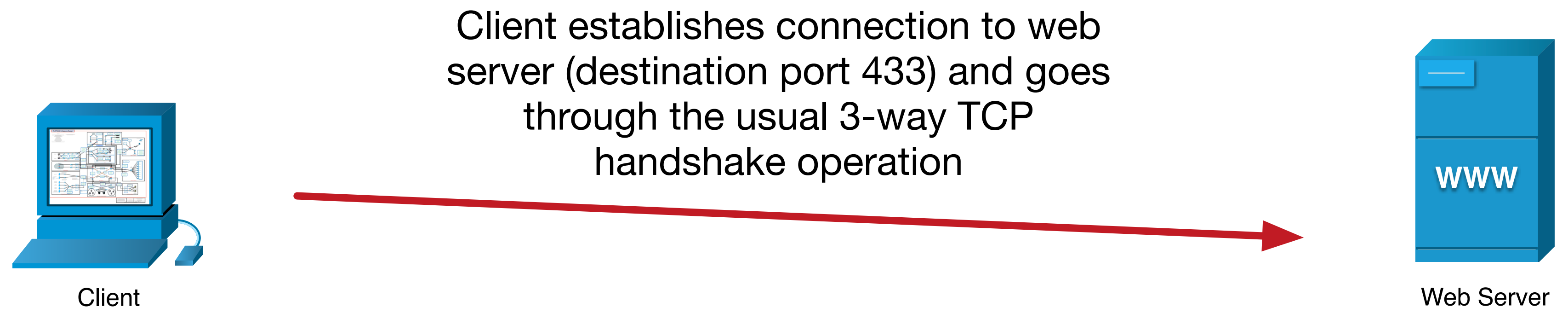
Operation of SSL

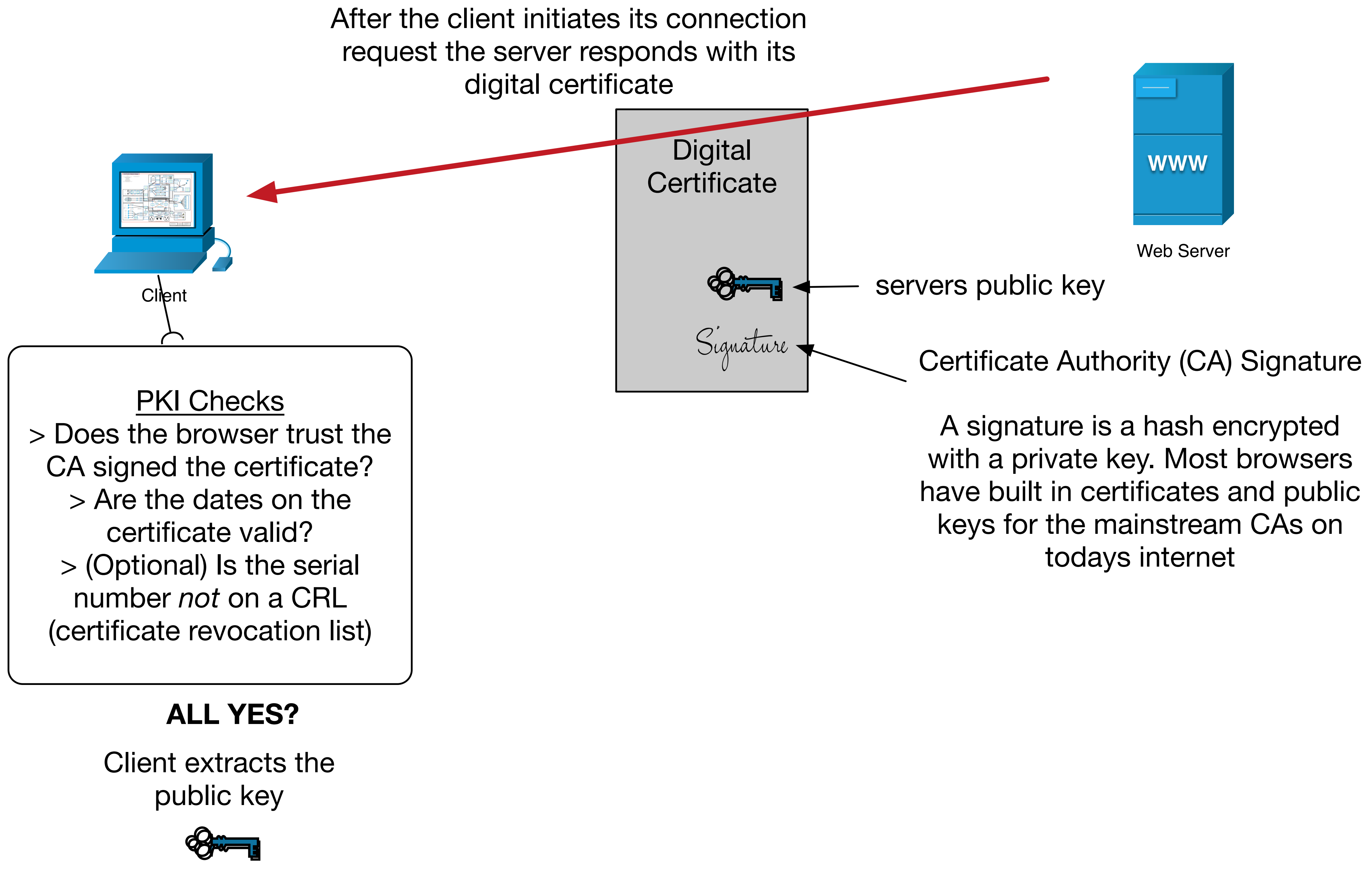
This outlines the order of operations when a client connects to a secure website using SSL through HTTPS

Legend

- Public Key of Server
- Private Key of Server
- CA Signature
- Private Shared Key
- Data Encrypted with a private key
- Unencrypted data



Client establishes connection to web server (destination port 433) and goes through the usual 3-way TCP handshake operation



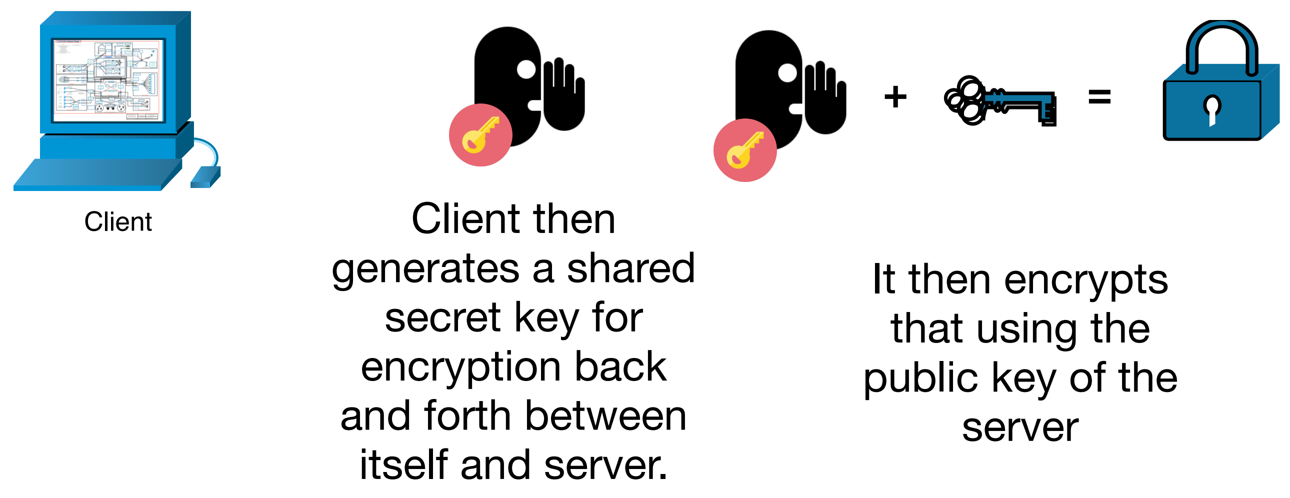
After the client initiates its connection request the server responds with its digital certificate

A signature is a hash encrypted with a private key. Most browsers have built in certificates and public keys for the mainstream CAs on todays internet

PKI Checks
> Does the browser trust the CA signed the certificate?
> Are the dates on the certificate valid?
> (Optional) Is the serial number *not* on a CRL (certificate revocation list)

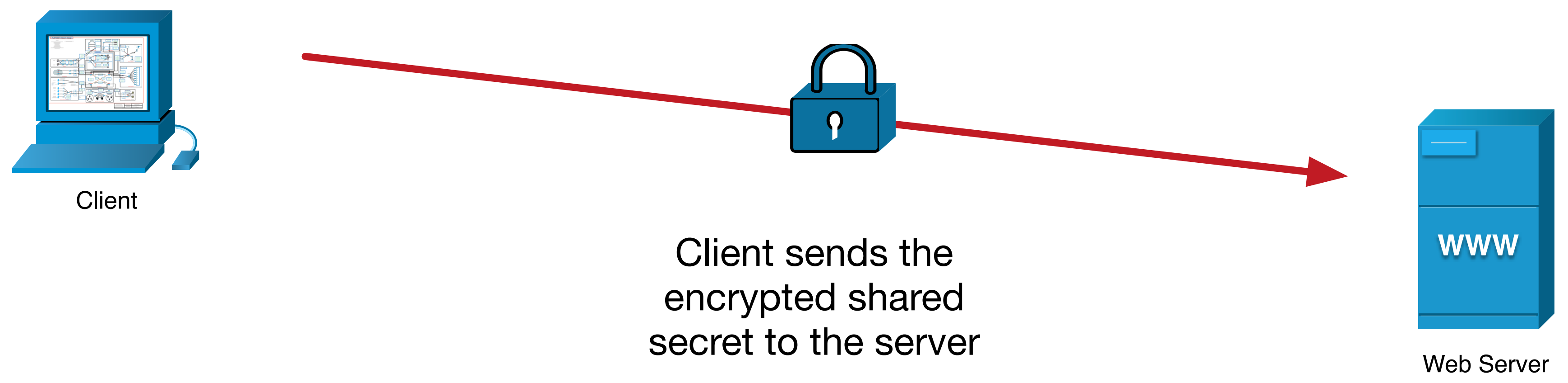
ALL YES?

Client extracts the public key

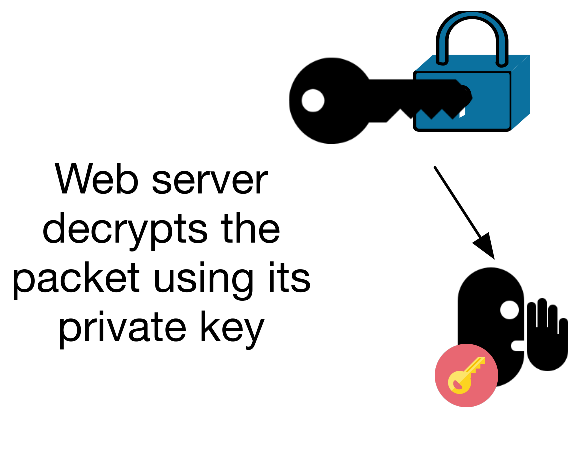


Client then generates a shared secret key for encryption back and forth between itself and server.

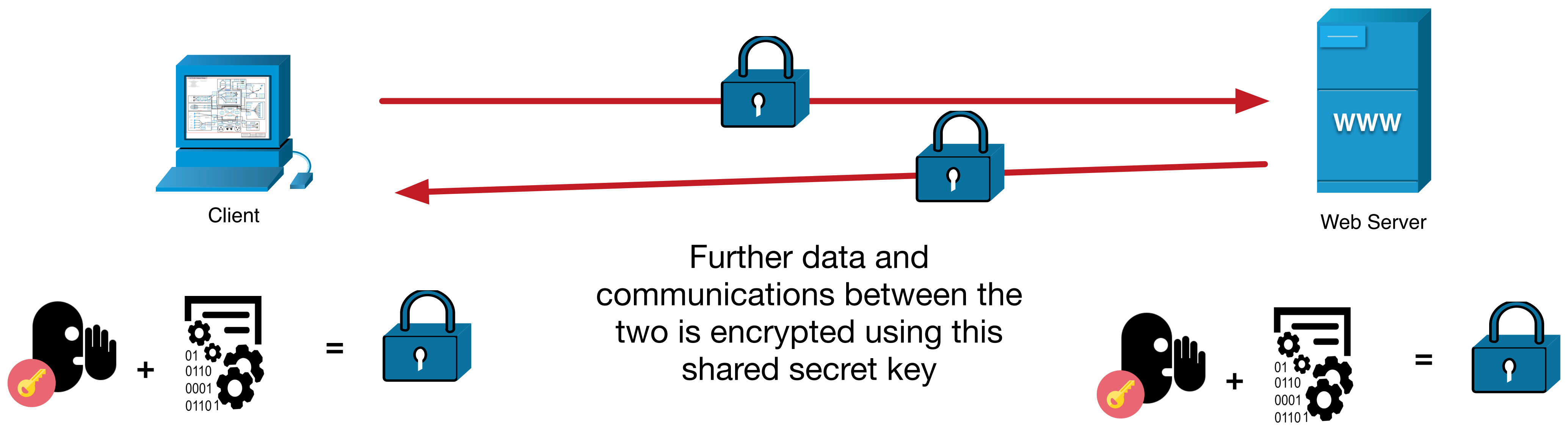
It then encrypts that using the public key of the server



Client sends the encrypted shared secret to the server



Web server decrypts the packet using its private key



Further data and communications between the two is encrypted using this shared secret key

by Steven Crutchley

www.netquirks.co.uk