

Data encryption – Pretty Good Privacy?

Encryption is a way of disguising plain text, so as to hide its substance. Since the days of Julius Caesar, people have been devising ways of encrypting messages so that, if they fall into the wrong hands, the information they contain remains hidden. Until recently, data encryption remained in the hands of the military, and required considerable computational resources both to encrypt and decrypt messages. The growth of email and personal computing has meant that the requirement for encryption has increased, but so has the availability of encryption methods. This requirement will continue to increase with the growth of e-commerce and further commercialisation of the Internet.

Forms of encryption

There are fundamentally two forms of encryption that can be used – conventional, or private key encryption, and public key encryption. ‘Private keys’ should be familiar to anyone who has a PIN number for their bank card, or a password to log on to a computer. Private key encryption relies on the sender and recipient both knowing the key, and ensuring that nobody else does. A difficulty with this method is in determining how the sender can communicate the key securely, particularly when they are in different physical locations. This is why the bank normally sends your PIN number by registered post, separately from the card itself.

Public key encryption is relatively recent, and relies on a ‘key pair’ consisting of a ‘public key’ and a ‘private key’, instead of a single key. Public key encryption solves the problem of distributing keys, as the public key is used only to encrypt the data, and so can be transmitted relatively safely, whilst the private key is used to decrypt the data, and does not need to be known by the sender. The disadvantage of public key encryption is that it is not as secure as private key encryption. ‘Pretty Good Privacy’ (PGP) is a method of encryption that combines features of both private and public key encryption, and whilst not as secure as private key encryption, is still ‘pretty good’!

Pretty Good Privacy

This article is not intended to be a comprehensive essay on encryption, and there are other types of encryption and digital security that are becoming important. It is, however, intended to identify PGP as a secure and freely available method to encrypt email that is also very straightforward and easy to use. PGP software which works with common email software like Outlook or Eudora is now available either free, or for very little cost. Once the software is installed, the user has to think of an easily remembered (but hard to guess) ‘pass phrase’ (e.g. the quick brown fox jumps over the lazy dog), and the software then generates a private key and a public key from the pass phrase, using pseudo-random numbers. The public key is essentially a block of text containing what looks like gibberish text. Persons who want to communicate with each other securely would exchange public keys with each other by sending them in an email, or within a document. The sender uses PGP software (it need not be the same software at both ends as long as it is PGP) to encrypt their message (or document) using the other person’s public key. When the message is received, the recipient enters their pass phrase, which identifies them as the owner of the correct private key, and the software then decrypts the message instantaneously, using a combination of the public key and the private key.

Digital signatures

PGP is also used as a way of creating 'digital signatures', which serve the same purpose as a hand-written signature. It is relatively easy for fraudsters to send email that appears to have been sent by someone other than the actual sender, but a digital signature is nearly impossible to counterfeit. Even if you do not care whether someone else can read your message, you might very well want people to be sure that it came from you. Being able to prove that a message came from you could equally well be important to the recipient, as it means that you would not be able to deny that you had sent a particular message.

Finally, PGP can be used as a secure way of 'wiping' the contents of computer disks, so that files which have been deleted cannot then be retrieved by unauthorised persons. The issue of how to dispose of redundant computer equipment containing sensitive data is one that should also be considered when developing an information security policy.

Commercial alternatives to PGP

The latest versions of Microsoft Outlook have support for encryption and digital signatures built-in. To use these, you will need to purchase a digital certificate from a certifying authority such as [Verisign](#).