3.5.3 Encryption protocols

SSL stands for Secure Sockets Layer. It provides a secure connection between internet browsers and websites, allowing you to transmit private data online. SSL has become part of an overall security protocol known as **Transport Layer Security** (TLS).

In your browser, you can tell when you are using a secure protocol, such as TLS, in a couple of ways. You will notice that the “http” in the address line is replaces with “https”, and you should see a small padlock as well when you are accessing sensitive information, such as an online bank account, any site where you have to enter credit card number, sites like PayPal or Google Checkout, etc… . You’ll know that your session is secure if you see a “https” and a padlock symbol.

If these websites did not make arrangements for this kind of security, then there will be a good chance that your personal information will be floating around on the internet for the public or even hackers to use for bad purposes.

TLS and its predecessor SSL make significant use of certificate authorities. Once your browser requests a secure page and adds the “s” onto the “http” the browser sends out the public key and the certificate, checking three things:

1) The certificate comes from a trusted party
2) The certificate is valid
3) The certificate has a relationship with the site from which it is coming.

So what is SSL used for? The SSL protocol is used by millions of e-Business providers to protect their customers, ensuring their online transactions remain confidential. A web page should use encryption expected to submit confidential data, including credit card details, passwords or any personal information. All web browsers have the ability to interact with secured sites so long as the site's certificate is from a recognized certificate authority.

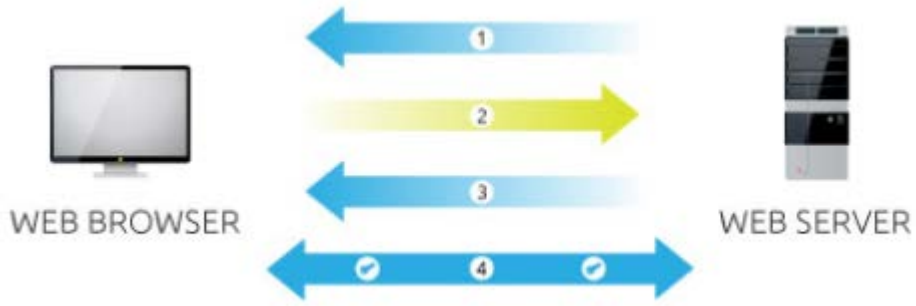
3.5.3 Encryption protocols

Why do you need SSL?

The internet has spawned new global opportunities for enterprises conducting online commerce. However, it has also attracted fraudsters and cyber criminals who are ready to exploit any opportunity to steal consumer bank account numbers and card details. Unless the connection between a client (e.g. internet browser) and a webserver is encrypted, then any moderately skilled hacker can easily intercept and read the traffic.

How SSL uses both Asymmetric and Symmetric Encryption

In SSL communications, the server's SSL Certificate contains an asymmetric public and private key pair. The session key that the server and the browser create during the SSL handshake is symmetric. This is explained further in the diagram below.



1. **Server** sends a copy of its asymmetric public key.
2. **Browser** creates a symmetric session key and encrypts it with the server's asymmetric public key.
3. **Server** decrypts the asymmetric public key with its asymmetric private key to get the symmetric session key.
4. **Server** and **Browser** now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that session. If the browser was to connect to the same server the next day, a new session key would be created.