of a given key size varies according to the cipher; therefore a 128 bit key size in one system may be deemed equivalent in security to a 1024 bit key size in another. For example, on average, a typical home computer, can crack a 40-bit key in a little under two weeks. However, a 128-bit key could potentially take years, depending on the cipher. More complex keys take longer for the computer to process during encryption and decryption, effectively limiting practical key length.

Though there are many different algorithms available for use today, here is a brief overview of the most popular ones:

DES - DES stands for Data Encryption Standard and is a standardized encryption algorithm developed by the US government in 1976. DES is sometimes referred to as DEA or Data Encryption Algorithm. DES is not considered secure anymore. This is because due to increase in processing power and decrease in hardware costs, it is now possible to implement a successful bruteforce attack on DES.

RSA – RSA, designed at MIT in 1977, was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

MD5 - MD5 is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. Designed in 1991, MD5 is still commonly used but several flaws in its integrity have been found.

SHA1/SHA2 – SHA, short for Secure Hash Algorithm, is under continual development by the NSA, and is believed to be quite secure (Although some theoretical vulnerabilities have been found, executing them in practice would be extremely difficult if not impossible for any hacker).

Blowfish/Twofish - Blowfish is a symmetric block cipher designed in 1993. It was designed by Bruce Schiener as a replacement for DES. The developer has also stated that the algorithm will always remain free for use by anyone. The unique thing about the algorithm is that it has a variable key size ranging from 32 to 448 bits (256 bits for Twofish). Twofish is a more recent development of the algorithm. These are considered among the most secure algorithms today, and there are no known vulnerabilities except massive brute-force cryptanalysis which could take decades (literally).

Some software (such as TrueCrypt, mentioned below) allows you to choose which algorithm to use. I personally use TwoFish when possible, but RSA and SHA are acceptable choices, too.

4. Encryption for home users

There are many software programs available to encrypt your data to keep it private. Even without your knowledge, much of your data is already encrypted. If you allow your browser or email handler program to save your password, it probably stores it encrypted. Anytime you access a secure website (using an https protocol), your traffic is being encrypted end-to-end between your machine and the server.

You can encrypt data on your computer, too. For instance, medical or financial information, a list of your passwords, or anything else you would like to keep private.

Windows comes with a rudimentary encryption tool included in the Zipped (compressed) folder utility. To compress and encrypt a folder, simply right-click the folder and click Send To > Compressed (zipped) Folder. This will create a .zip format file, in the same location as the original folder, with the same name as the folder. Double-click this new zip file to open it. Click File > Add a Password. Enter your password (and again to confirm it) and click OK. Once done, you must enter a password to access this Zip file.

This is a very simple encryption program and is reasonably easy for a hacker to crack – for truly sensitive information, consider dedicated encryption software. There are several excellent free encryption programs, namely and TrueCrypt. Google around for more info.

You can also choose to use encryption for your email. These options differ between email handlers, but generally will be under the Tools > Options / Preferences menu. In Outlook, it's under Tools > Options > Security > Encrypted Email.

When using encrypted email, the recipient must also have encryption-enabled software to be able to decode and read your message.

OpenPGP, provides a free email encryption tool.

5. Storing encrypted data

Encrypted data is, obviously, useless without the key – so make sure you store a copy of the key in a safe place. Where the key is stored is one of the largest potential vulnerabilities in encryption – encrypting the data doesn't serve much purpose if the key to decrypt it is easily found.

Once data is encrypted, it can be stored on your hard drive, a disk (such as a CD or floppy), Flash media (such as a USB flash drive or memory card), or nearly any other data storage medium. If you are encrypting truly sensitive data, consider putting a copy on a disk or flash drive and storing it off-site (a safe deposit box, or relatives house) in case of fire.

This write-up was largely constructed of material from Wikipedia. Wikipedia has a HUGE amount of information about encryption, for those that are interested in learning more.