|  |  |
| --- | --- |
| **Generate a Self-Signed SSL Certificate** | |
| **Generate a Private Key**: | openssl genrsa -out private.key 2048 |
| **Create a Certificate Signing Request (CSR)**:  You’ll be prompted for details like:   * Country Name (e.g., US) * State/Province * Organization Name * Common Name (your domain or localhost). | openssl req -new -key private.key -out request.csr |
| **Generate the Self-Signed Certificate**: | openssl x509 -req -days 365 -in request.csr -signkey private.key -out certificate.crt |
| You’ll now have:   * private.key (your private key) * request.csr (the CSR file) * certificate.crt (the self-signed certificate) | |

|  |  |
| --- | --- |
| **Converting Certificates Between Formats** | |
| Convert PEM to DER | openssl x509 -outform der -in certificate.crt -out certificate.der |
| Convert PEM to PKCS12 (for Windows IIS) | openssl pkcs12 -export -out certificate.pfx -inkey private.key -in certificate.crt |

|  |  |
| --- | --- |
| **Encrypting and Decrypting Files** | |
| Encrypt a File: | openssl enc -aes-256-cbc -salt -in file.txt -out file.enc |
| Decrypt a File: | openssl enc -aes-256-cbc -d -in file.enc -out file\_decrypted.txt |

|  |  |
| --- | --- |
| Generating a Hash (Checksum) | openssl dgst -sha256 file.txt |

|  |  |
| --- | --- |
| Check HTTPS Certificate Details: | openssl s\_client -connect google.com:443 |

|  |  |
| --- | --- |
| **Creating a Root CA**  If you need to act as your own Certificate Authority (CA), follow these steps. | |
| **Generate the Root CA Key**: | openssl genrsa -out rootCA.key 2048 |
| **Create the Root CA Certificate**: | openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem |
| **Sign a Certificate with Your Root CA**: | openssl x509 -req -in request.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out signed\_certificate.crt -days 500 -sha256 |

|  |  |
| --- | --- |
| **Checking Certificate Details** | |
| Inspect a Certificate: | openssl x509 -in certificate.crt -text -noout |
| Verify a Certificate: | openssl verify -CAfile rootCA.pem signed\_certificate.crt |

|  |  |
| --- | --- |
| **Export Public Key** | |
| To extract the public key from a private key: | openssl rsa -in private.key -pubout -out public.key |

|  |  |
| --- | --- |
| **Create Random Passwords or Files** | |
| Generate a Random Password: | openssl rand -base64 12 |
| Generate a Random File: | openssl rand -out randomfile.bin 1024 |

|  |  |
| --- | --- |
| **Debugging SSL/TLS Issues** | |
| Check for SSL/TLS Vulnerabilities: | openssl s\_client -connect <hostname>:443 -tls1\_2 |
| Debug Certificate Chains: | openssl s\_client -connect <hostname>:443 -showcerts |