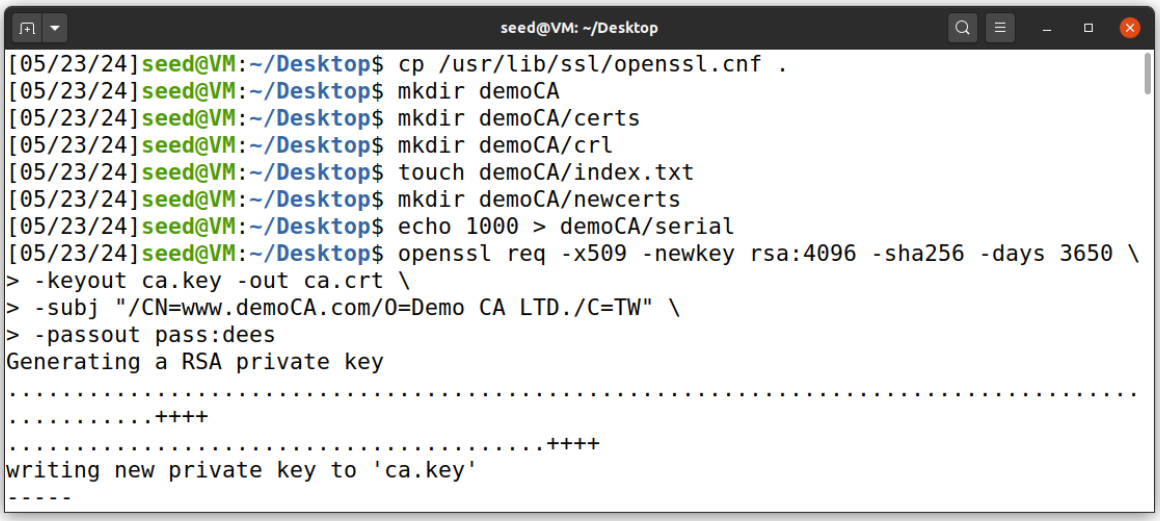
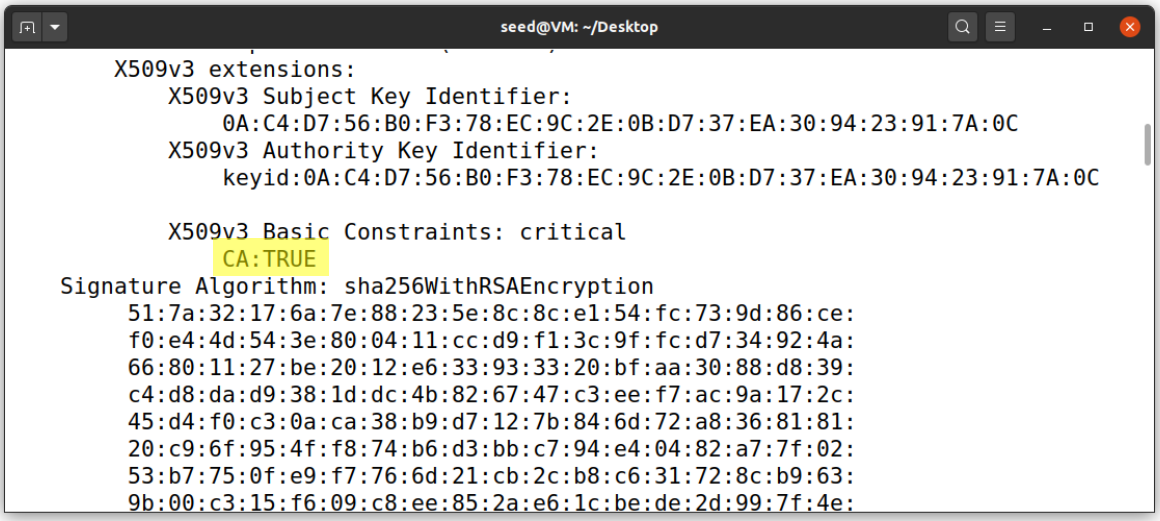
姓名：蔡佩蓉　　學號：109511286

Secret-Key Encryption Lab (Lab5)

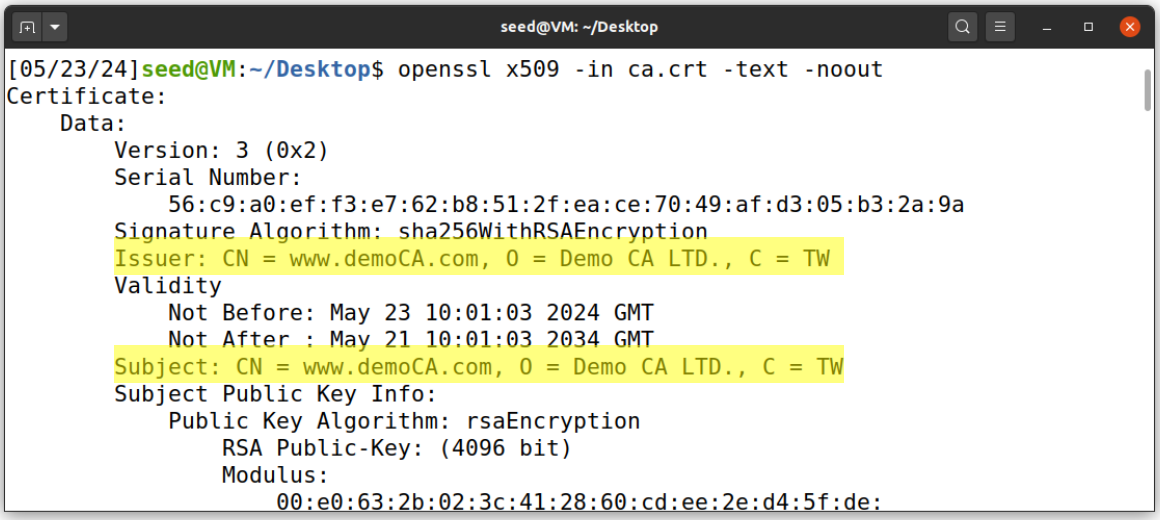
Task 1: Becoming a Certificate Authority (CA)



What part of the certificate indicates this is a CA's certificate?

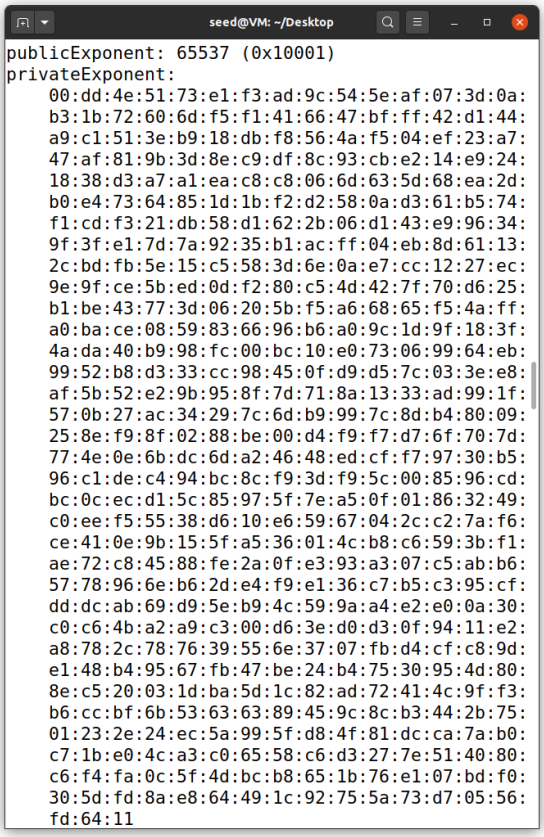


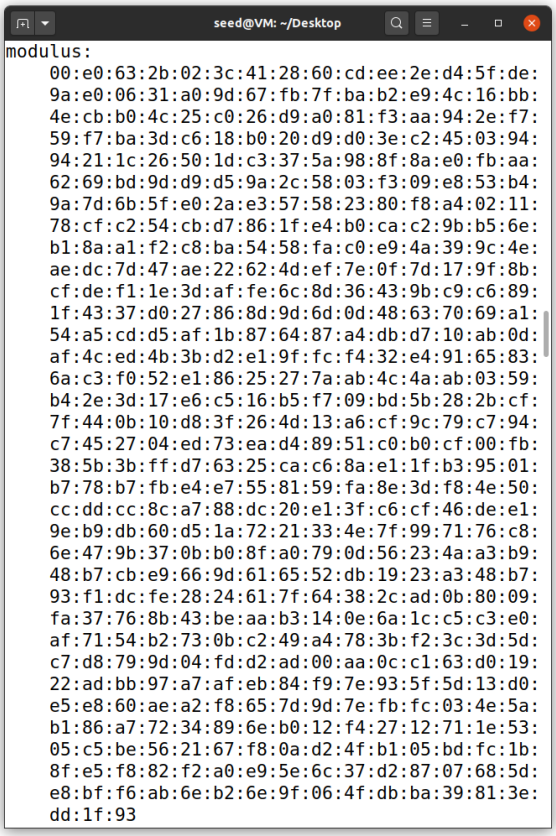
What part of the certificate indicates this is a self-signed certificate?

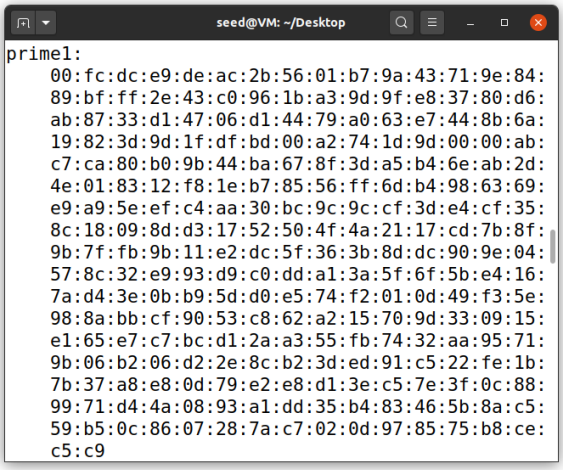


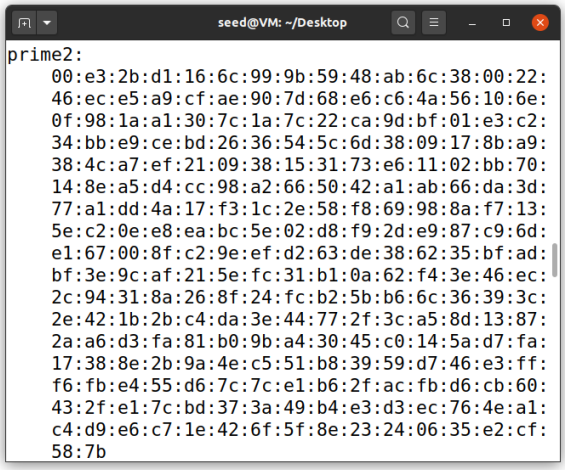
Subject and Issuer panel contains the same information indicates that this is a self-signed certificate.

In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that n = pq. Please identify the values for these elements in your certificate and key files.

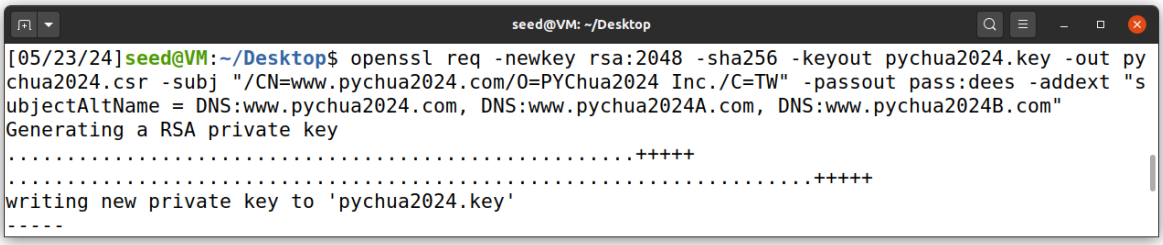


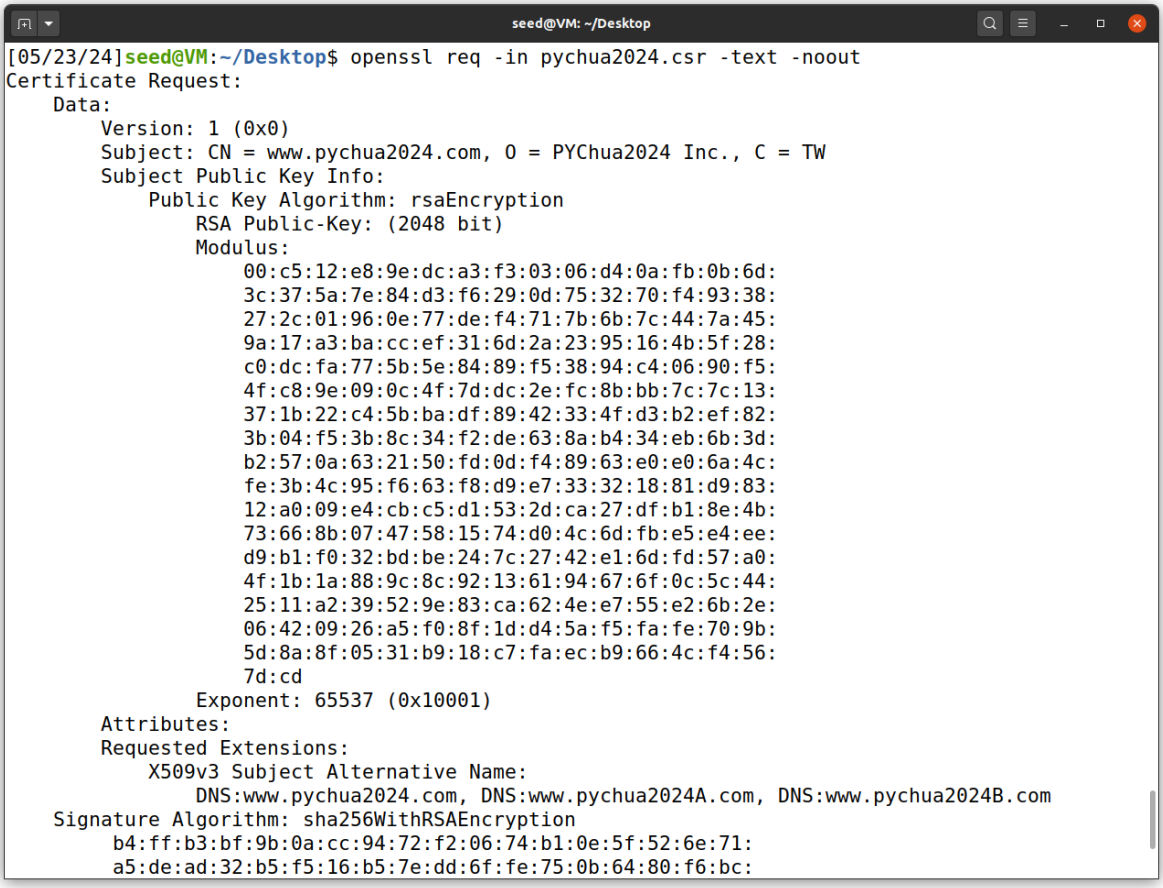




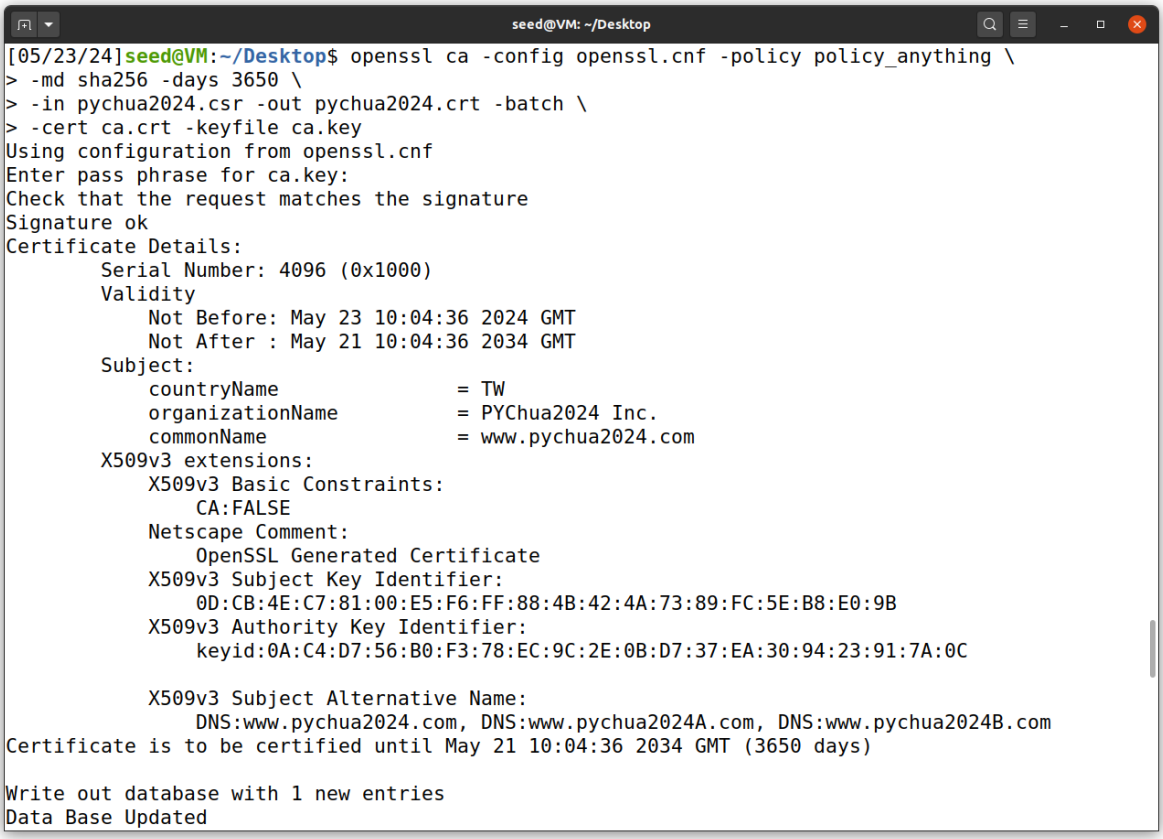


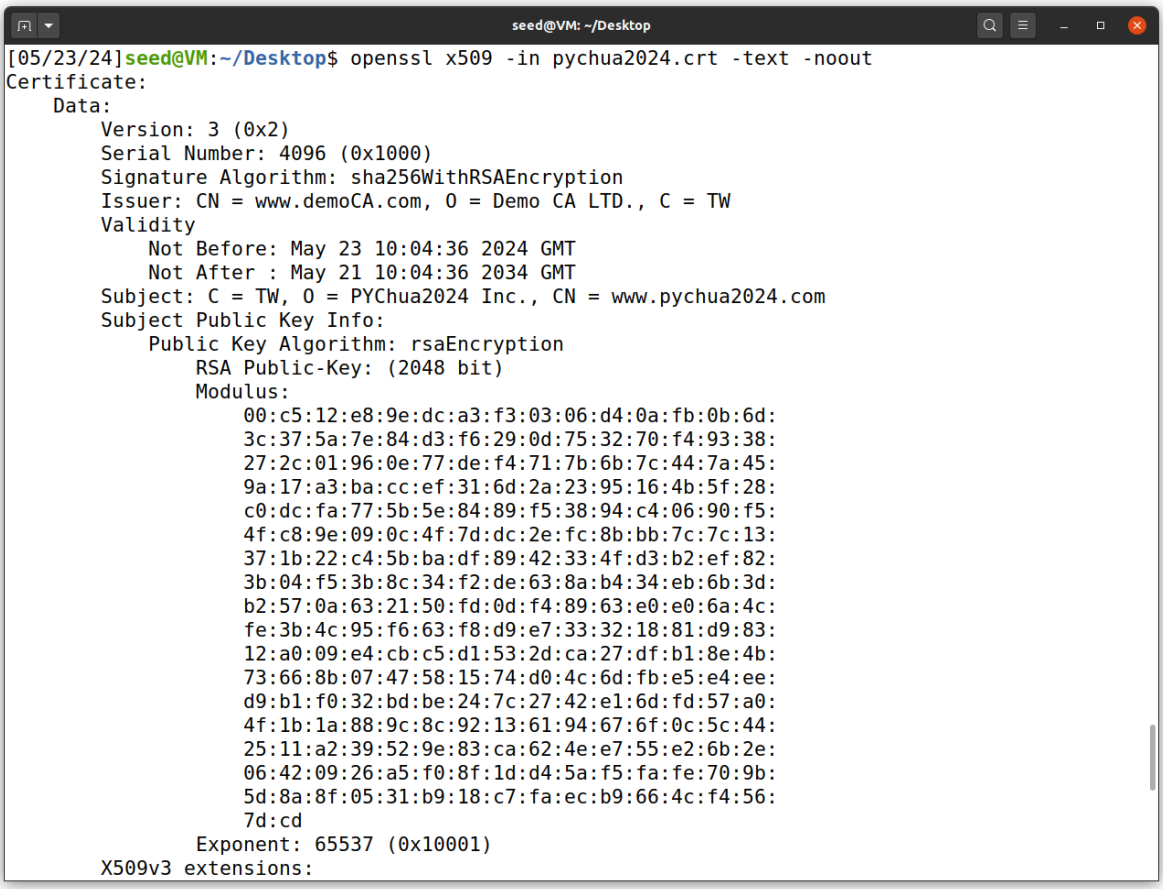
Task 2: Generating a Certificate Request for Your Web Server



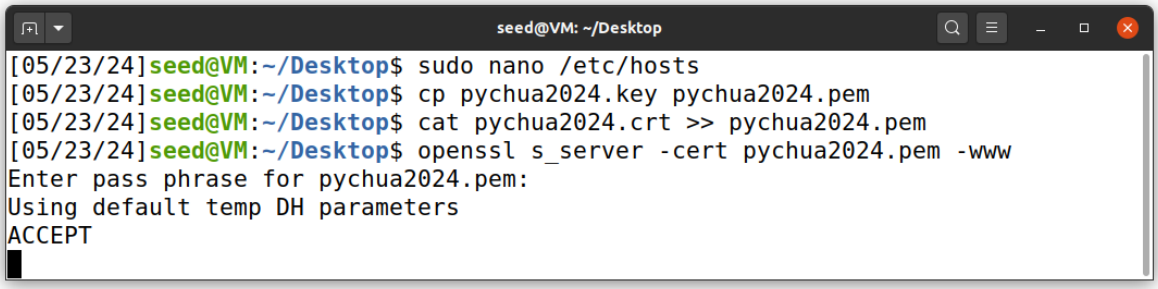


Task 3: Generating a Certificate for your server





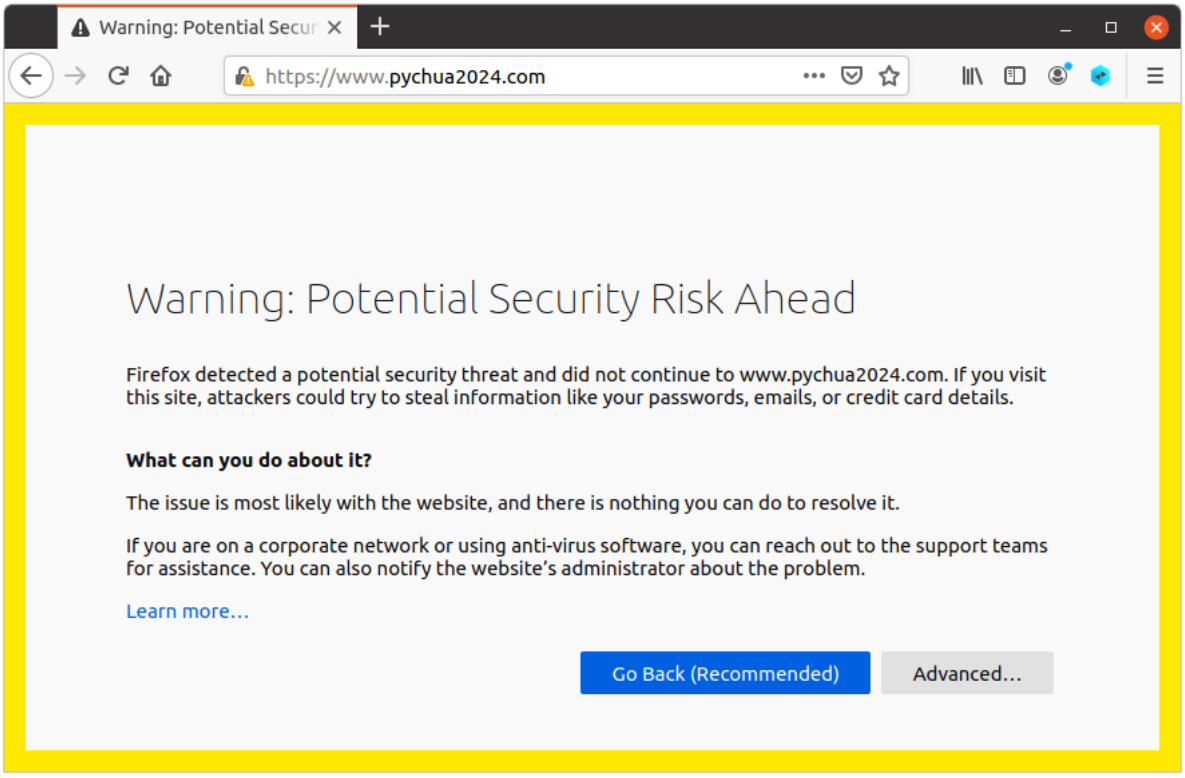
Task 4: Deploying Certificate in an Apache-Based HTTPS Website



Edit /etc/hosts file. Then, combine the secret key and the certificate into one file to configure the web server. Then launch our web server using pychua2024.pem.

This server can be accessed by typing https://www.pychua2024.com in Firefox but we will get an error that connection is not secure.

Before adding certificate to the Firefox browser:

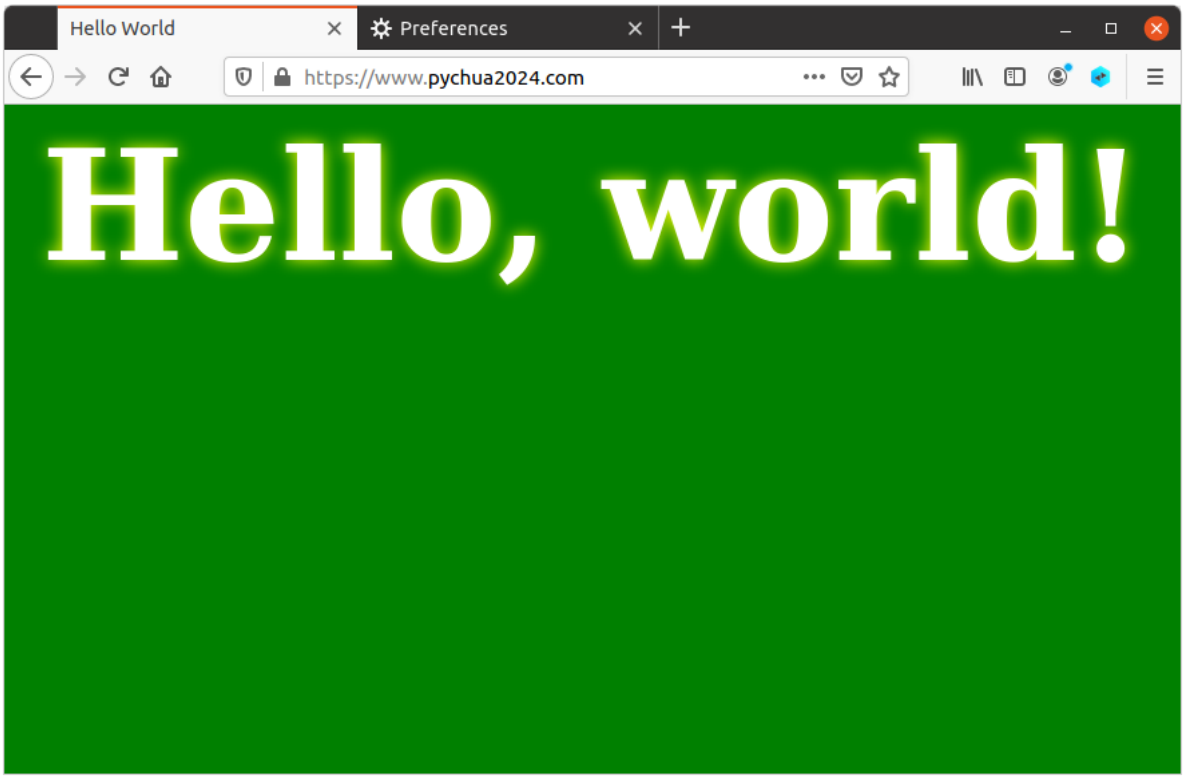


The connection is not secure due to an invalid security certificate. As the certificate issuer is unknown to Firefox (self-signed). Hence, we need to add our certificate to the browser so that it is recognized as a legitimate certificate.

For that we will go to preferences, security and then in the end view certificates and add our certificate there. Make sure to check the box saying that “Trust this CA to identify websites”.

Now when we run our website it will be accessed without error.

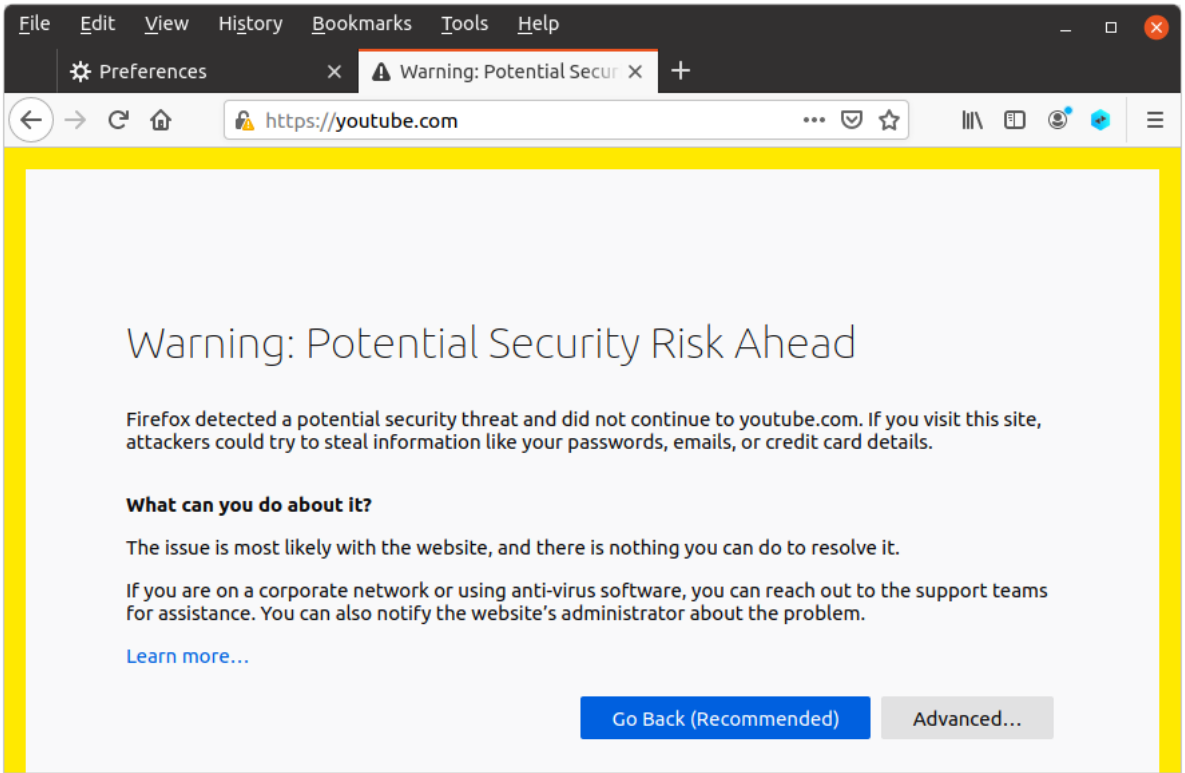
After adding certificate:



The terminal will also print accept each time the website is reloaded.

Task 5: Launching a Man-In-The-Middle Attack

Edit /etc/hosts file. [10.9.0.80 youtube.com]



We accessed the server we built, but the certificate is not trusted.