Experiment 4: OpenSSL – Keys & Certificates

Experiment 4: OpenSSL – Key Generation, Certificate Creation and Verification

This experiment demonstrates RSA private key generation, creation of a self-signed X.509 certificate, and verification using OpenSSL.

Files Included:

1) Commands.txt – Contains the exact OpenSSL commands used.

2) certificate.crt – Generated self-signed certificate.

Steps Performed

1) Installing OpenSSL:

Linux: sudo apt-get install openssl

Windows: Download from slproweb.com (Win32OpenSSL)

2) Generating Private Key:

openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048

3) Creating a Self-Signed Certificate:

openssl req -new -x509 -key private.key -out certificate.crt -days 365

User is prompted for fields like CN, Organization, Country, etc.

4) Viewing Certificate Details:

openssl x509 -in certificate.crt -text -noout

Shows subject, issuer, validity, public key, signature algorithm.

5) Verifying Certificate:

openssl verify -CAfile certificate.crt certificate.crt

Output: certificate.crt: OK

Folder Structure:

Experiment-4/

■■■ private.key

■■■ certificate.crt

■■■ Commands.txt

■■■ README_Exp4.pdf