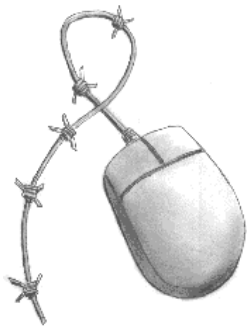
GreenNet CSIR Toolkit Briefing no.3

Encryption and Digital Signatures



How to protect privacy, and your identity, online

Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*, 2002.
http://www.internetrights.org.uk/

What is encryption?

Encryption is a means of encoding information and communications to make them secure, so that they cannot be decoded and read (or *decrypted*) without a special *key*.

Encryption 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 user 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 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.

Digital information can easily be manipulated, copied or forged. Even if you do not 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. Even if you do not use encryption to send messages, you may wish to encrypt personal information, or information that you have an obligation to protect under data protection laws[1], such as sensitive customer or professional information.

Because of the high speed at which they can encode and decode, computers have revolutionised encryption; nowadays they can use complex systems of encryption that are very hard to break.

Prior to the 1980s, systems of encryption meant that the key to enable decryption had to be securely transmitted to a recipient before they could receive an encrypted message. A new system called *public key encryption* was introduced in the 1980s, not only making the process easier, but ensuring that encryption was more secure.

Public key encryption uses two keys called a *key pair*; a public key is used to encrypt the data and a private key, is used to decrypt it. Public key encryption systems are based on mathematical functions that are so complex they cannot be solved without the unique combination of these two keys. It would take an impractical amount of time, even with a super-computer, to find the combination that allows decryption. This means that even though you can make 'public' the key for encrypting a message, the complexity of the

[1]See the GreenNet CSIR Briefing no.2 on *Data Protection*

system means that the 'private' key for decrypting the message 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 it is, because it requires more computer power 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 (2^{56}); so a 56-bit key has a total of 72 million billion combinations. During the 1990s, however, this system was easily cracked by linking computers, or by building specialised computers to decrypt the DES standard.

The most common standard for public key encryption systems today is based around the program *Pretty Good Privacy* (PGP). This employs a different set of mathematical algorithms using key lengths from 512-bits (2^{512}) to 2048-bits (2^{2048}). This of course gives a massive number of possible combinations.

Using Encryption

Encryption used to be a highly 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*[2], are available free of charge over the Internet, or from give-away CD-ROMs in computer magazines. 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. Most will also allow you to use a digital signature to sign messages.

Creating your keys

When you install a program such as PGP you are asked to create your *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 find it difficult to remember the complex passwords required for each key pair.

A key pair is generated using extremely large prime numbers (a prime number is a number that can only be divided by itself or the number one). 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; without this password, the key becomes useless. Passwords should be at least eight or ten characters long. Longer passwords make the system more secure (the words of a song or poem can help you remember 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 cannot be easily

[2]For information on PGP go to http://www.pgpi.com/

found (printing out the private key and hiding it in the sleeve of a book, for example - although it is best if you devise your own unique method of physically hiding your keys).

Using encryption

The same key pair can be used for both message encryption and the creation of digital signatures, as the systems are roughly the same. Usually encryption is used as part of email, but you can also use it for files. Some systems also allow you to keep a library/address book of other people's public keys so that you can more easily encrypt messages to them.

If your encryption program is integrated into your email program, all you have to do is select 'encrypt message' or 'decrypt message' from the relevant menu option. If encryption is not integrated then you will have to type the message using a word processor, encrypt the file containing the message and attach the encrypted file. Some systems are able to encrypt using the computer's clipboard. This means all you have to do is type the message, copy it to the *clipboard* using the 'cut' function, encrypt it, and then paste the encrypted message back into your email program. Decrypting can also be done using cut and paste.

Using digital signatures

The purpose of digital signatures is to provide an encrypted digest of the message alongside a plain text version 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.

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 comparing the results to the body of the message. If the result is the same as the plain message the computer gives you the OK.

It should be noted that ordinary digital signatures are not considered to be legal 'signatures'. The purpose of digital signatures is to verify the authenticity of a message, not to provide absolute proof of identity. In UK law a legal signature must be in manuscript. A digital signature cannot be used to legally conclude a contract via the Internet. Although both parties involved in the deal might agree that a digital signature is sufficient, if the matter you are negotiating were to end in some form of legal action the courts would not recognise the digital signature.

One way of ensuring the legality of self-signed digital signatures is to use a *trusted third party*. *The Electronic Communications Act 2000*[3] enacts into law a licensing system for 'trusted third parties', as part of the government's general package of measures to enable e-commerce. The purpose of a trusted third party is that they verify your identity, first using documentation, such as passports or birth certificates, which proves it. They then issue you with a key-pair for signing digital signatures. Should the validity of the signature ever be questioned it is the third party who will be able to confirm whether the digital signature relates to a valid identity. You usually have to make regular payments to the trusted third party organisation in order to maintain your digital signature with them.

Using encrypted web services

All web browsers 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.

[3]*The Electronic Communications Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm

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 do not use a long key, so it is 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 to which you are sending your data. 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, though not foolproof way to do this).

Encrypting disks

Some encryption systems allow you to encrypt floppy disks, or 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. But if you use a key pair for encrypting files you must always back up the keys, and be sure to remember the password for the key pair. If you do not do this, you will not be able to retrieve the contents of the files.

Whilst disk encryption is a simple way to keep data secure, it is not totally secure. When you edit files on your computer certain portions of the information will be stored in 'swap files' used by your operating system. It is likely that the word processor or database program will also open temporary files to keep a back-up of the edited file. If someone with the available tools wanted to scan your computer for information it is likely that some or all of this information could be available to them because it is stored outside of the encrypted area of the hard disk.

Encryption and the law

Encryption, particularly applications such as digital signature, is a very useful technology. The security of these systems is such that even state security services cannot crack them. In recent years there has been great debate on whether the public should be allowed to use encryption, and if so, under what conditions. There is a concern that criminals and terrorists may use these systems to plan their activities, leaving the state unable to stop them. In response, there is another argument that these people would use encryption anyway, and that people who break the law as part of their activities would have no problems breaking the law in relation to encryption.

Following various proposals this debate culminated with the passing of *The Regulation of Investigatory Powers Act 2000*[4] (the RIP Act). The Act was intended to update the powers of the police and security services to take account of the Internet and new electronic communications services. Section 49 of the Act permits those investigating issues relating to the prevention or detection of crime, national security or the economic interests of the UK to request that a person suspected of holding a relevant encryption key should hand over that key. If the person does not hand over a key in their possession then they can be prosecuted, and on conviction face up to two years in prison, a fine or both. There is a further restriction under section 54 requiring that the person to whom a section 49 notice is given, and anyone else who becomes aware of it at that time, must not disclose that they have been given the notice, if this is a condition of the notice.

[4] *Regulation of Investigatory Powers Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm

There is a clause in the RIP Act which states that a person is not required to hand over a key that has only been used for the generation of digital signatures. But given the Act allows access to all keys in that person's possession the person might have difficult proving they had not used the key for encrypting data.

Under the RIP Act you can defend against a section 49 notice by proving that you no longer have the required encryption key. But as part of this defence you would have to show that you would have been willing to co-operate with the investigation. Under the existing 'right to silence' law, and under the rights against self-incrimination under the *Human Rights Act 1998*, you can refuse to comply with the order if you believe handing over the encryption key would incriminate you. This would still leave you open to prosecution.

The future for encryption

As computer networks become ever more pervasive it is likely that the use of encryption will increase as a basic security measure. Mobile phones began using encryption in the early 1990s, when it became widely known that conversations were regularly monitored by radio scanners. Computer-based communications are similarly likely to use encryption increasingly, as monitoring of networks grows. Rather than user-level encryption, such as the PGP program, however, it is likely that encryption will be built into systems, much like it is with digital mobile phones. As with mobile phones, this raises the issue of who has access to the encryption keys.

The RIP Act applies as much to telecommunications service providers, such as mobile phone companies who provide the encryption keys for your mobile phone, as it does to user-level encryption that may be controlled as part of the registration of your software, or with the registration of your Internet or telephone account. It is likely, then, that if system-level encryption becomes the norm telecommunications or software providers may become the repository for people's encryption keys; effectively a kind of *key escrow*[5] by default.

There have been a number of recent developments in response to the perceived invasion of privacy brought by new Internet monitoring legislation, such as the RIP Act. Many encrypted computer networks, such as FreeNet[6], use peer-to-peer file sharing to store data in a large virtual network; users do not have the keys to the information stored on their part of the system, however, so the RIP Act's section 49 notice cannot be applied.

As governments try to restrict the scope for encryption, it is likely that programmers will come back with new ways of circumventing the controls. Therefore the debate over the use of encryption will continue. There are very positive benefits created by public use of encryption. These have to be weighed against the threats perceived by governments; these threats are often merely notional, with little evidence available on the extent to which encryption is used for illegal purposes.

Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key

[5]Key escrow, where a trusted third party holds your encryption key in much the same way as trusted third parties for digital signatures hold/generate your key pair, was the original response to encryption proposed by governments. It was defeated because of resistance from civil liberties groups in the US and Europe.

[6]For more information see the FreeNet web site - http://freenet.sourceforge.net/

points you will need to find out are:

- What the legal position with regard to the use of any form of encryption is, and if encryption is permitted whether there are any requirements you must fulfil before you use encryption systems;
- Whether the state makes any particular legal provisions for digital signatures held with third parties;
- Whether the automated use of encrypted networks, such as FreeNet, is permitted by national laws.

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need on laws relating to encryption.

The GreenNet Internet Rights Project

GreenNet[7] is the UK member of the Association for Progressive Communications[8] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project[9]. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series[10] that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

[7] GreenNet - http://www.gn.apc.org/
[8] APC - http://www.apc.org/
[9] CSIR Project - http://rights.apc.org/
[10] http://www.internetrights.org.uk/

Free Documentation License:

For more information about the Civil Society Internet Rights Project, or if you have questions about the briefings, contact ir@gn.apc.org.