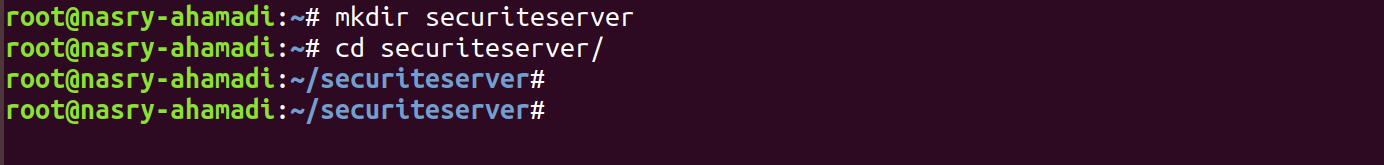
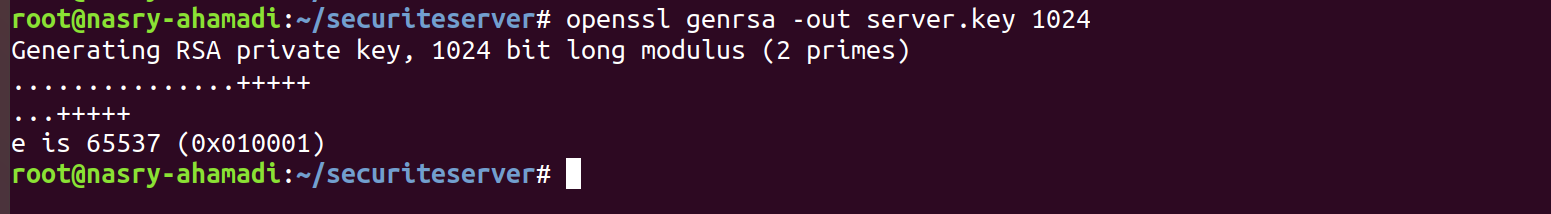
Activité 1: comment générer un certificat openssl.



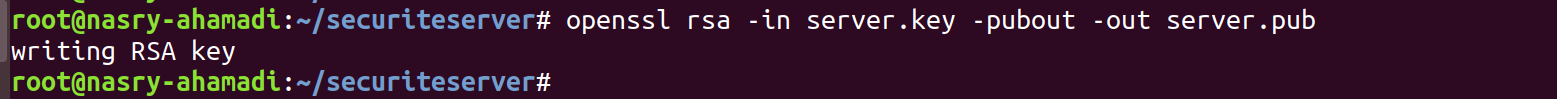
root@nasry-ahamadi:~/securiteserver# openssl genrsa -out server.key 1024



root@nasry-ahamadi:~/securiteserver# ls



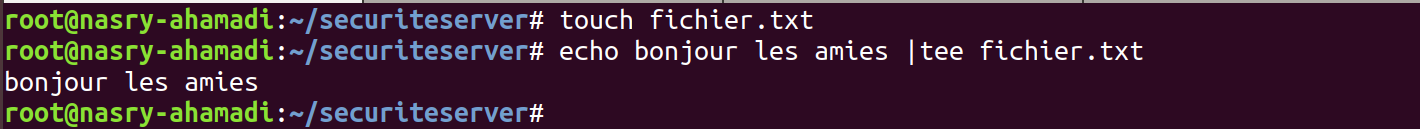
root@nasry-ahamadi:~/securiteserver# openssl rsa -in server.key -pubout -out server.pub



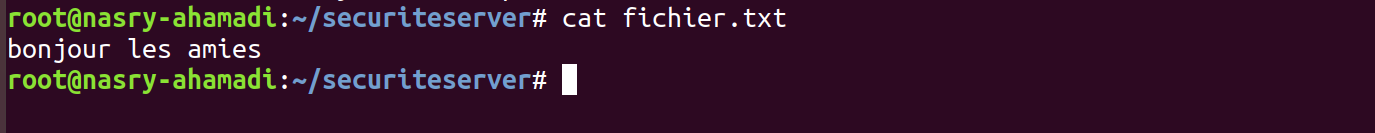


root@nasry-ahamadi:~/securiteserver# touch fichier.txt

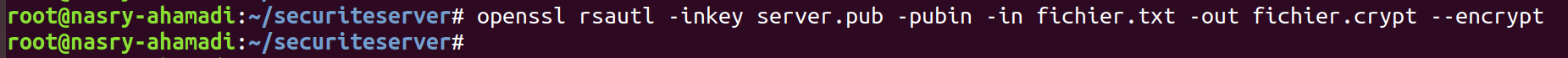
root@nasry-ahamadi:~/securiteserver# echo bonjour les amies |tee fichier.txt



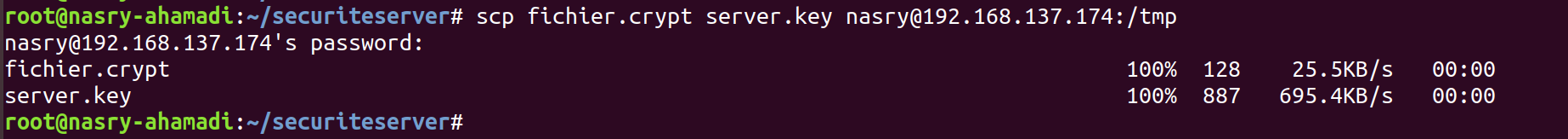
root@nasry-ahamadi:~/securiteserver# cat fichier.txt



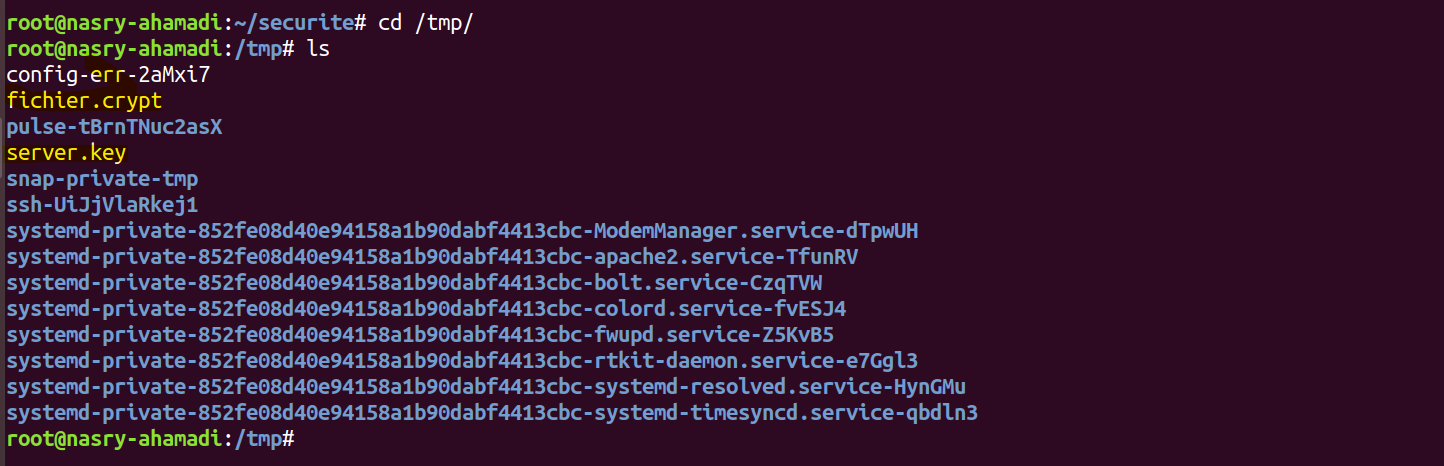
root@nasry-ahamadi:~/securiteserver# openssl rsautl -inkey server.pub -pubin -in fichier.txt -out fichier.crypt --encrypt





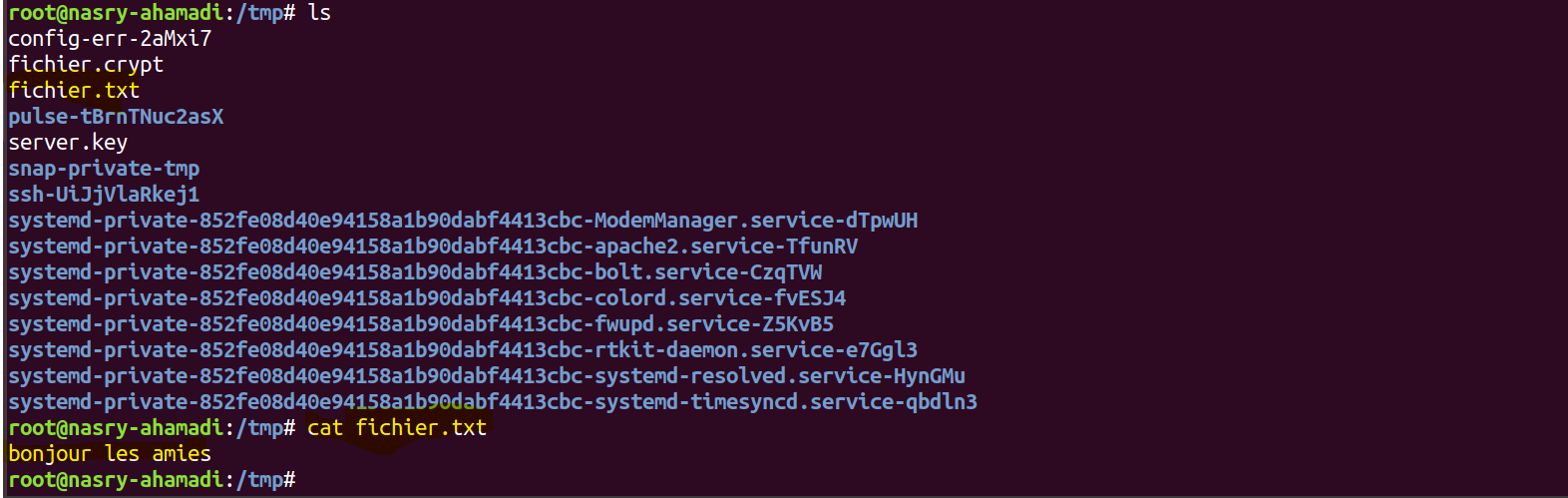


Cote client :



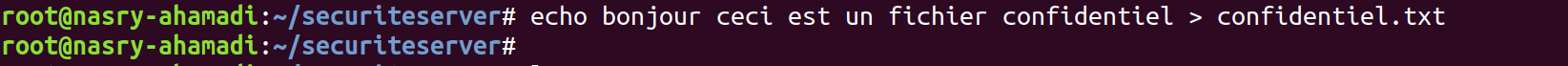
root@nasry-ahamadi:/tmp# openssl rsautl -inkey server.key -in fichier.crypt -out fichier.txt -decrypt

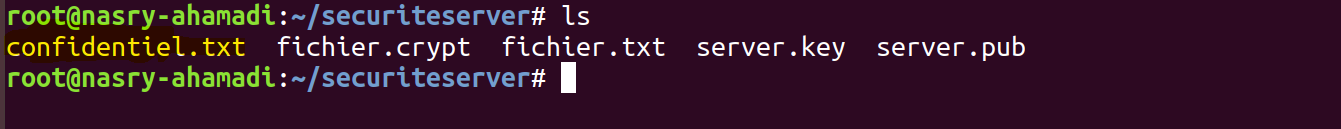




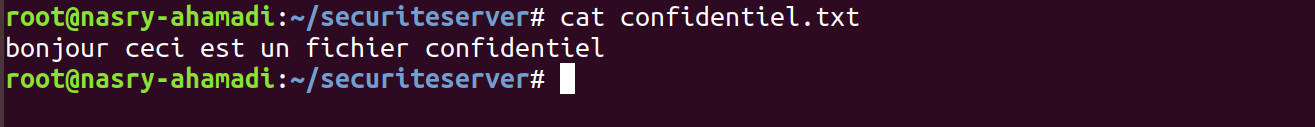
Activité 2 : Chiffrement et déchiffrement avec openssl.

root@nasry-ahamadi:~/securiteserver# echo bonjour ceci est un fichier confidentiel > confidentiel.txt

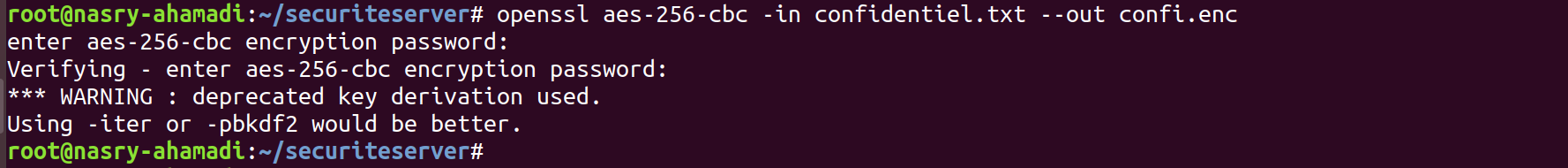


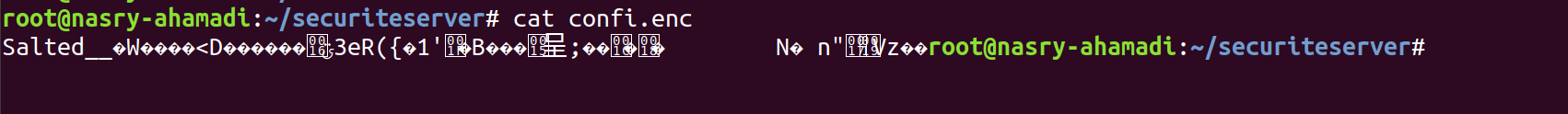


root@nasry-ahamadi:~/securiteserver# cat confidentiel.txt

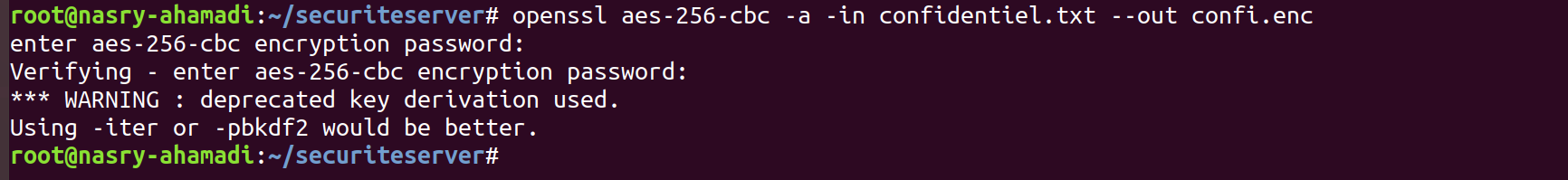


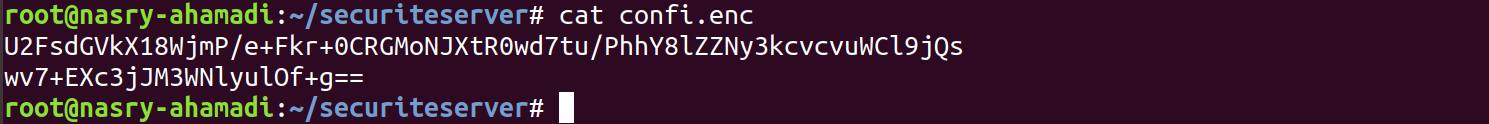
root@nasry-ahamadi:~/securiteserver# openssl aes-256-cbc -in confidentiel.txt --out confi.enc

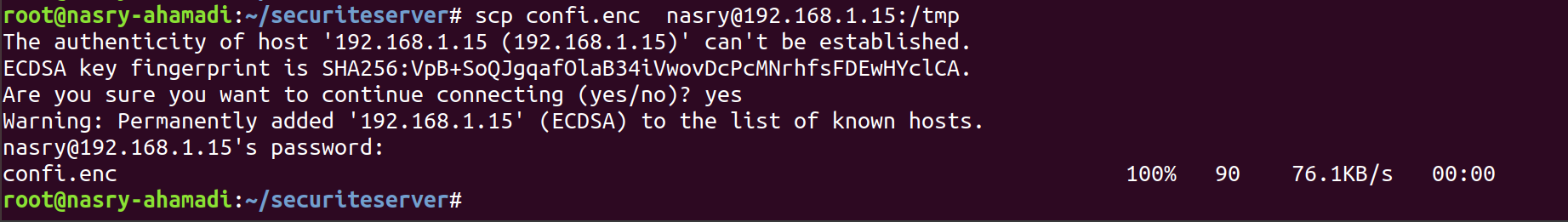


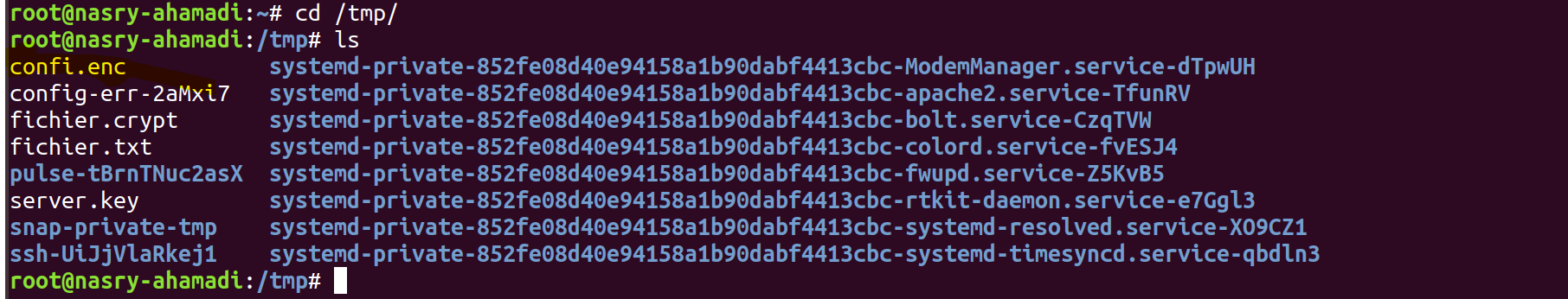


root@nasry-ahamadi:~/securiteserver# openssl aes-256-cbc -a -in confidentiel.txt --out confi.enc

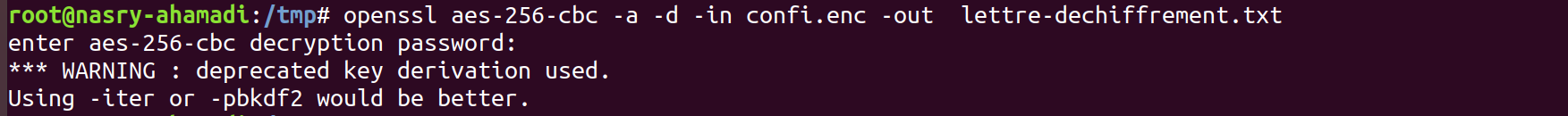


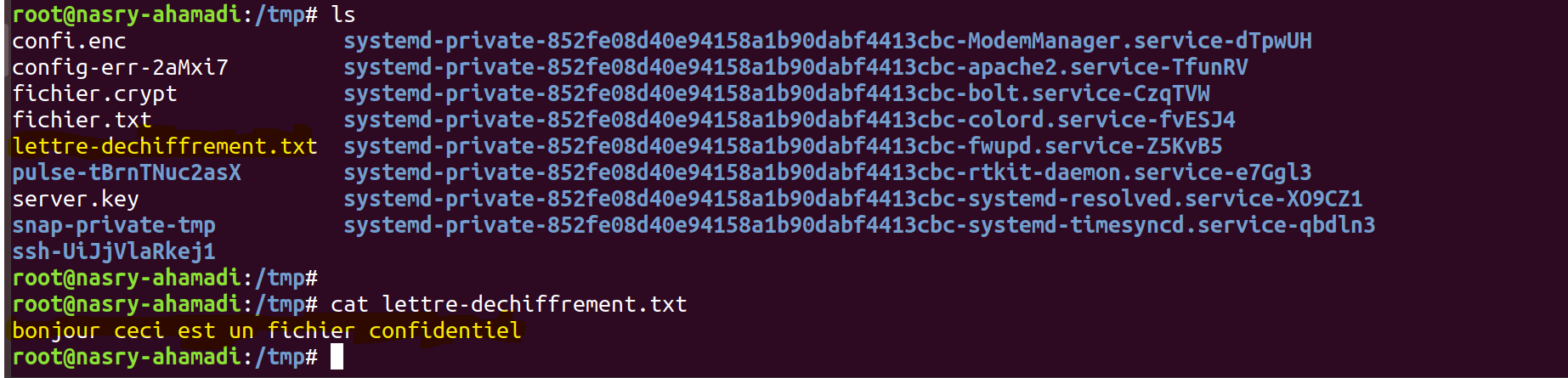






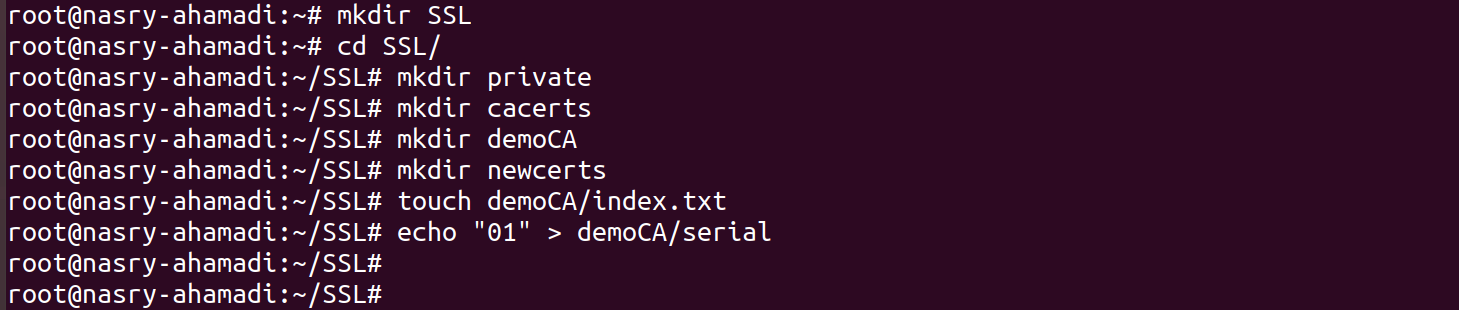
root@nasry-ahamadi:/tmp# openssl aes-256-cbc -a -d -in confi.enc -out lettre-dechiffrement.txt



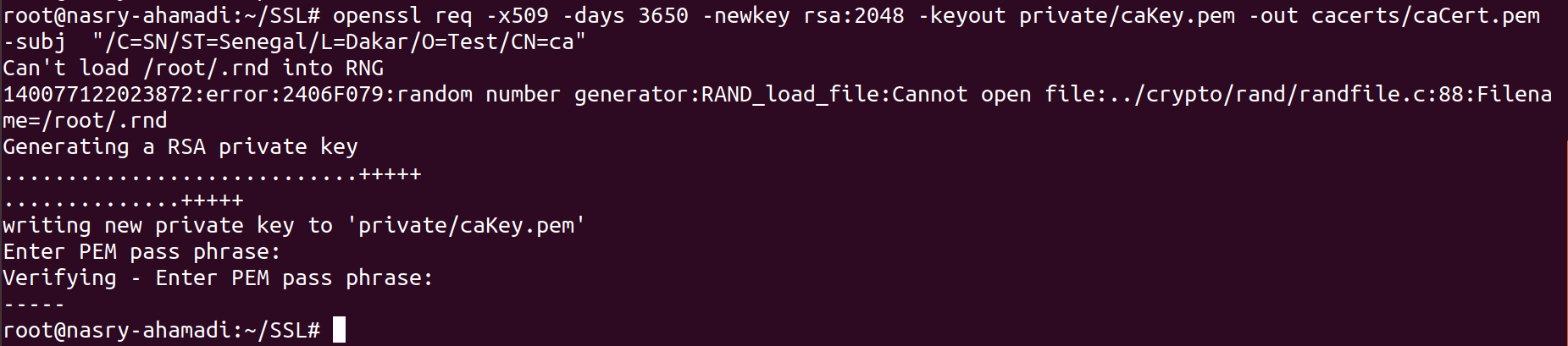


Activite 3 :

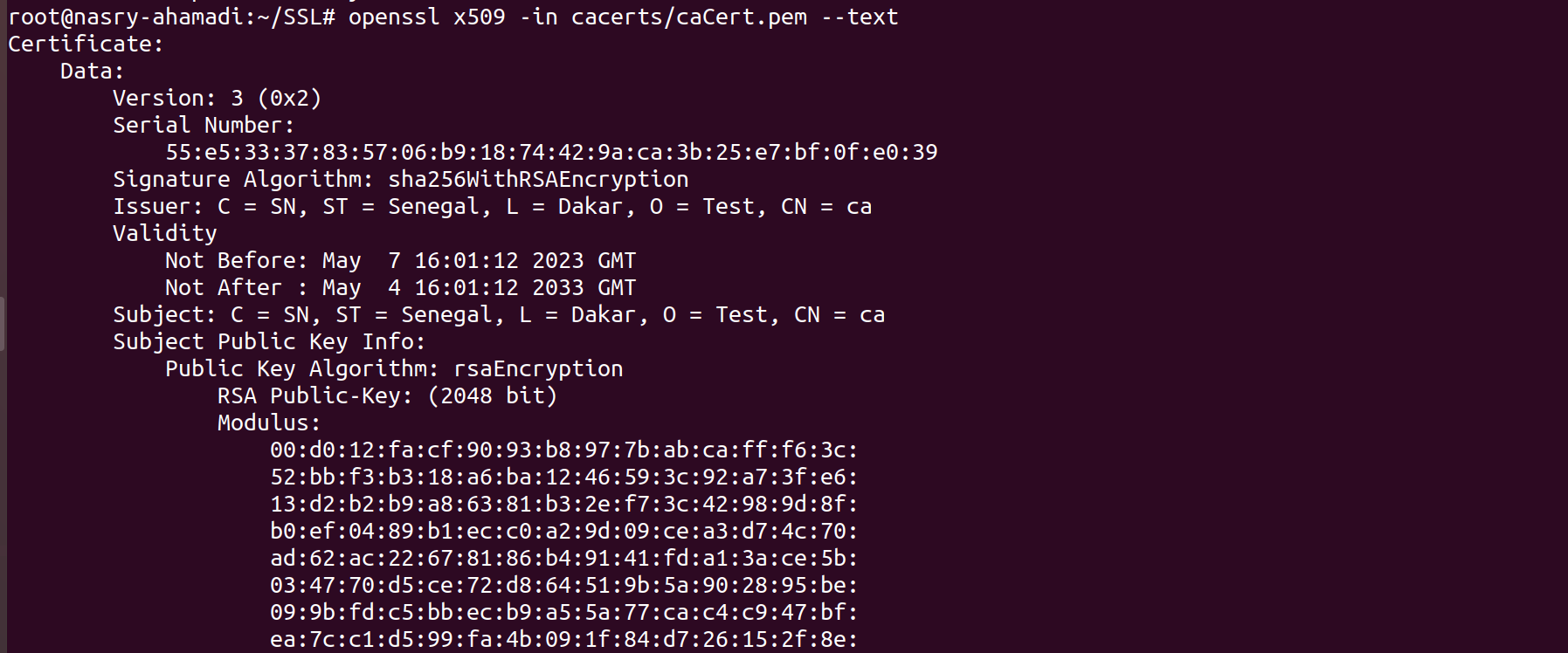




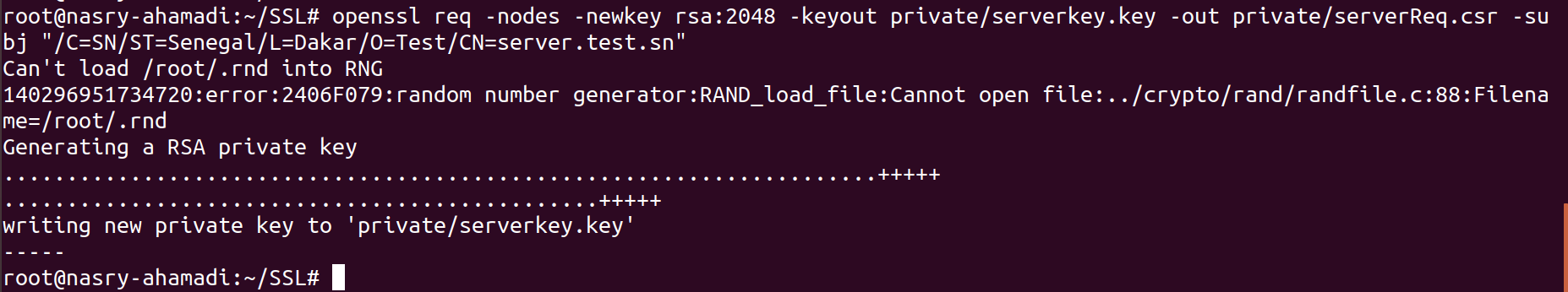
openssl req -x509 -days 3650 -newkey rsa:2048 -keyout private/caKey.pem -out cacerts/caCert.pem -subj "/C=SN/ST=Senegal/L=Dakar/O=Test/CN=ca"



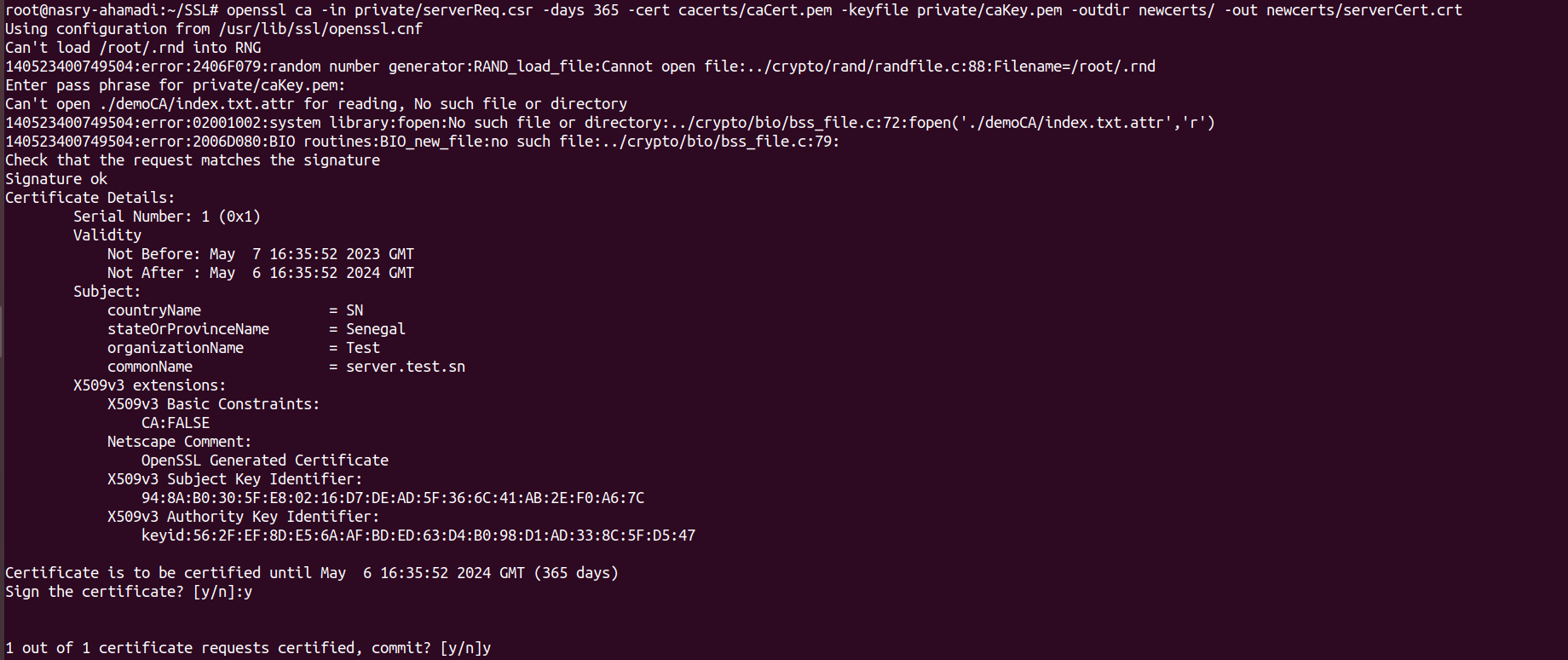
openssl x509 -in cacerts/caCert.pem --text



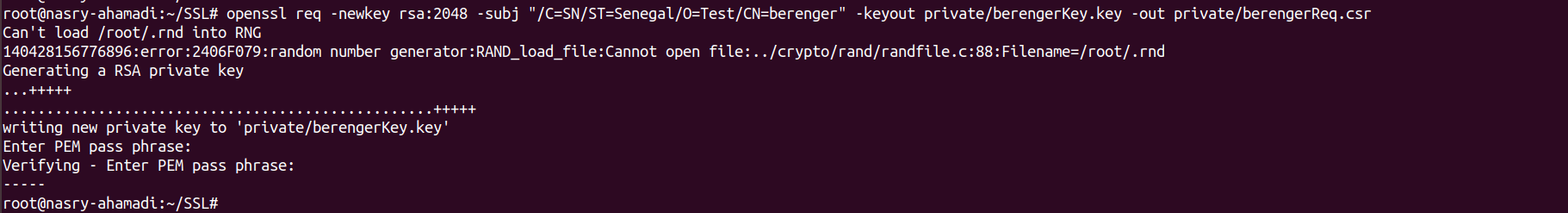
root@nasry-ahamadi:~/SSL# openssl req -nodes -newkey rsa:2048 -keyout private/serverkey.key -out private/serverReq.csr -subj "/C=SN/ST=Senegal/L=Dakar/O=Test/CN=server.test.sn"



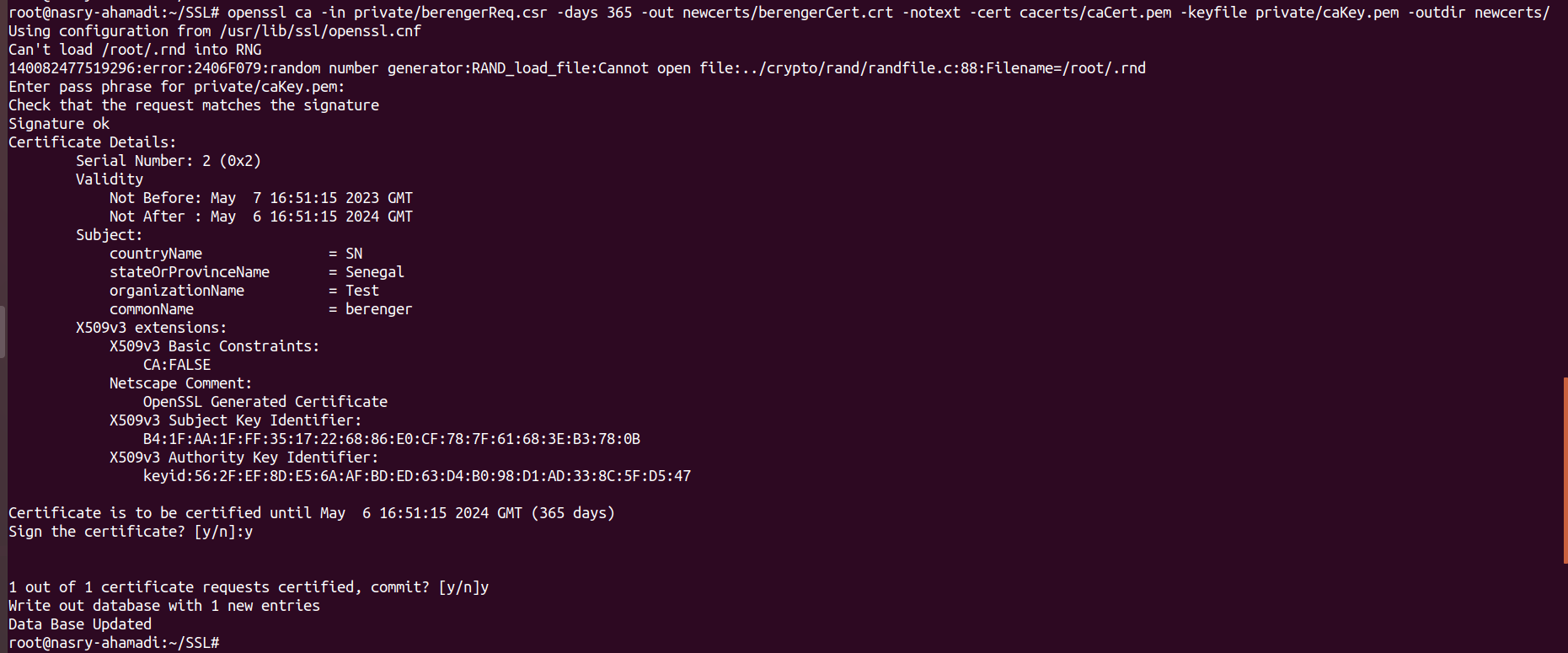
root@nasry-ahamadi:~/SSL# openssl ca -in private/serverReq.csr -days 365 -cert cacerts/caCert.pem -keyfile private/caKey.pem -outdir newcerts/ -out newcerts/serverCert.crt



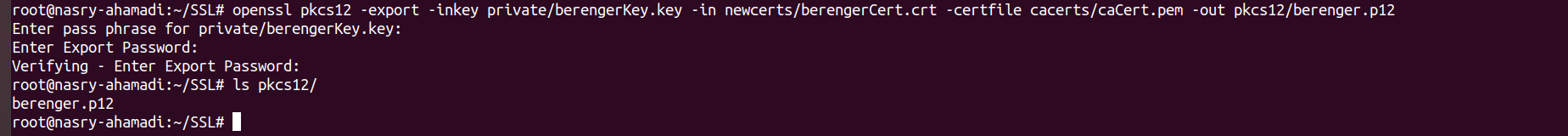
root@nasry-ahamadi:~/SSL# openssl req -newkey rsa:2048 -subj "/C=SN/ST=Senegal/O=Test/CN=berenger" -keyout private/berengerKey.key -out private/berengerReq.csr



root@nasry-ahamadi:~/SSL# openssl ca -in private/berengerReq.csr -days 365 -out newcerts/berengerCert.crt -notext -cert cacerts/caCert.pem -keyfile private/caKey.pem -outdir newcerts/

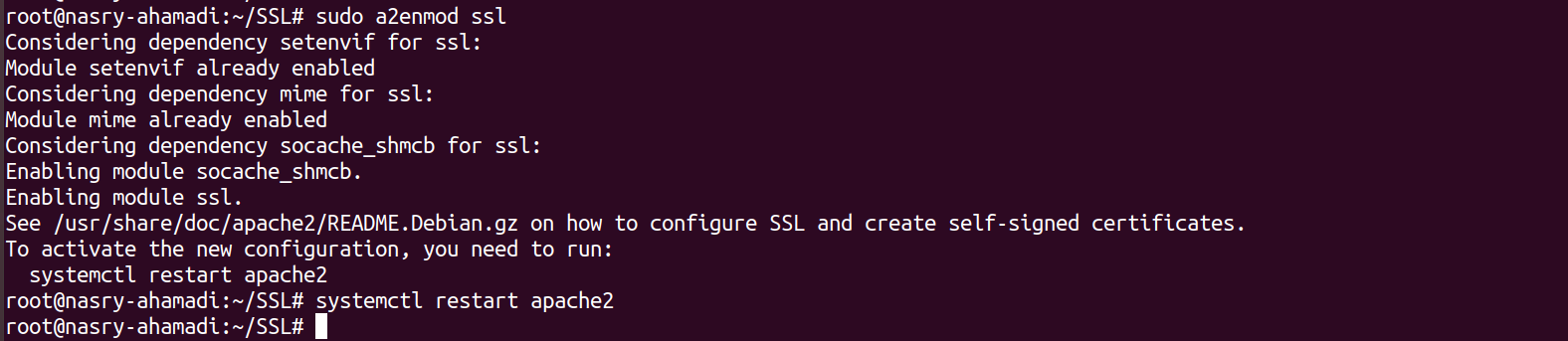


root@nasry-ahamadi:~/SSL# openssl pkcs12 -export -inkey private/berengerKey.key -in newcerts/berengerCert.crt -certfile cacerts/caCert.pem -out pkcs12/berenger.p12

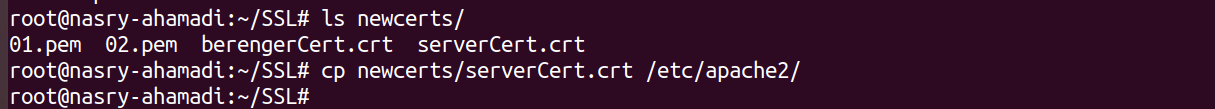


root@nasry-ahamadi:~/SSL# sudo a2enmod ssl

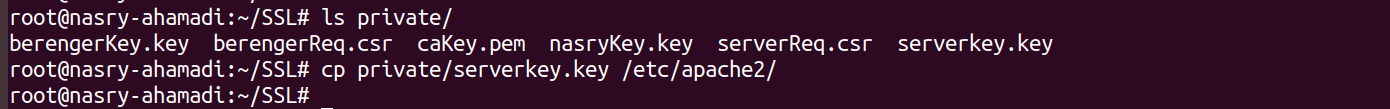
root@nasry-ahamadi:~/SSL# systemctl restart apache2



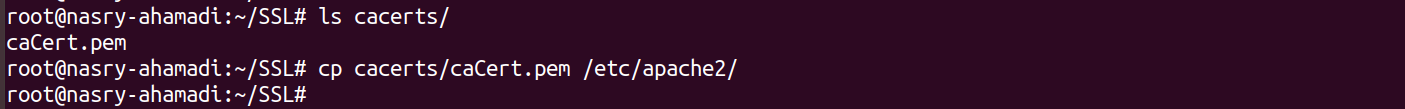
cp newcerts/serverCert.crt /etc/apache2/



root@nasry-ahamadi:~/SSL# cp private/serverkey.key /etc/apache2/



root@nasry-ahamadi:~/SSL# cp cacerts/caCert.pem /etc/apache2/



root@nasry-ahamadi:~/SSL# nano /etc/apache2/sites-available/ssl-site.conf



<VirtualHost \_default\_:443>

ServerName server.test.sn

ServerAlias 192.168.1.15

DocumentRoot /var/www/html/ssl

SSLEngine on

SSLCertificateFile /etc/apache2/serverCert.crt

SSLCertificateKeyFile /etc/apache2/serverkey.key

SSLVerifyClient require

SSLVerifyDepth 10

SSLCACertificateFile /etc/apache2/caCert.pem

</VirtualHost>

root@nasry-ahamadi:~/SSL# a2ensite ssl-site.conf

root@nasry-ahamadi:~/SSL# systemctl reload apache2

