Explaining Encryption

Introduction

Make any enquiry about computer security, and you will almost immediately fall over the terms cryptography and encryption (and also decryption), but what exactly is meant by this?

The dictionary (in my case the Oxford English), defines cryptography as hidden writing. It has been around for a very long time. The Ancient Egyptians, the Arabs and the Romans developed their own systems.

But what is it used for?

Cryptography is used whenever someone want to send a secret message to someone else, in a situation where anyone might be able to get hold of the message and read it. It was often used by generals to send orders to their armies, or to send messages between lovers. The most famous encryption machine invented was the Enigma, used in the Second World War to send military messages. (Several books and at least one film have featured on Enigma.)

How does it work?

One of the best examples of early cryptography is the Caesar cipher, named after Julius Caesar because he is thought to have used it even if he didn't actually invent it.

It works like this. Take a piece of paper and write along the top edge the alphabet. Take another piece of paper and do the same thing.

You should then have two lines of letters like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Now write your message. SEND MONEY TONIGHT

Move one of your pieces of paper along to the right one or more letters so that they no longer line up. That should look like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

YZABCDEFGHIJKLMNOPQRSTUVWX

Now every time you see a letter of your message in the top line, write down instead the letter on the bottom line.

SEND MONEY TONIGHT becomes

QCLB KMLCW RMLGEFR

What you have done is performed a cryptographic transformation (encrypted) your message. To do it you have used an algorithm (for each letter in your message, move a number of locations on in the alphabet and write that one down instead) and a key, in this case the value 2 because we moved A two places forwards on the bottom line.

All we have to do now is make sure that the person receiving our message knows the key and the algorithm. As long as they know it's the Caesar cipher and the key is 2 they can put their lower line two places to the right, and by taking each letter of the message and writing down the letter immediately above it, they can re-create the original message.

However, if you think about it, the Caesar cipher wasn't all that brilliant. After all, it didn't have many keys. A value of zero meant that you didn't actually encrypt anything, as did 26 because it also moved A under A. An enemy, knowing that was the algorithm, therefore only had to try a relatively small number of keys before finding yours. By just trial and error he could run quickly through all 25 possible keys on just the first word. As soon as he finds a real word the system is broken.

The symmetric cipher

Until we started using computers, these ciphers, with very much better algorithms and much more complex keys were the order of the day. However, the basic approach to this way of creating secret messages has not really changed.

So now you understand the basic method used in any symmetric cipher. Taking our example above, the operation is as follows:

- take your message (plaintext)
- take an algorithm (Caesar)
- take a key (a number between 1 and 25)
- transform the message according to the algorithm using the key
- now you have an encrypted message (ciphertext)

The recipient then:

- takes the encrypted message (ciphertext)
- takes the algorithm (Caesar)
- takes the same key (the same number as chosen above)
- transforms the encrypted message according to the algorithm using the key
- now they have the original message back (plaintext)

This is called a symmetric cipher because you use the same algorithm and the same key to carry out both encryption and decryption. There are other types of cipher systems but they are covered in other white papers.

Strength of encryption

The quality of the algorithm and key combination (as we saw with the Caesar cipher, making the key bigger on its own did not actually make the encryption any stronger at all) were the factors that made the strength of the system. However, until there was some automation you could not use really complex methods because it simply took too long to encrypt and decrypt messages.

Thanks to computers we are now able to do these things much faster and better than Caesar, or, indeed Enigma. There are many algorithms available far harder to break than the Caesar cipher. They have strange names, such as Rijndahl, Blowfish, RC2, RC4, Triple DES, CAST. They have key sizes that are enormous by comparison to our Caesar cipher.

Of course, just as computers are able to operate such powerful algorithms, computers can be harnessed to break them. The algorithm DES (Data Encryption Standard) in use for many years to protect banking transactions was considered very strong until the University of Cambridge published a design for a custom machine to break the cipher in minutes, for a manufacturing cost of under $1 million. Fortunately, the algorithms mentioned above are still considered effective.

Further Reading

There are many books available describing cryptography, either as a history or as a mathematical system or as a guide to use and implementation. The following is a very short list of books appealing to each group.

The Code Book: Simon Singh. ISBN 0-385-49531-5. Doubleday, 1999.

Cryptology: Albrecht Beutelspacher. Mathematical Association of America,1994.

The Crypto controversy: Bert-Jaap Koops. Kluwer, 1998.

Seizing the Enigma: David Kahn. Arrow, 1996.

Cryptography and E-commerce: Jon C. Graff. Wiley, 2000.

Applied cryptography: Protocols, algorithms, and source code in C 2nd edition: Bruce Schneier. Wiley,1995.