# Data Encryption

## What is Encryption?

Encryption means to scramble data in such a way that only someone with the secret code or key can read it.

## Why is it important?

Today, encryption is far more sophisticated, but it serves the same purpose - to pass a secret message from one place to another without anyone else being able to read it.

Encryption is extremely important for e-commerce as it allows confidential information such as your credit card details to be sent safely to the online shop you are visiting.

Web browsers are able to encrypt your purchase details using an encryption method called 'SSL' (Secure Socket Layer). You know this is switched on when a small padlock appears in the bottom right of the browser. SSL gets switched on when you visit a 'secure server' that has an address that starts with HTTPS:// (note the 'S').

## How does it work?

Encryption works by scrambling the original message with a very large digital number (key). This is done using advanced mathematics. Commercial-level encryption uses 128 bit key that is very, very hard to crack. The computer receiving the message knows the digital key and so is able to work out the original message.

## Problems with encryption

**There are three problems;**

a) It is slower than normal browsing. It takes a while for the browser to do the maths required to scramble the message and another delay on the server that has to unscramble the data.

b) Online shops have to have a digital certificate that contains part of the key. This is not free and has to be supplied by a 'certificate authority'.

c) It can be a complicated business running a secure server, so very often, ordinary online shops will hire a specialist 'Payment Gateway' such as WorldPay or Paypal to handle payments for them.

## Symmetric vs Asymmetric encryption

### Symmetric Encryption

Symmetric encryption's job is to take readable data, scramble it to make it unreadable (protecting it from prying eyes while it's being stored on a disk or transmitted over a network), then unscramble it again when it's needed. It's generally fast, and there are lots of good encryption methods to choose from. The most important thing to remember about symmetric encryption is that both sides—the encrypter, and the decrypter—need access to the same key.

### Asymmetric Encryption

Asymmetric encryption also takes readable data, scrambles it, and unscrambles it again at the other end, but a different key is used for each end. Encrypters use a public key to scramble the data, and decrypters use the matching private (secret) key on the other end to unscramble it again.

The public key means that it can and should be published. (This is why asymmetric encryption is also often referred to as public-key encryption), but the private key must be kept private, protected much like the key for symmetric encryption.