Walk like an encryption

Preserve your privacy on the net. Nigel Whitfield shows you how PGP encryption works.

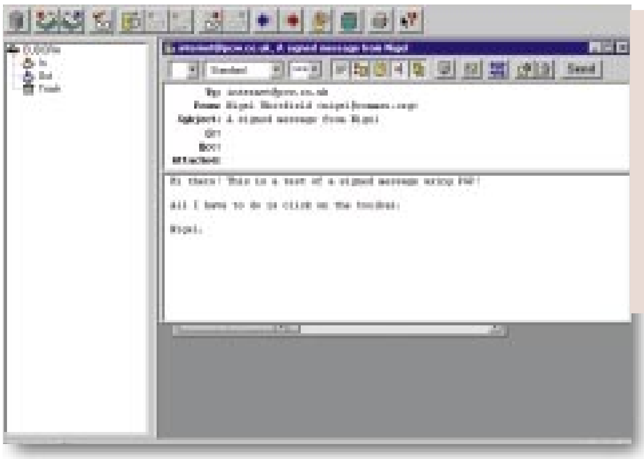
Do you have anything to hide? Of course not, you're innocent. And innocent people never have secrets… or so some would have us believe when it comes to wanting to protect our privacy on the internet. There are plenty of reasons, though, for ordinary people to desire privacy. Survivors of abuse might want to discuss things without fear of being identified, some people may want to share details of their finances with a specific person but not with any 'passerby' who happens to see a message. Others might be planning a surprise, or a change of job.

One of the key tools which can be used to enhance your privacy is encryption; turning information into a scrambled form that needs a password or 'key' to unlock it.

With the usual slightly wonky logic of the lawmakers, though, proposals emanating from the Government had until recently suggested that we would have to put up with a system of 'key escrow'. What that would have meant is that you would have been allowed to use encryption to keep information private but you would have to lodge the encryption key with a trusted agency, who would have been able to hand it over to the police if a court deemed it necessary. It would have been rather like giving a security firm a copy of your house keys in case you might one day be suspected of having committed a crime.

PGP is one of the most widely used encryption programs

Anyway, good sense now appears to have prevailed partly because of the realisation that real criminals would be unlikely to hand over their keys and also due to pressure from businesses which feared that not being able to encrypt data would make e-commerce slow to take off. Even France, which had banned the personal use of encryption, has now relented. So, if the way ahead is clear legally, what does it mean to you?



internet@pcw.co.uk, A signed message from Nigel

To: internet@pcw.co.uk
From: Nigel Whitfield [illegible]
Subject: A signed message from Nigel
Cc:
Bcc:
Attached:

Hi there! This is a test of a signed message using PGP!

All I have to do is click on the toolbar.

Nigel.

◀ Fig 1 PGP plugs into popular email programs like Eudora and Outlook, giving you better security

What can you do with encryption? The first thing to do is visit the PGP International home page at www.pgpi.com, where you'll find links that allow you to download the latest version of Pretty Good Privacy which is one of the most widely-used encryption programs. It uses a system called 'public key cryptography'. For the uninitiated, this means you have two keys: a public key which can be given to everyone, and a private key known only to you.

When a file or message is encrypted with your public key it can only be read with the private key. And, if you send a message to someone else, you can 'sign' it with your private key. Anyone who has the public key can then check that it really was you who sent the message.

Encryption can be much more than just hiding information from prying eyes. You can use it to verify that someone is who they say they are, giving you extra security when you're doing business on the internet.

How do you get started with it? The PGP International web site has freeware programs for Windows and Macintosh users alike, as well as plenty of links to background information for those who want to find out more about the theory behind it.

The best place to start with PGP is the documentation that comes with it. But if you're using Eudora, Outlook, Outlook Express or Exchange, you should find it fairly straightforward as there are plug-ins which allow you to access encryption from within the email program [Fig 1]. The days when using encryption meant writing a message, then running it through a program to produce the encrypted version are, thankfully, long gone.

Step one after you've installed the program is to click the padlock icon that will appear in your Windows task bar and launch PGP Keys to create a new key for yourself. You'll be walked through the process by a wizard and you'll need a passphrase that you'll be able to easily remember without writing it down, and which other people won't be able to guess. Then the Wizard will generate your private and public key pairs for you and send them to a central server where other people will be able to retrieve them if they wish to look you up.

Using the system is simple. With the plug-ins you will see extra buttons appear in your email program providing PGP functions. All you have to do is click on them to provide yourself with a little added security.

For example, the screen in Fig 1 shows Eudora Light. To sign a message, just click the PGP Signature button on the toolbar and choose the Send option. You'll be asked to enter your passphrase and then the message will be signed automatically for you and sent to the recipient. If they know your public key,

Questions & answers

Q On the web, I also have an email account with Yahoo!. How can I view my Yahoo! mail in Outlook Express? I know that there is Accounts on the Tools menu but don't know the server details. Can you help?

a *The simple answer to this is 'No'. There are plenty of free email services available on the web but they don't usually offer the access using POP 3 which mail programs like Outlook need to be able to pick up messages. Instead, they use dedicated programs running on the mail server, so the only way to access your messages is via a browser. Some services will allow POP3 access as a premium option for which you pay an annual subscription. If you want that flexibility it may be worth looking around for a system which offers this option, and remember that many ISPs are now providing web access to your email anyway, making the need for services like Yahoo! Mail and Hotmail less pressing.*

Q I am having to create a web page consisting of a large number of pages, each of which contains text. Is it possible to have a text file or database so that I can bring up a reference from the file which has text linked to it? Then, I would only have to add a reference of some kind to a script on each page to bring up a paragraph of text.

a *Yes, this sort of thing is fairly easy to do. In fact, one of my own web sites consists largely of pages like this which are created on-the-fly and can be accessed by a unique reference number (also see Fig 2). You need to write a script which could be in almost any language, even a batch file on a Windows web server, which takes the name of a file, opens it and then prints it out with any appropriate HTML tags you want. These could include standard page headers and footers to give a consistent look to your site. By linking to pages with a reference such as*

```
<a href="/cgi-bin✓
/getdoc?id=997">Click✓
 here for document✓
 997</a>
```

(Key: ✓ code string continues)

your script will be passed a query string with the variable id set to 997, and can then open the appropriate file. If you want to make things clever, to avoid doing much HTML coding in files yet still link them, consider writing a script that doesn't just print out the text files but also looks for patterns and replaces them. For example, you could search for a string like @REF 997 and replace it with the HTML above, giving you linked pages with the minimum of effort in updating text files. Remember, though, to do this sort of thing you'll need web space that provides you with the ability to run your own scripts, which means you'll most likely have to pay for it.

An alternative is to use a product like Tango or FileMaker 4, which will allow you to use a proper database connected to a web server so you won't need to do any coding of your own, though you may find it hard to track down an ISP that offers services like FileMaker web hosting. There is a partial list at www.filemaker.com.

▼ Fig 2 You can write your own script to access text files and still add buttons and links to pages

▼ Fig 3 Database programs like FileMaker can be hosted for you, so with no programming it makes publishing simple

they'll be able to verify that it really was sent by you.

Managing an encrypted message is just as simple; all you need to do is click the decode button that is added to Eudora and it all works in a similar way with other supported email programs. For those that do not, or if you want to encrypt information elsewhere, you can simply copy and paste it to and from the clipboard.

Unfortunately, there is not the space available here for a complete tutorial on using Pretty Good Privacy but if you are concerned about your privacy on the internet, or if you simply want a way in which you can verify the sender of a message, then it is well worth spending the time getting to grips with the system, even if you only use it in the simplest way. It is still not clear, though, what sort of encryption regulations we will end up with in the UK but in the meantime PGP is free and easy. So, however innocent you are, it can be a useful enhancement to your privacy and security.

PCW internet list

To join other readers of this column in discussions and see at first hand how a mailing list works, send an email to pcw-internet-subscribe@onelist.com or visit www.onelist.com/subscribe.cgi/pcw-internet.

PCW CONTACTS

Nigel Whitfield welcomes your feedback on the Internet column. He can be contacted by post via the PCW editorial office (address p14) or email internet@pcw.co.uk