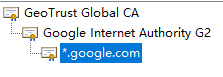
Question 4

The connection to this site is encrypted and authenticated using QUIC (a strong protocol), X25519 (a strong key exchange), and AES\_128\_GCM (a strong cipher).



TLS 1.2: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

|  |  |  |
| --- | --- | --- |
| Description of the key | Name of the entities who know the key | Purpose of the key |
| Google.ca verification key | Everyone | Verify the signature of google.ca EC Diffie-Hellman public key |
| Google.ca EC Diffie-Hellman public key | Everyone | Server Key Exchange  Public key agreement |
| Client EC Diffie-Hellman public key | Everyone | Client Key Exchange  Public key agreement |
| GeoTrust Global CA signing key | Only GeoTrust | Sign Google Internet Authority G2’s certificate |
| GeoTrust Global CA verification key | Everyone | Verify the signatures of GeoTrust’s certificate and Google Internet Authority G2’s certificate |
| Google Internet Authority G2 signing key | Only Google Internet Authority G2 | Sign google.ca’s certificate |
| Google Internet Authority G2 verification key | Everyone | Verify signature of google.ca’s certificate |
| Google .ca signing key | Only google .ca | Sign google.ca EC Diffie-Hellman public key |
| Google.ca EC Diffie-Hellman private key | Only google .ca | Generate the corresponding public key & Apply to client’s public key to form shared secret |
| Client EC Diffie-Hellman private key | Only Client | Generate the corresponding public key & Apply to google.ca’s public key to form shared secret |
| Duffle-Hellman shared secret | Only client and server | Derive master secret |
| Master secret | Only client and server | Derive symmetric keys |
| Client-write symmetric encryption key | Only client and server | Client: Encrypt message  Server: Decrypt message |
| Server-write symmetric encryption key | Only client and server | Server: Encrypt message  Client: Decrypt message |
| Client-write MAC key | Only client and server | Client: Generate a MAC tag  Server: Verify MAC tag |
| Server-write MAC key | Only client and server | Server: Generate a MAC tag  Client: Verify MAC tag |