



Introduction to Encryption

Introduction

The Shorter Oxford English Dictionary lists the 5th meaning of the word cipher as, "A secret manner of writing by any of various methods, intelligible only to those possessing the key (1528)."

Encryption, the use of ciphers, is not new. Far from it. It has been with us for a very long time.

I used to say that encryption was traditionally for the four P's. Princes, Popes, Purveyors and Paramours, since they were the people who had secrets and needed to keep them.

Julius Caesar used encryption to send his instructions to his armies, and the Caesar cipher, one of the earliest recorded ciphers, is named after him.

But the honours for the groundwork to our modern use of cryptography should probably go to the Turkish community for their application of mathematical algorithms (formulae to convert by a mathematical process between ordinary information, called plaintext by the cryptography community, and cipher text, the encrypted information that is impossible to understand without the key) to automate and make routine the business of encrypting and decrypting information.

When Mary, Queen of Scots sent her encrypted messages to raise a revolt against Elizabeth I, the process was very manual, and slow. It took Elizabeth's code breaker some weeks to figure out what the secret information meant. By comparison, by the time the Germans introduced their Enigma machines (and subsequently the British their computers at Bletchley Park to decrypt them) the process was becoming fully automated, and down to days or just hours.

Today, every PC is equipped with enough powerful mathematically proven encryption engines to process information at many megabytes per minute – something beyond the wildest dreams of our ancestors, and little realised by most PC users.

Why use encryption?

Most often, to keep secrets. Everyone has a need to keep some things secret. The operating system has secrets it needs to keep away from users, users want their credit card details kept secret and away from hackers, everyone wants their financial and health affairs secret, and, sadly, it appears that even today people still need to keep their religious persuasions secret.

It is unfortunate, but the need to keep a wide variety of information secret also means that people can also use encryption to keep secret things that society has decided are unlawful, such as the plans to rob a bank.

Encryption technologies also have other valuable capabilities. Any attempt to falsify the content of an encrypted message will cause failure during decryption. This was not the case with the Caesar cipher, where each letter was transformed separately from every other letter, so altering one or more letters might well not be noticed by the recipient. But modern mathematical systems are such that it is highly unlikely that anyone could change even one element (usually called a bit or binary digit) in an encrypted file without causing everything from that point onwards to be turned into gibberish.

Further, encryption can be used to detect if information has been changed or corrupted, whether it is actually encrypted or not. And this can be very valuable if you cannot encrypt the information itself but need to be able to show that it is correct. This technique is commonly used to verify computer applications software that has been downloaded from the web.

So encryption is used for keeping secrets, preventing information falsification and verifying that the information received is the information that was sent.



Where is encryption commonly used?

The commonest use of encryption probably occurs in Internet transactions using a technology called Secure Sockets Layer (SSL). It is in use whenever you see a little padlock appear in the bottom right hand corner of your Internet browser. What SSL means is that information passing between two points in a network is encrypted so that nobody else can read it or readily change it. Unfortunately the way SSL is usually implemented has created a few problems:

- neither point on the network knows exactly who the other point is;
- there is no proof at all as to where the information actually came from;
- the information is immediately decrypted on arrival, so you cannot possibly rely on SSL alone to keep the information secret because that is something it was never designed to do (beware of snake-oil merchants who appear to say that if your information is protected by SSL it is totally secure, its only when passing between those two undefined points, and never at any other time).

The second and third commonest uses (and it's now anyone's guess as to which is the winner) are secure email/messaging and [digital rights management \(DRM\)](#).

The massive number of financial transactions passing over public and private networks are all protected using encryption. So is much healthcare information, all credit card information, and increasingly, aerospace and administration (government).

Add to that the increasing number of occasions when encrypted information is attached to emails covering everything from communications between corporate management and their lawyers to information for the R&D department and you have a really huge amount of encrypted information.

DRM, digital rights management systems, can only be implemented if information is encrypted. And the reason is very simple. No encryption and there is no way of applying management. DRM controls only get implemented where encryption is used to ensure that only the authorized can get in, and their rights are limited by the interpretation of the license by the application carrying out the decryption.

Is encryption a perfect solution?

Like any technology, it is all down to implementation. Often people tell you its all down to key length. But you also have to know the algorithm that is being used. If you implemented the Caesar cipher that we mentioned earlier on, you can claim any key length you like, but the algorithm works by switching so many letters along the alphabet from the letter you selected to the one that is used in the cipher. So regardless of what you think, the maximum effective key length is 25, and breaking it does not require the brain of a planet.

You need to know what algorithm and key length have actually been used. It would help if you knew that the implementation is actually good and effective. Unfortunately, at the moment you don't have any external test systems that will tell you if the supplier has actually implemented the algorithm they claim with the key they claim because it is very difficult to inspect an encrypted file and say if the implementation is any good or not.

Avoid any algorithm using a key length of less than 64 bits, and be aware that 64 bit keys are likely to have a limited life because the power of desktop computers is increasing so rapidly that a technique called 'brute force attack' where you simply try every possible key until you find the one that works is now entirely feasible. Not so long ago the NSA retired an algorithm called DES (data encryption standard, originally developed by IBM and called Lucifer) which had an effective key length of 56 bits, because designs had been published to allow it to be broken in minutes, and things have moved along since then.



In any event, a 128 bit key is the minimum you should be considering. Here, standards and other opinions can help you make an informed decision.

Standards and algorithms

So what should you be looking for? Well in the game of encryption it is best to play safe. Avoid anyone claiming to have some new, powerful and unbreakable system. Peter Guttman, the well known New Zealand cryptologist maintains a formidable list of the companies selling snake-oil crypto at <http://www.cs.auckland.ac.nz/~pgut001/links/products.html>. It's well worth a read, especially for the unwary.

Fortunately there are international standards bodies with the competence to document and publish standards for encryption algorithms. The principal group is ISO/IEC JTC1/SC27 (a bit of a mouthful but they are the sub-committee responsible for standards in security methods and techniques) and they create standards for algorithms for different purposes. But you have to remember that they create standards for use in many different applications, so you need to refine your search a little more.

Look for people implementing algorithms endorsed by organizations such as the NSA (American security agency) or GCHQ (the UK security agency). At least they know what they are doing.

Their current recommendation is an algorithm called AES (advanced encryption standard) with a key length of either 128 or 256 bits. AES has been specified as suitable for U.S. Government organizations to protect sensitive (unclassified) information (see http://www.nist.gov/public_affairs/releases/aesq&a.htm). As an alternative, triple DES (also known as 3DES) is probably fine.