SSL protocol

- Secure socket layer (SSL) is a protocol that provides security of data sent between applications over the Internet.
- SSL is normally implemented on top of TCP in order to encrypt Application Layer protocols such as HTTP, FTP, SMTP and IMAP.
- One common use of SSL is to secure Web HTTP communication between a browser and a webserver, by creating an encrypted link between the two. When you request a URL, the server sends your browser a copy of its SSL certificate. The browser verifies that it's authentic, and the server then sends back a signed acknowledgment. Upon arrival, both start an SSL encrypted session and can share data safely.

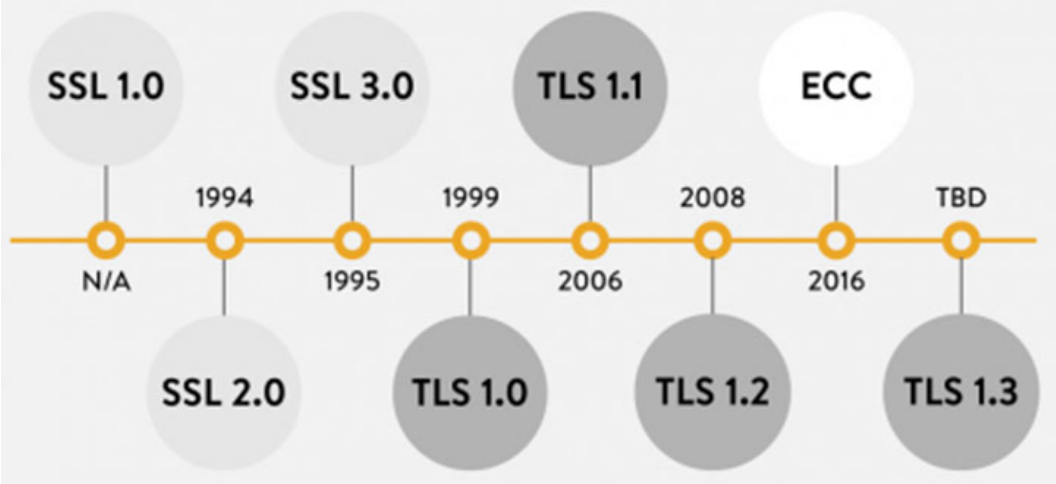
SSL protocol cont…

- SSL always authenticates the server. The server presents a certificate, signed by the private key of a certificate authority, and your browser verifies it against the authorities public key.
- This is all relatively easy and well supported by most web servers.
- However, the SSL can also authenticate the client if desired. This means the client has to have certificate. In this case, you configure your browser to present a client certificate when it connects to a remote server, and the remote server will authenticate the certificate against some authority.

SSL protocol cont…

- SSL last version was 3.0, and TLS succeeds SSL, and become the new standard.
- But still some components of the protocols have the name SSL, like SSL certificate for example, so when you see the name SSL it most probably means the new TLS, because SSL is rarely used any more.
- TLS can be viewed as SSL v3.1.

Elliptic Curve Cryptography (ECC)
Both ECC and RSA are protocols used for encryption in SSL/TLS certificate.
TBD means To be done



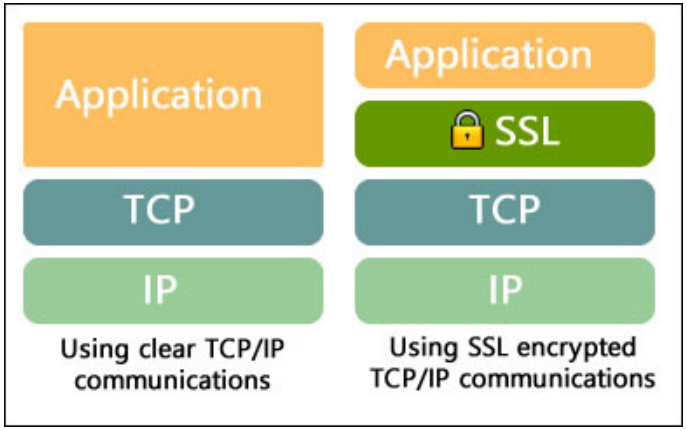
SSL protocol cont…

- Typically, TLS support is part of the OS based on one of the following products, which come with a BSD, GPL, or commercial license:
  - OpenSSL
  - GnuTLS
  - CyaSSL
  - PolarSSL

SSL protocol cont…

- SSL works on top of TCP/IP.
- SSL exists between the application layer and the transport layer.

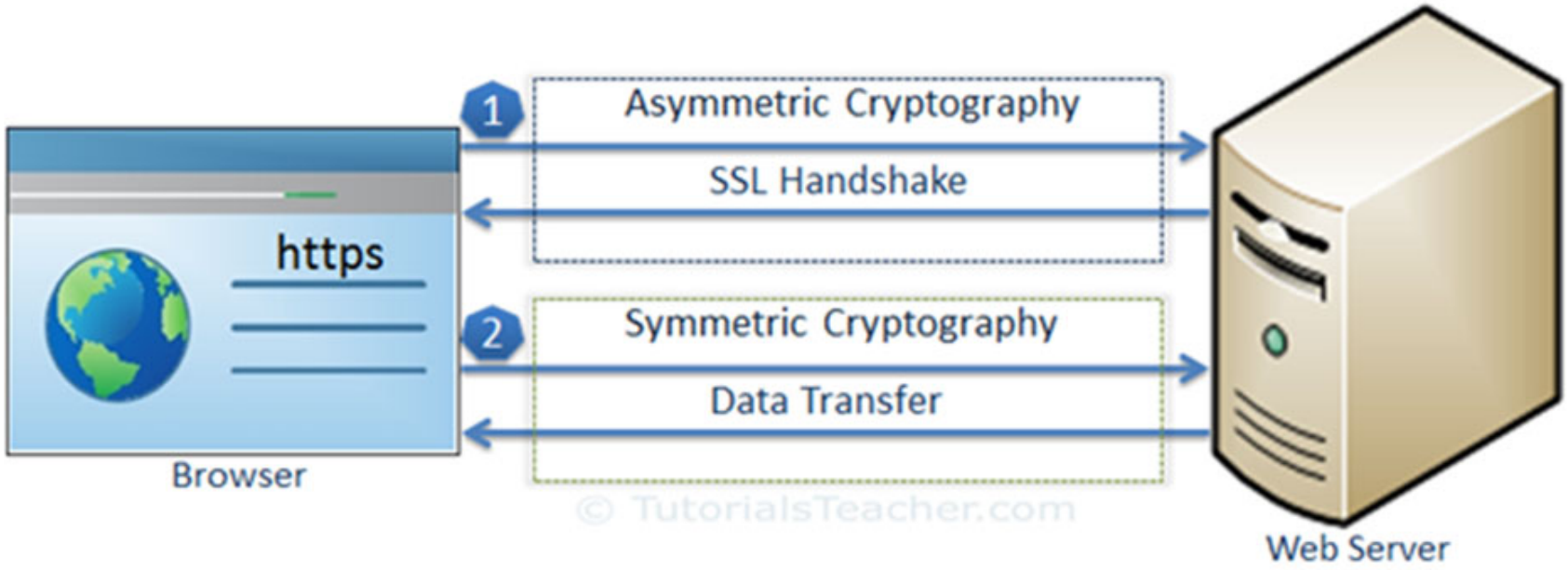
```
> Frame 72: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
> Ethernet II, Src: 00:12:3f:97:92:01, Dst: 00:22:19:22:54:9e
> Internet Protocol Version 4, Src: 169.254.255.66, Dst: 169.254.100.98
> Transmission Control Protocol, Src Port: 52926, Dst Port: 443, Seq: 1633, Ack: 947, Len: 181
v Secure Sockets Layer
  v TLSv1 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 176
      Encrypted Application Data: 96310e30353538bce9edc2c2691748e9d914999c4d83bb94...
```



SSL protocol cont…

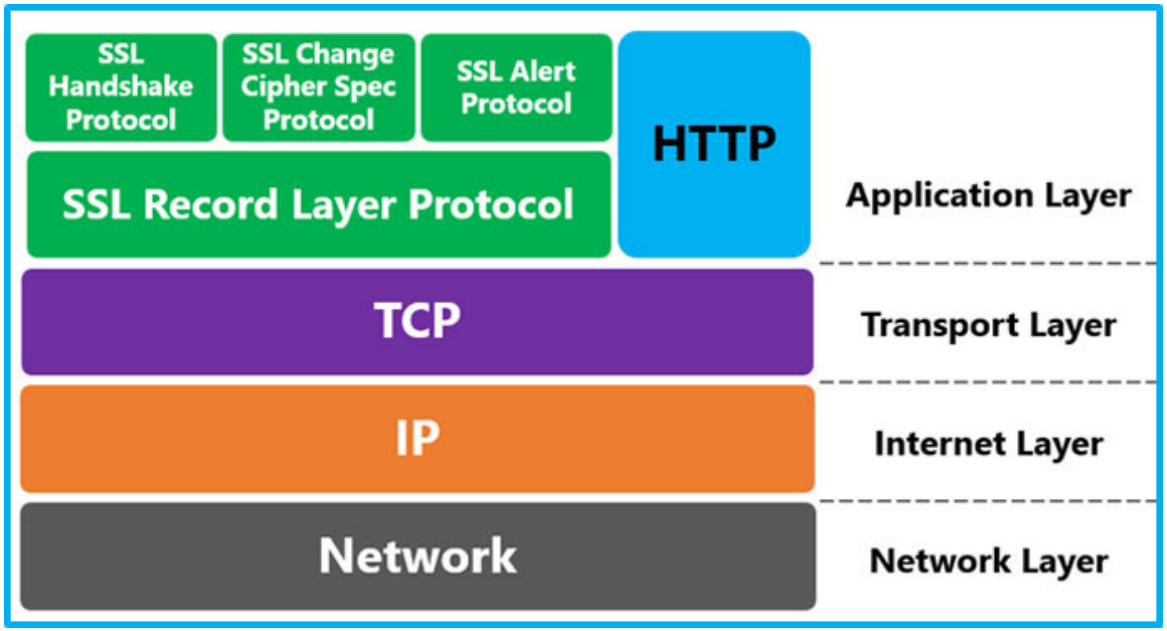
- SSL fundamentally works with the following concepts:
  - Asymmetric Cryptography
  - Symmetric Cryptography
  - CA

SSL protocol cont…

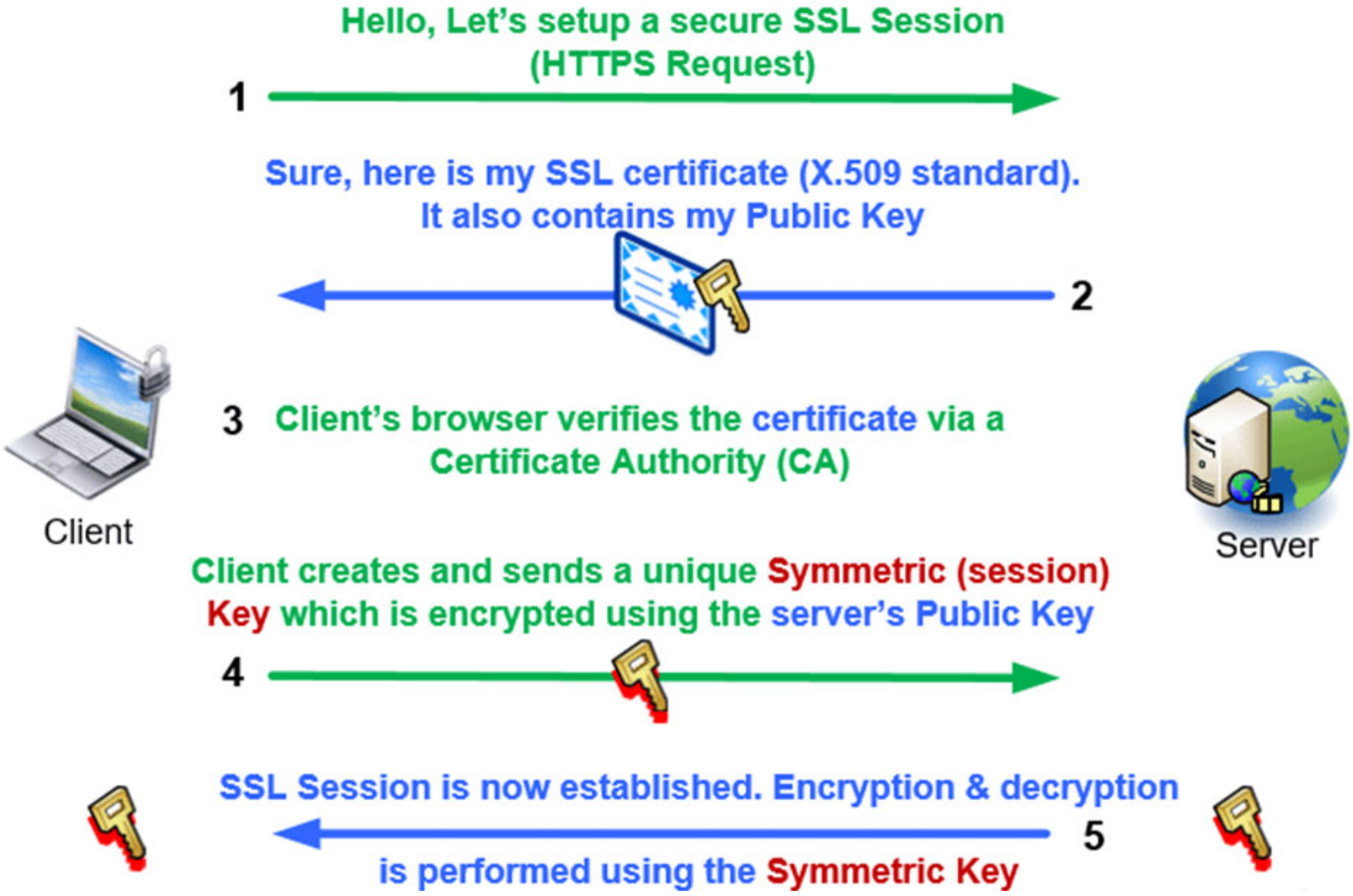


SSL protocol cont…

- Technically, TLS/SSL consists of two parts:
  - TLS handshake layer: manages which cipher (the type of encryption algorithm), which authentication (using a certificate specific to your domain name and organization), and the key exchange (based on the public-private key pair from the certificate) will be used. The handshake process is performed only once to establish a secure network connection (SSL/TLS tunnel) for both parties (client and server).
  - TLS record layer: gets data from the application layer, encrypts it, fragments it to an appropriate size (as determined by the cipher), and sends it to the transport layer.



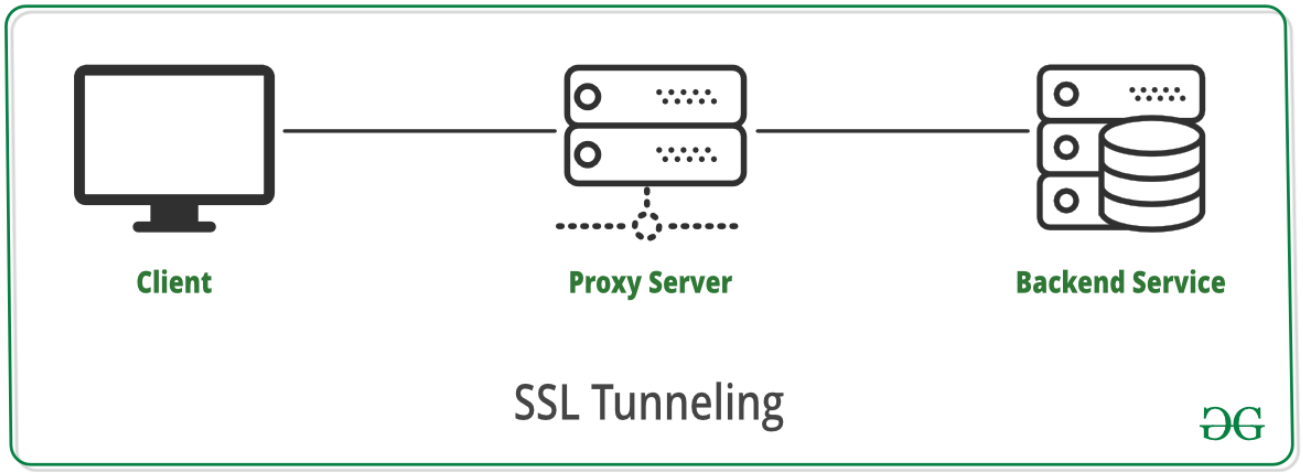
SSL/TLS handshake process cont…



SSL tunneling through a Proxy Server

- Stunnel can be used to provide secure encrypted connections for clients or servers that do not support SSL. A SSL tunnel can route traffic between an unsecured client and an unsecured server over the hostile internet.

- SSL Tunneling involves a client that requires an SSL connection to a backend service or secure server via a proxy server. This proxy server opens the connection between the client and the backend service and copies the data to both sides without any direct interference in the SSL connection:



IPsec

- Internet Protocol Security (IPsec) is a framework consisting of protocols and algorithms for protecting data through an un-trusted network such as the internet.

- Why do we need IPsec?
- Because the IP protocol itself doesn't have any security features at all. IPsec is a complex framework consisting of many settings, which is why it provides a powerful and flexible set of security features that can be used.

- The main reason that IPSec is so powerful is that it provides security to IP, the basis for all other TCP/IP protocols. In protecting IP, we are protecting pretty much everything else in TCP/IP as well.

- IPsec is mandatory in IPv6 and can be used with IPv4 too.