Chrome 51 connects under TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Short Description	Visibility	Usage Description
Geotrust root CA public key	Visible to everyone	Contained in the Geotrust root certificate, which is stored in the browser's trust store. Eventually used to verify certificates signed using the Geotrust Root private key
Geotrust root CA private key	Super secret, physically secure to probably only a handful of people at Geotrust	Used to sign identity info in csrs to generate subordinate certificates. Also used it to sign its own certificate
Google Internet Authority G2 public key	Visible to everyone	Contained in the Google Internet Authority G2 certificate and used by the browser to verify certificates signed with Google Internet Authority G2's private key
Google Internet Authority G2 private key	Probably less secure than the root certificate, but still super secret visible only to the people at Google Internet Authority G2	Used by google to sign csrs for its own products and generate subordinate certificates.
*.google.com public (RSA) key	Visible to everyone	Used by the google.com server to verify the signature of the public key, Sig(public_key) for DH key exchange where public_key is the clien'ts public DH key. Also used to verify the csr when the certificate is made
*.google.com private (RSA) key	Kept secretly on google.com's server -- only visible to goolge employees who have access to that server	Generated as a pair with their public key. It is used to sign the DH public key. It's also used when getting the certificate to sign a portion of the csr
DH server public key	Visible to everyone	This is g^b from before - used as the server's public key for establishing a shared secret

		under ECDHE
DH client public key	Visible to everyone	This is g^a which will be used to establish a shared secret
DH server private key	Super secret on google.com's server, visible only to google	Generated as a pair with the server's DH public key - used in combination with the client's public key to generate a shared secret
DH client private key	Kept secret on my computer, visible only to me and maybe Joe if he screws with my computer while I'm in the washroom	Generated as a pair with my DH public key - used in combination with the server's public key to generate a shared secret
Pre-Master secret	Visible to client and server only, very important to keep secret.	Defines the final master secret format since different key exchange mechanisms have different formats. Will be hashed into the master secret. Deleted from memory once the Master secret has been computed
Master shared secret	Visible to me, and google.com's server. Not visible to any eve's or signing authorities	Used to encrypt and decrypt all future messages sent to and from google.com
Client write MAC key (and HMAC key derived from this)	Available on both server and client, since it's derived from the master key	Derived from the master key, this is used in the GCM part of AES_GCM to add integrity to messages sent by the client. Used to generate the tag on the client and verify on the server
Server write MAC key (and HMAC key derived from this)	Available on both server and client, since it's derived from the master key	Derived from the master key, this is used in the GCM part of AES_GCM to add integrity to messages sent by the server. Used to generate the tag on the server and verify on the client
Client write encryption key	Available on both server and client, since it's derived from the master key	This is the key used to actually do the encryption part of AES on the client and the decryption part of AES on the server

Server write encryption key	Available on both server and client, since it's derived from the master key	This is the key used to actually do the encryption part of AES on the server and the decryption part of AES on the client
Client write IV	Available on both server and client, since it's derived from the master key	Not technically a key, but it'll definitely be there since this is GCM mode and that uses and IV. Used in the AES portion of AES_GCM
Server write IV	Available on both server and client, since it's derived from the master key	Not technically a key, but it'll definitely be there since this is GCM mode and that uses and IV. Used in the AES portion of AES_GCM