**Cyber Security Fundamentals**

**Assignment 2:**

**Overview: Use the openssl command-line tool to generate an RSA key pair (public and private key). Export the keys and display them in PEM format.**

Step 1: Open Your Terminal or Command Prompt

Make sure OpenSSL is installed and accessible. Type:

**openssl version**

You should see the OpenSSL version displayed.

Step 2: Generate the Private Key

Run the following command to generate a 2048-bit RSA private key and save it in private\_key.pem:

**openssl genrsa -out private\_key.pem 2048**

Step 3: Generate the Public Key from the Private Key

Create the public key public\_key.pem with this command:

**openssl rsa -in private\_key.pem -pubout -out public\_key.pem**

Step 4: Verify the Private Key (View the PEM Format)

Display the private key file contents:

**cat private\_key.pem**

Your output will begin with:

-----BEGIN RSA PRIVATE KEY-----

Step 5: Verify the Public Key (View the PEM Format)

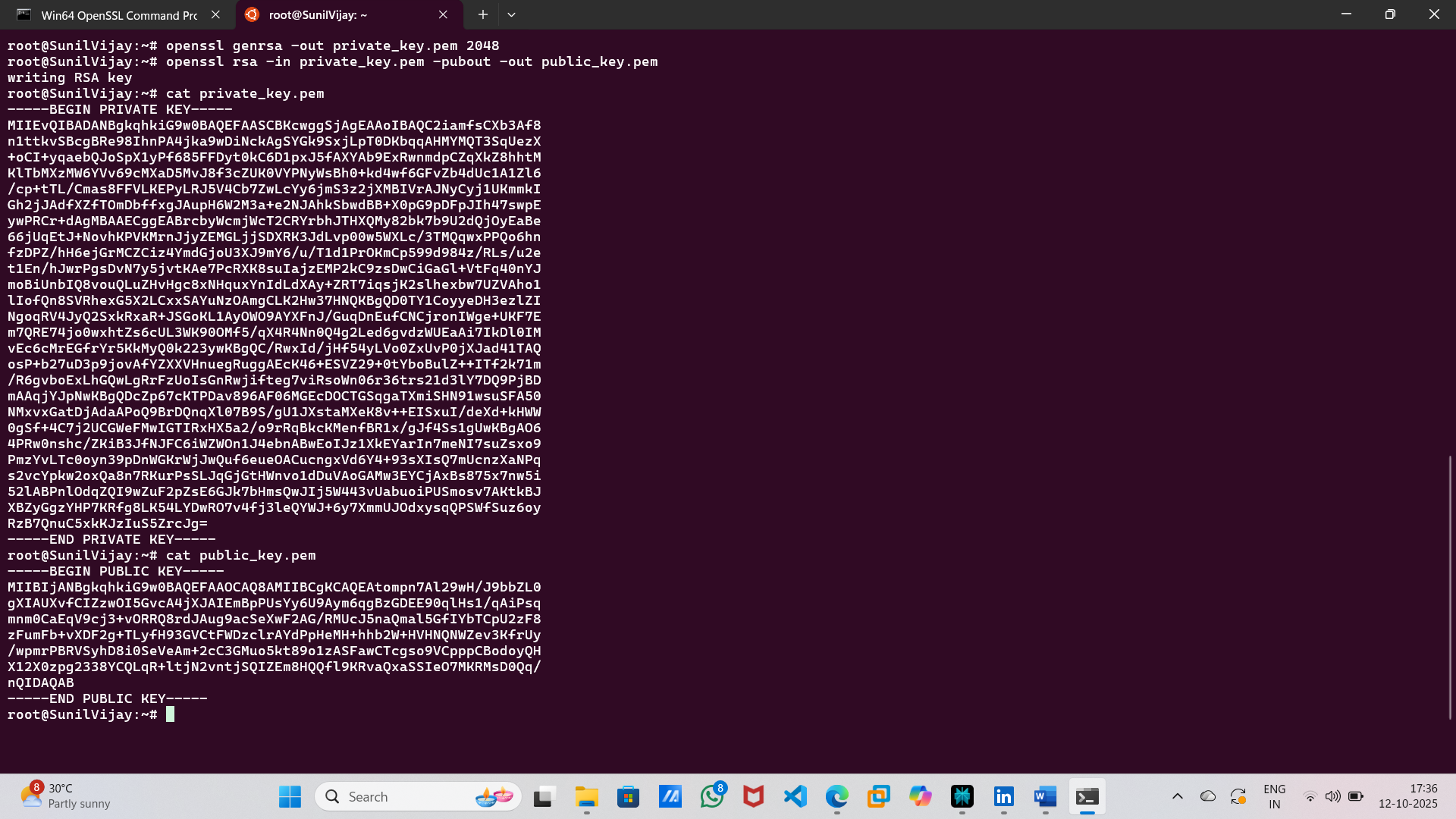
Display the public key file contents:

**cat public\_key.pem**

Your output will begin with:

text

-----BEGIN PUBLIC KEY-----

****