How SSL Works

What I will cover?

Why SSL and certificates exist?

1. Encrpytion

Hiding what is sent from one computer to another.

2. Identification

Making sure the computer you are speaking to is the one you can trust.

Encryption

Why?

Imagine, you want to send your credit card details to a server over the internet. Without SSL this information can easily be grabbed by a third server(someone untrusted). So, if you do not use SSL, any computer on any of the networks between you and the server, can grab the data that you are sending or receiving.

SSL puts a barrier around this data, so that when another user looks at it, it will just see garbage.

How?

1. **Computers agree on how to encrypt**

CLIENT

SERVER

Key	**Cipher**	**Hash**
RSA	RC4	HMAC-MD5
Diffie Helman	Triple DES	HMAC-SHA
DSA	AES	

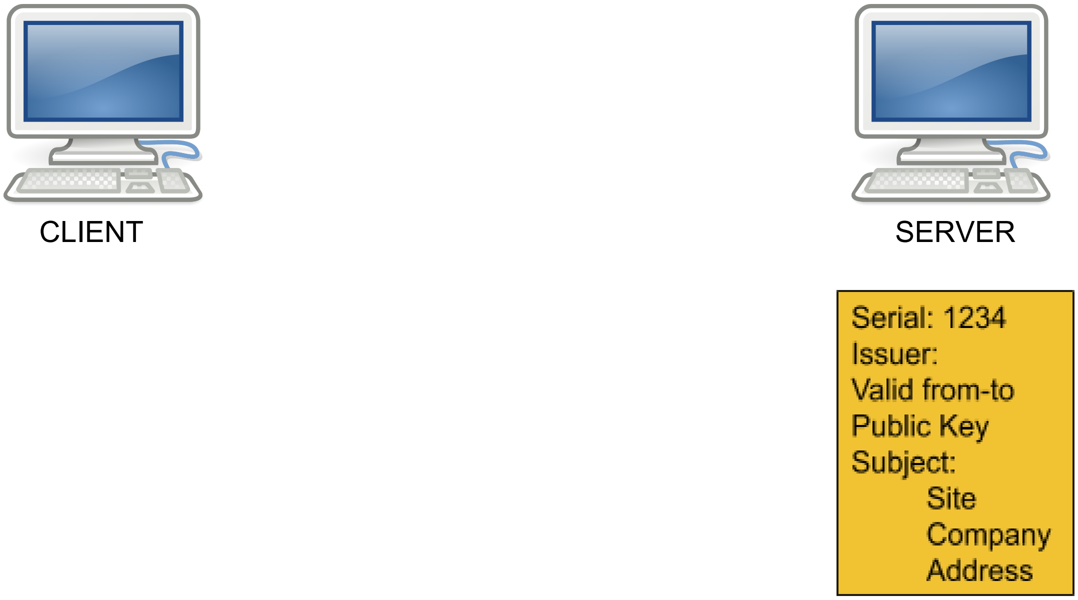
Key	**Cipher**	**Hash**
RSA	RC4	HMAC-MD5
Diffie Helman	Triple DES	HMAC-SHA
DSA	AES	

Version	3.3
Random Number	18923….

The client sends a HELLO message along with a few other information. It sends the kind of Key generation algorithm, key encryption algorithm and message authentication it can use. (To understand what these are, see other notes.) It sends the version number of SSL and a random number which is used to calculate the master secret. The master secret is then used to calculate the encryption keys.

The server receives the HELLO message from the client and sends the HELLO message back along with the selected choices from the Key generation algorithm, key encryption algorithm and message authentication that they should use for the communication.

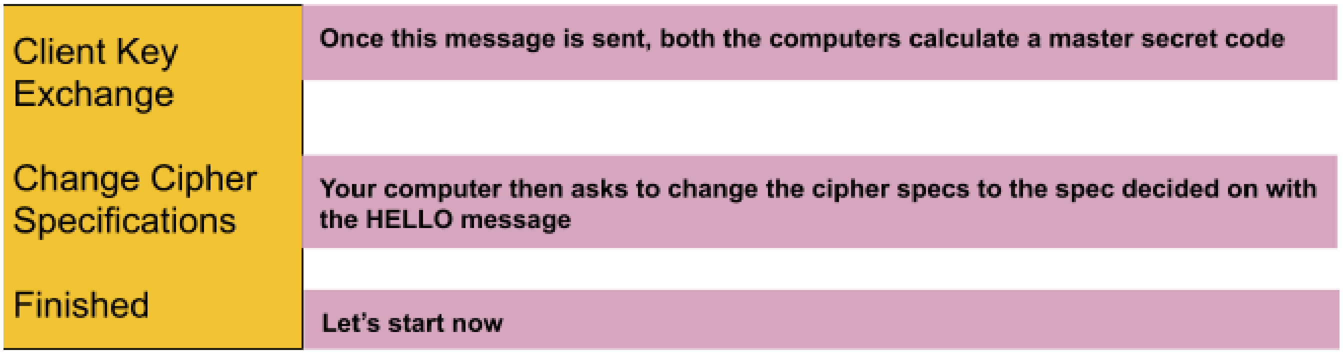
2. **Server sends certificate**



Serial: 1234
Issuer:
Valid from-to
Public Key
Subject:
Site
Company
Address

The server now sends a certificate containing the above shown information. It contains the serial number of the certificate. The issuer's name, the valid from-to date and the public key of the certificate. It also contains the information of the subject for which the certificate was generated.

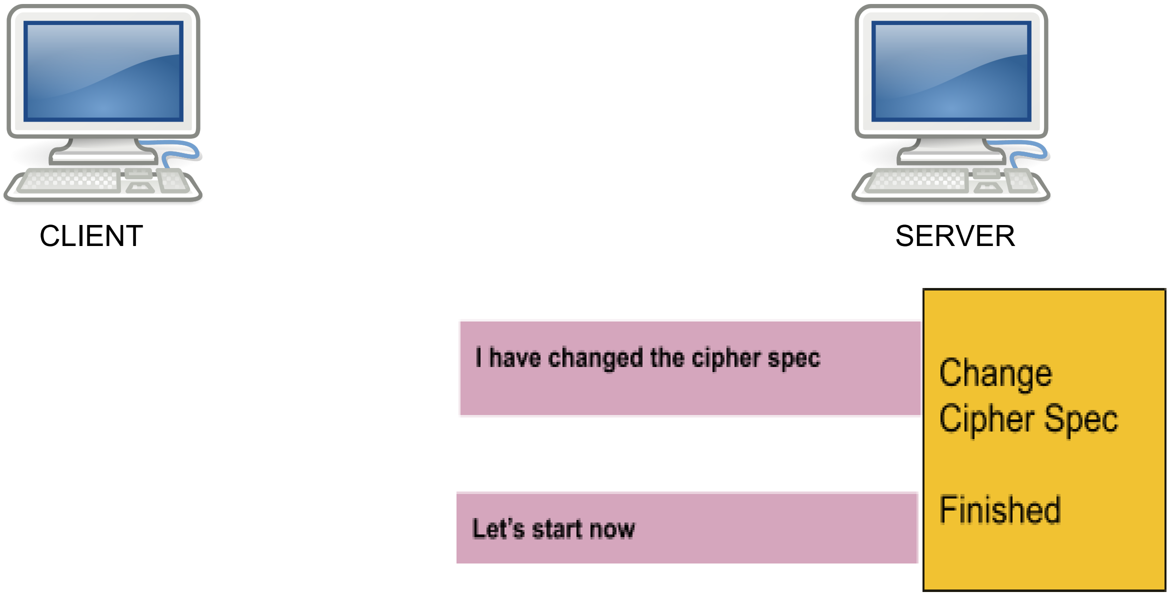
3. **Your computer starts encrypting**



Client Key Exchange	Once this message is sent, both the computers calculate a master secret code
Change Cipher Specifications	Your computer then asks to change the cipher specs to the spec decided on with the HELLO message
Finished	Let's start now

Your computer now wants to indicate to the server that it is ready to communicate and it does so with the help of 3 messages as shown above.

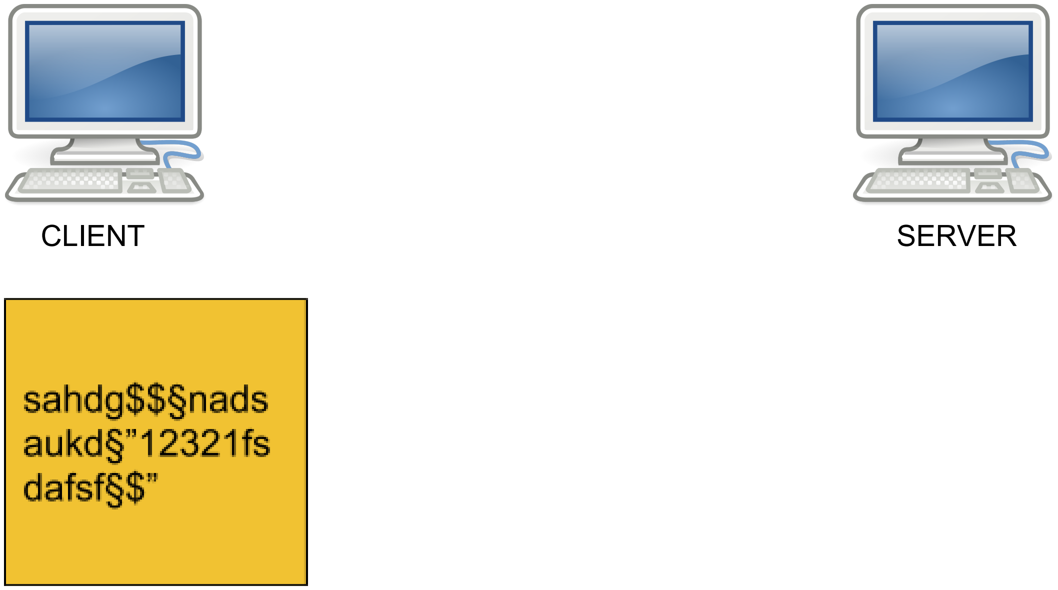
4. **Server says start encrypting**



I have changed the cipher spec	Change Cipher Spec
Let's start now	Finished

The server informs the client that it has changed the cipher spec and that they should start the communication now. NOTE: The finished message that server sends is encrypted now!

5. **All messages are now encrypted**



Now, all your messages that are sent to the server would be garbage to anyone trying to eavesdrop on your conversation!

Identification

Even if your computer has a SSL certificate, it does not necessarily mean the computer that you are talking to is the one you think it is.

Who to Trust?

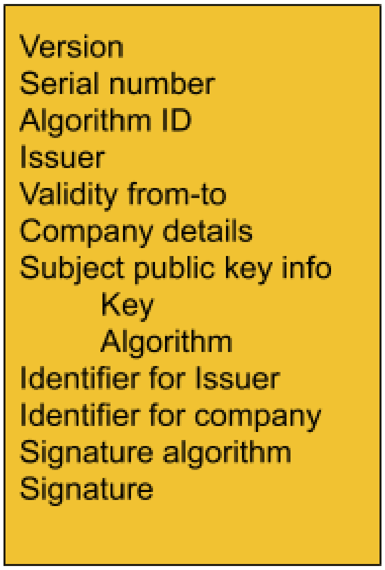
1. **Company asks CA for a certificate**

For this step, the company sends a whole lot of information about itself like:

- The web server
- Company location
- What company it is

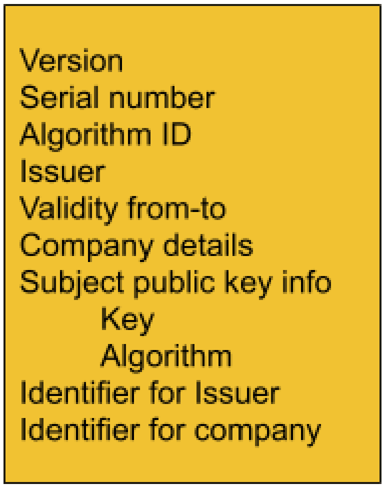
2. **CA verifies the company, generates a certificate and signs it**

The Certificate Authority then checks the correctness and authenticity of this information.



Version
Serial number
Algorithm ID
Issuer
Validity from-to
Company details
Subject public key info
    Key
    Algorithm
Identifier for Issuer
Identifier for company
Signature algorithm
Signature

The certificate generated contains the above presented information.



Version
Serial number
Algorithm ID
Issuer
Validity from-to
Company details
Subject public key info
    Key
    Algorithm
Identifier for Issuer
Identifier for company

The Signature is created by condensing all the above presented information into a number(through hashing). Now, this number is encrypted with a private key. Therefore, anyone that holds the public key can verify if it is correct. (Asymmetric encryption)

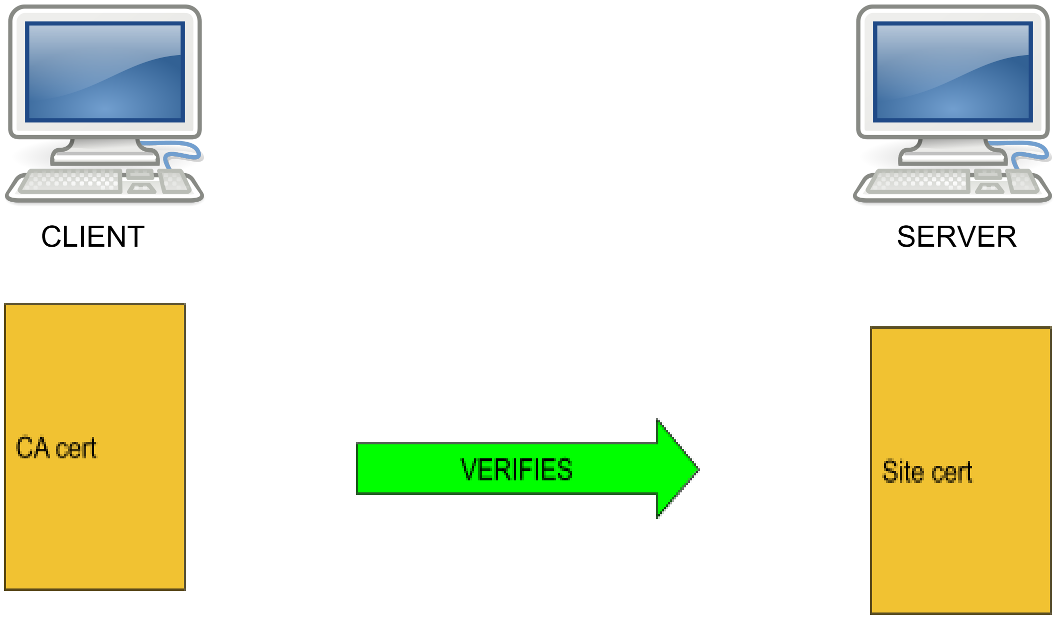
3. **Company installs certificate on server**

The certificate is provided to the company. The company is running a web server on which they will install this certificate. This certificate will now be used for the handshake process for Encryption as discussed above.

4. Browsers are issued with Root certificates

Now you are trying to get information on your browser from a site with SSL. How does the browser know whether to alert you or not? The browser contains a box of certificates issued by all CA's of the world. That enables it to check the authenticity of the certificate of the server.

5. Browser trusts correctly signed certificates



Your browser comes shipped with all the CA's certificates that contain the public key. When the site is loaded, the browser received a site certificate that it checks using the public key from the CA certificate.

Browser only alerts you if the certificate is not signed!!