**Kiran Qaiser 251683919**

**Information Security COMP 421**

**Fall 2024 Section B**

**Assignment 2**

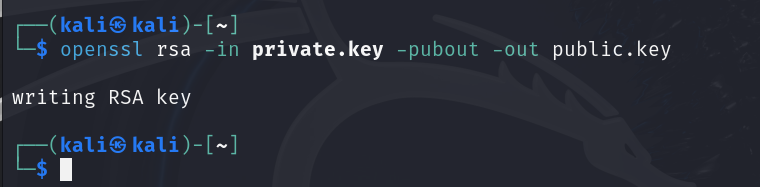
**Step 1: Generate Private and Public Keys**

1. **Command to generate a private key:**

openssl genrsa -out private.key 2048

  
  
 **2.Command to generate a public key using the private key:**

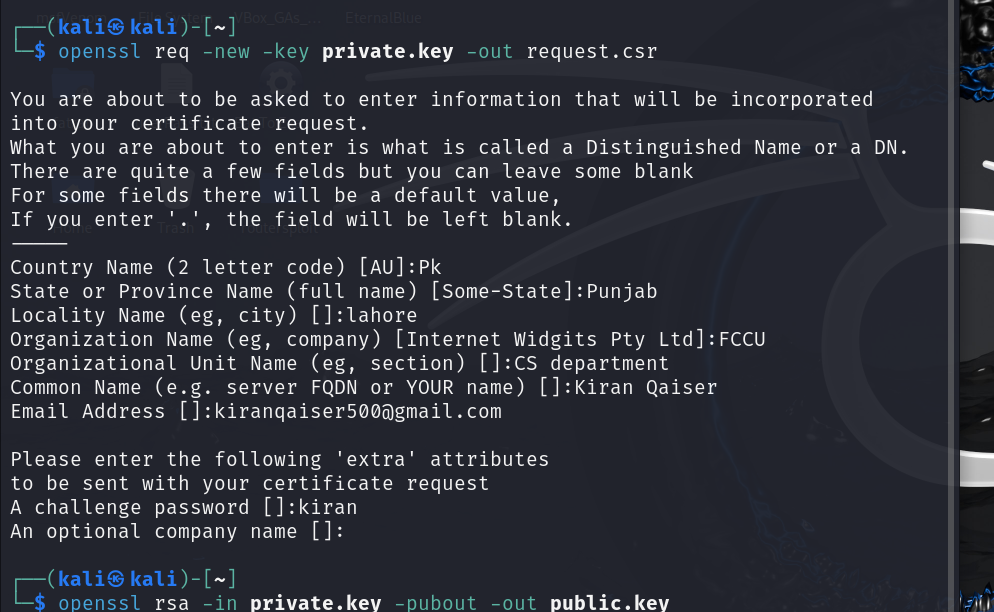
openssl rsa -in private.key -pubout -out public.key



**Step 2: Generate a Certificate Signing Request (CSR)**

1. **Create a CSR using the private key:**

openssl req -new -key private.key -out request.csr



**Step 3: Create a Self-Signed Certificate**

1. **Use the CSR to generate a self-signed certificate:**

openssl x509 -req -in request.csr -signkey private.key -out selfsigned.crt -days 365

A computer screen with white text

Description automatically generated

**Step 4: Act as a Certification Authority (CA)**

1. **Create a CA private key:**

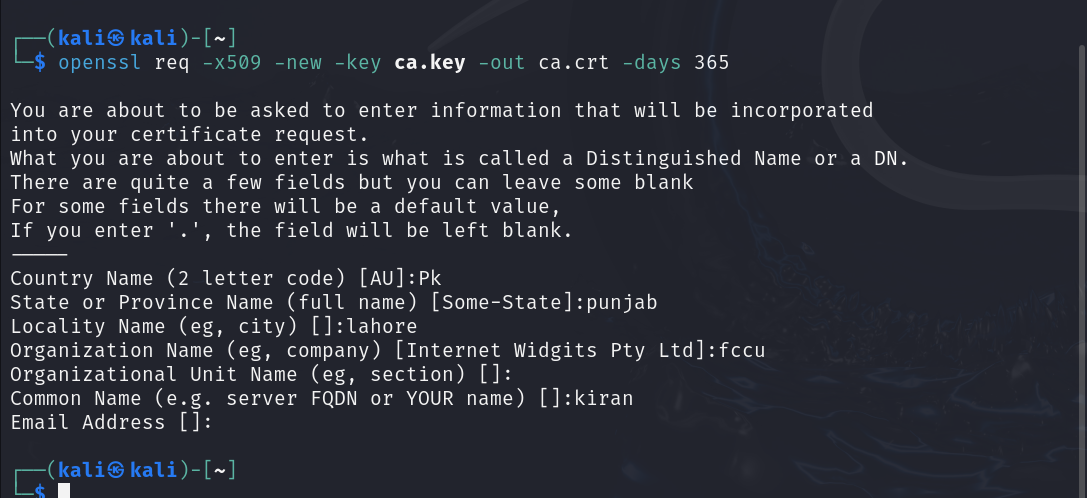
openssl genrsa -out ca.key 2048

A screen shot of a computer

Description automatically generated

1. **Generate a CA certificate:**

openssl req -x509 -new -key ca.key -out ca.crt -days 365



1. **Issue a certificate using the CA:**

openssl x509 -req -in request.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out issued\_cert.crt -days 365

