

Introduction to encryption

Why do we need security

Before the Internet changed the ways we communicate, cryptography, codes and ciphers were the province of government secrets, of a James Bond world where valuable but dangerous information was scrambled to ensure that it remained 'For your eyes only'. For the rest of us, the seal of an envelope was sufficient proof that our mail had not been intercepted or tampered with.

With the advent of the Internet, we could not be so confident about the privacy or secrecy of our communication. As data – whether it's personal correspondence, company trade secrets, financial data or our grocery shopping list – travels across the Internet, it passes through many computers. Because it is digital data rather than sealed pieces of paper, we have no way of knowing how many people have seen it, copied it, or had access to it.

That is, without the security provided by the advanced cryptography which is now an everyday feature of many Internet services. Cryptographic security systems provide confidentiality, message integrity, authentication, and non-repudiation.

Why is cryptography a good solution

Cryptography is the ideal solution for ensuring privacy and security on the Internet. The computational power of both the host server and the user's PC can be used to generate the codes used to scramble data so that it can only be read by a recipient who has received the correct code or key to decrypt it back into its original form.

By using long numbers and complex mathematical formulae to generate the keys used to secure data, a high level of security can be achieved. The codes are sufficiently secure that even a powerful computer could not guess them – though the science of cryptanalysis is devoted to using computers to crack codes and find weaknesses in cryptographic systems. In fact, the scrutiny of security systems ensures that weaknesses in proposed systems are found quickly, and that systems are based on standards which have undergone long term, detailed analysis and testing are likely to be more secure than proprietary systems which have not been attacked and tested.

Using secret (or symmetric) keys

The simplest forms of computer-based cryptography are secret key systems. Here, the same key is used both to encrypt (scramble) and decrypt (unscramble) the data. Both the sender and the recipient therefore need copies of the same keys. Secret key systems employ shorter key lengths, requiring less processing, making them particularly suitable for handling the encryption of bulk data. With secret key security, the risk of data being read is transferred to the risk of the private key being discovered or exposed. Security efforts must therefore focus around creating an architecture that keeps the key secret and safe, and a method of distributing keys which is also safe and secure.

In practice this means that private key cryptography is used to secure communications between two parties who have already established a trusted relationship, or a separate secure communications channel. Algorithms (mathematical methods) used for private key cryptography include DES (Digital Encryption Standard), triple DES and the new AES or advanced encryption standard. This new algorithm has recently been developed to overcome the problem that computers have now become so powerful that they are potentially able to crack or decode DES keys that are used in real-life settings.

Using public (or asymmetric) keys

Public key cryptography is a more recent innovation – it was first used commercially during the 1970s, and has now become the mainstay of Internet security architectures. Public key systems rely on a related pair of keys, one of which is kept private and used to decrypt data (the private key), and one which is made publicly available and used to encrypt data (the public key). The ability to make the public key widely available makes it much easier to exchange information with people regardless of whether or not you have established a trust relationship. This will be the case for all organisations wanting to use the Web to communicate and transact with hundreds, thousands or even millions of customers or users.

Public key algorithms in common use include RSA, which creates pairs of keys from the prime factors of very large numbers, and elliptic curve cryptography, which uses keys derived from the mathematics of complex curves. A significant consequence of using complex numbers is the strain placed upon the computers that encrypt and decrypt data. This can severely impact the performance of cryptographic systems, such as secure Web servers, and has led to a growing market for cryptographic acceleration products.

Again, public key systems rely on the security of the private key. The level of protection required depends on the level of risk involved. For anyone handling very high value information or large volumes of sensitive data, software protection alone is not enough. In these situations the keys are usually stored in a hardware security module where they are only accessible to authorised users and systems.

Hybrid systems

By combining public and private key cryptosystems, it is possible to overcome some of the disadvantages of each. The main Web security system, Secure Sockets Layer or SSL, uses both secret keys and public keys to establish secure connections between the host Web server and many separate client browsers. Public key pairs are used to set up a secure session, and then data is exchanged using a secret key system. This provides both the security and authentication processes associated with public key systems, and the bulk data encryption capabilities of secret key systems.

PGP, another well known security system used by computer enthusiasts to encrypt their email, is another example of a hybrid system which uses both secret key and public key algorithms.

Digital signatures

One of the most important current uses of cryptography is to identify and authenticate digital information, so that it can be proved that a particular person sent a particular message, and that it had not been tampered with in transit. Public key systems are used to authenticate messages, so that the recipient can be assured that they came from the supposed sender, and the sender cannot deny or repudiate having sent the messages.

Because only the sender has the private key, any message which the public key can decrypt must therefore have been sent by the holder of the private key. That person has therefore, effectively signed it – as long as the private key is safe. While encryption by a private key in a public key system is the equivalent of signing the document, most public key systems add additional features to a signature such as time stamps and other security codes to prove that the document is genuine.

Digital certificates

Digital certificates are special documents that prove that a digital signature is valid. Certificates are issued by 'Trusted Third Parties' or certification authorities, which generate the public and private key for the user, and maintain a directory of issued certificates. When a

message with a certificate is received, the recipient can check with the certification authority that the certificate is genuine and that they can therefore trust the message.

This process requires the establishment of an infrastructure for it to be useful. It must be simple and instantaneous for the recipient to check a certificate's validity with the certification authority. Lists of valid and invalid (revoked) certificates must be secure but accessible to the service's users. If the public key infrastructure is to be useful outside the confines of a single organisation, there needs to be an over-riding system so that certificates can be cross-validated by different systems.

The risk in these systems is concentrated in the central servers which issue and validate certificates. If the underlying private key (the root key) is compromised, none of the certificates, which it has been used to sign, can be trusted. Certification authorities therefore use the strongest possible physical and logical security arrangements to guarantee the security of their own keys.

Managing keys

Thus the risk is transferred from the problem of securing the data to the problem of securing and managing keys. Fortunately, hardware security modules can be used with key management software to provide additional security to protect the keys so that they cannot be stolen. By using a layered security approach you can ensure that there is no single point of failure as there are several systems, physical security devices, software and operating procedures, protecting the keys.

Conclusion

Cryptography is not magic. It does not remove the risk that data can be intercepted, but moves the risk to an area of a system which can be protected more easily. Cryptography only provides security when used as part of a well-designed architecture which has been designed to protect the known areas of risk. The security of private keys is of particular importance, and these are usually stored in special secure hardware modules.

Standards are particularly important in cryptography because they guarantee that a system has been peer-reviewed and tested. All systems have weak points, but those of well-understood public key systems are known and have been worked around. New algorithms such as AES have undergone testing by researchers and industry experts to expose any potential problems. Cryptography is one area where novelty does not necessarily equate to improvement, and users should beware of claims made on behalf of untested technologies.