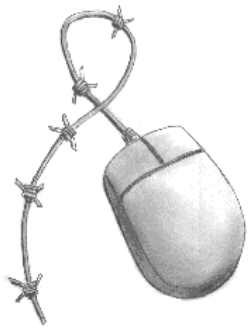
Participating With Safety Briefing no. 4

Using Encryption and Digital Signatures



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

What is encryption?

Encryption is a means of encoding information so that it cannot be decoded and read without a 'key'. Computers have revolutionised encryption because they can encode and decode at high speed and encryption programs now come as 'plug-ins' for a lot of common software. They can also use far more complex systems of encryption that are far harder to break.

Older systems of encryption required the transmission of the encrypted message, but also the key to enable decryption. This is a problem because it requires that you are able to securely send the key to the message recipient before they could receive an encrypted message. This problem was solved in the 1980s with a new system called 'public key encryption'. Public key encryption uses two keys; one key, the public key, is used to encrypt the data, and another, the private key, is used to decrypt it. Public key encryption system is based on highly complex mathematical functions so complex that they cannot be solved without the unique combination of these two keys. It would take an impractical amount of time with even a super computer to find the solution to the mathematical problem that allows decryption. This means that you can make 'public' half of the key available to anyone to encrypt a message with, but the complexity of the encryption system means that the 'private' key cannot be determined from the content of the public key.

There are various public key encryption systems available. But what determines the strength of these systems is the size of the key; the larger the key, the more secure, because the more computer power it requires to break the message. An early system, called DES (Data Encryption Standard), used a 56-bit key. The number of permutations in a binary 56-bit key is 2 raised to the power 56; a total of 72 million billion combinations. The most common standard today is based around the program *Pretty Good Privacy* (PGP). This uses a different set of mathematical algorithms that use key lengths from 128-bits to 2048-bits or higher. This gives a huge number of possible combinations; too big a number to sensibly write on this page as a real number.

The flexibility of computers means that cryptographic systems, like PGP, can be used for a number of different purposes to help secure the data held on, or transmitted by, a computer system:

- Messages being sent over the Internet can be encrypted to prevent anyone other than their intended recipient reading them;
- Messages can be routinely 'signed', using a digital signature based around encryption, so that it can be proven that the source of the message is authentic;
- Information on a computer disk can be encrypted to prevent others having access to it, for example if the computer or disk is stolen, without the required password private key; and
- Encryption systems can be built into communications apparatus, such as telephones or web browsers, to provide encryption of information in real time to prevent interception or eavesdropping of communications.

Even if you don't wish to make your communications secret, some functions enabled by encryption, such as digital signatures, are an immensely useful way of authenticating the source of the message because of the ease with which digital information can be manipulated, copied or forged. Also, though you may not use encryption to send messages, you may wish to encrypt personal information, or information that you have an obligation to protect under the data protection law such as sensitive customer or professional information.

Using Encryption

Encryption used to be a technical operation. Today using encryption systems is a seamless part of using email or web browsers. The most common encryption program, PGP, comes in a variety of versions. Many of them, such as *PGP Free*, are available free of charge over the Internet. Some operating systems, such as Linux, usually include PGP or similar programs as standard.

Most recent PGP systems integrate themselves into your computer system. They ask you what email system you use, and install the appropriate 'plug-ins' to provide encryption functions within your email programs and the operating system's desktop. Some versions of these programs also provide the option to encrypt parts of your hard disk, or to encrypt individual files as part of other programs. Most will also allow you to use a digital signatures to sign files or email messages.

When you install a program such as PGP you are asked to create you 'key pair', the public and private key, for use in encryption. You can actually use more than one key pair, but this may be a problem if you have problems remembering complex passwords required for each key pair. Also some programs, such as email, also have problems accepting more than one secret key for encryption.

A key pair is generated using extremely large prime numbers. These form the basis of the keys. But to add a personal lock on the key pair you are also required to provide a password that you must remember, or the key becomes useless. Passwords should be at least eight or ten characters long. But if you use longer passwords the system is more secure (the words of a song or poem can help you remember a longer passwords more easily).

When you have generated your key pair you can send your public key to your friends, or even post it on a web site if you have one. But you must never disclose your private key, or the password you use with your key pair when decrypting messages. You should also back up your private key to prevent losing it should your computer fail, especially if you use your key to encrypt important files. But you need to back it up in such a way that it can't be easily found (for example, you could print out the private key and hide it in the sleeve of a book - but it is better if you devise your own unique method of physically hiding your keys).

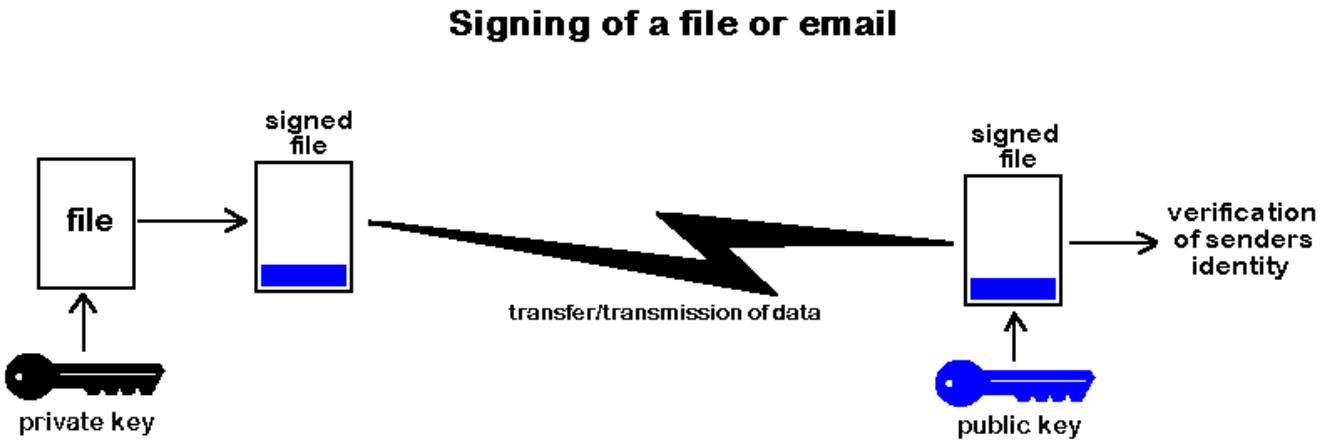
There are various ways in which encryption can aid the use of computers:

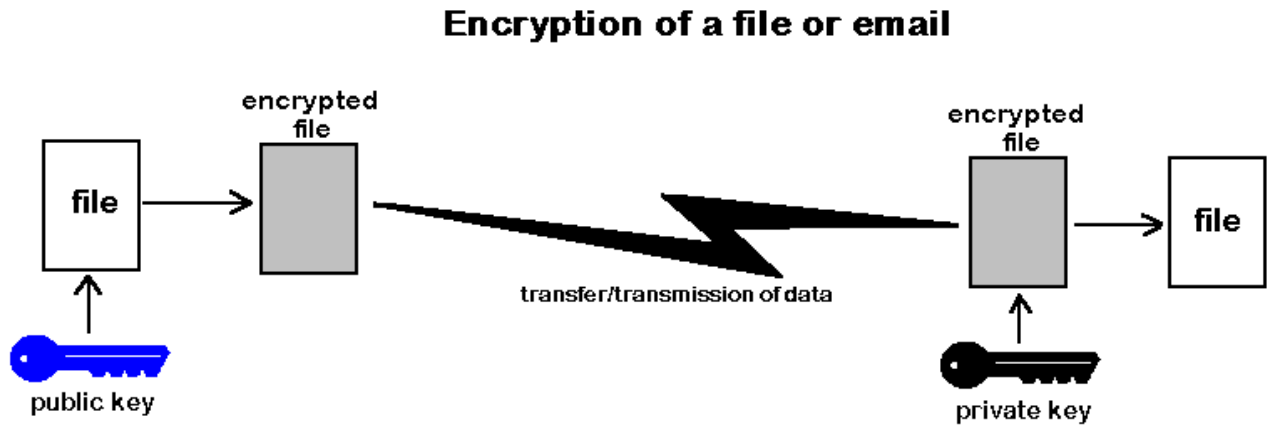
Digital signatures

Even if you don't wish to encrypt data, using digital signatures is a very easy means of preventing your identity from being misused on the Internet. The purpose of digital signatures is to provide an encrypted 'digest' of the message alongside the normal copy of the message. Sending a signed message usually involves the same process as sending an encrypted message, but instead you ask the program only to sign the message. This 'signature' is then appended to the end of the file or email message.

When you receive a signed message you ask the program to verify that the message has not been changed. The program does this by decrypting the message signature and compare the results to the body

of the message. If the result is the same as the plain message the computer gives you the OK.





Secure web services

Web browsers also support encrypted communications under a standard called 'secure sockets'. Secure sockets allows you to give sensitive personal information over the 'Net, such as your credit card number, without people being able to read that data as it travels to its destination. The encrypted secure sockets session is enabled by the web server you are contacting. You can always keep a check on whether or not the session you are using is encrypted because the address you are connected to should be prefixed 'https://' rather than 'http://', and the little padlock graphic in the corner of the screen should be closed rather than open.

Secure sockets does not use a long key - therefore it's not as secure as PGP and other systems that allow you to use longer encryption keys. However, the most likely way that your personal information will be compromised will be through lax security at the computer system you are sending your data to. Therefore when giving your personal information to another system on the 'Net, you should always check first that the system operators have a good reputation for security (a search of the Internet for the name of the company, plus the keywords 'hack', 'crack' or 'security' is a simple, but not foolproof way to do this).

How to tell if your browser is using 'secure sockets'

Encrypting disks

Some encryption systems allow you to encrypt areas of your hard disk, to store files more easily in an encrypted form. These provide a secure way of holding information, particularly information that you may use regularly and need to keep secret such as mailing lists and other personal information.

There is a more detailed outline of disk encryption in the Briefing 2 on *Backing-up Information*

Encryption and security

Encryption can improve security - but only if you take care to protect your secret/private key, and your password. Anyone who does not take steps to secure other areas of their computer, such as setting up a boot password, will not be guaranteed secure encryption.

Setting up hard disk encryption, to keep all data on the computer secure, can be difficult for new computer users. But the effort involved in doing this has to be weighed against the risks to a person's data. For everyday use the signing and encryption of the most sensitive information will be sufficient for most people. But for those who fear that their data on their computer is vulnerable to disclosure, they should install, or get advice on installing, disk encryption.

Encryption with Linux

Linux provides a number of options for using encryption. Like PGP for Windows, on Linux systems you have tools to manage keys, and encrypt/decrypt files. These are usually based around a console program called *gpg* - GNU Privacy Guard - although there are graphical front ends, working with the Gnome and KDE desktops, for gpg. gpg not only uses the public key ciphers used in *PGP Free* and other windows programs. It can also use a number of other ciphers such as triple-DES and Blowfish, and hashing algorithms (used to verify a file's integrity) such as MD5.

Using the graphical front ends to gpg is similar to using *PGP Free*, outlined in the Appendix of this briefing. But using the console version of gpg often provides more flexibility for how you encrypt data. For details about using gpg open an console/terminal window and enter `man gpg`

For example:

```
gpg -r fred --encrypt a_file_name  -encrypt a file with Fred's public key
gpg --decrypt encrypted_file       - decrypt a file
gpg --help                        - display gpg's help information
```

Many other programs can access the functions of gpg to enable the use of encryption as part of their functions. This means that many different programs, such as email programs, can access the private/public keys maintained by each user and use encryption.

When you set up a Linux system it is also possible to instal kernel-level encryption of the hard disk(s) on the computer. This is one of the most secure ways of securing information on a computer. Not only does it provide an extra barrier within the operating system. But if the hard disk is removed from the computer and read from another machine, or if an attempt is made to read the Linux partition from the Windows partition of a dual-boot system, it is still not possible to access information.