PRACTICA 4

Certificados

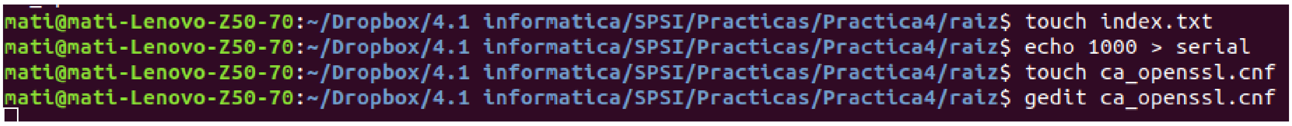
Matilde Cabrera González

Tareas por realizar:

*** (3 puntos) Cread una autoridad certificadora raíz. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.**

En la carpeta de la practica4 me creo un directorio llamado raiz, dentro de este preparo el escenario:

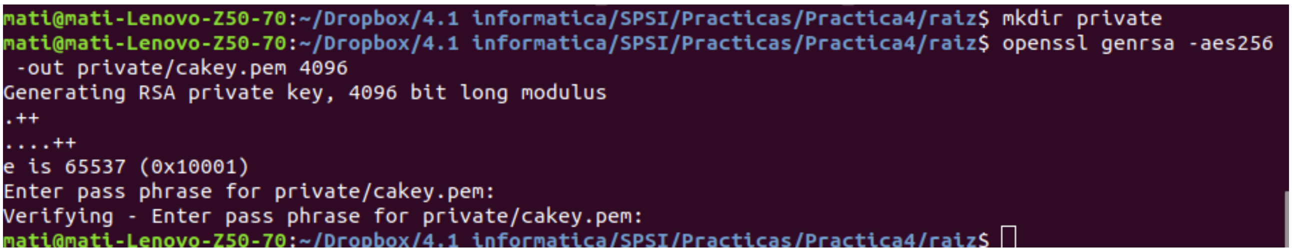
mkdir certs crl newcerts private
touch index.txt
echo 1000 > serial
touch ca_openssl.cnf



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ touch index.txt
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ echo 1000 > serial
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ touch ca_openssl.cnf
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ gedit ca_openssl.cnf
```

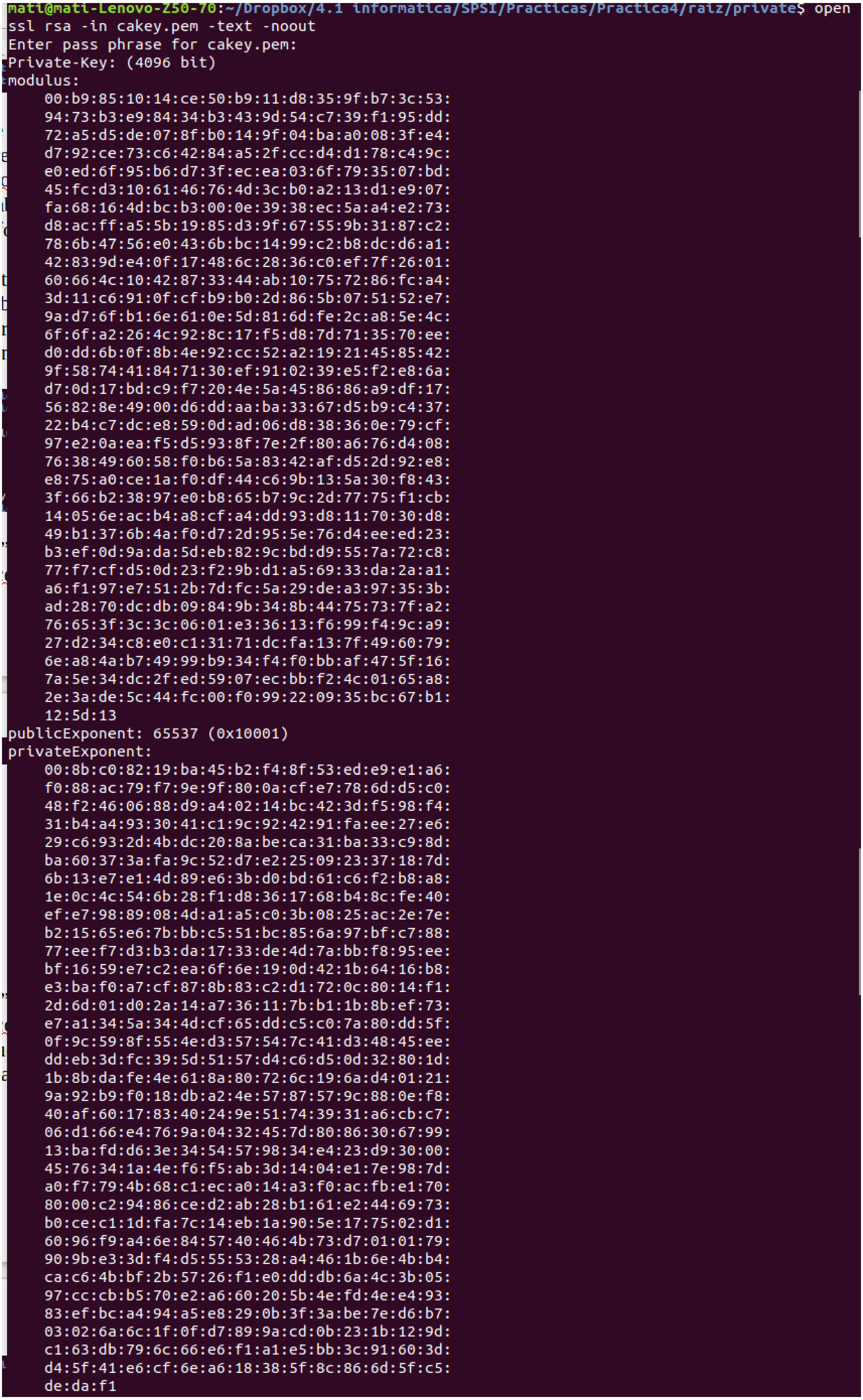
“Index.txt” es el índice de la base de datos para los certificados.
“Serial” es para mantener el numero del siguiente certificado firmado.
“Ca_openssl.cnf”, con “sudo nano ca_openssl.cnf” abro el fichero y copio el fichero “/etc/ssl/openssl.cnf”, abro con gedit y cambiamos el atributo “dir =/home/mati/Dropbox/4.1informatica/SPSI/Practicas/Practica4/raiz”

Creamos clave privada para la entidad certificadora, buscamos en el archivo “ca_openssl.cnf” la variable “private_key= $dir/private/cakey.pem # The private key”, creamos el directorio “private” y la clave privada con el nombre indicado en el documento(cakey.pem):

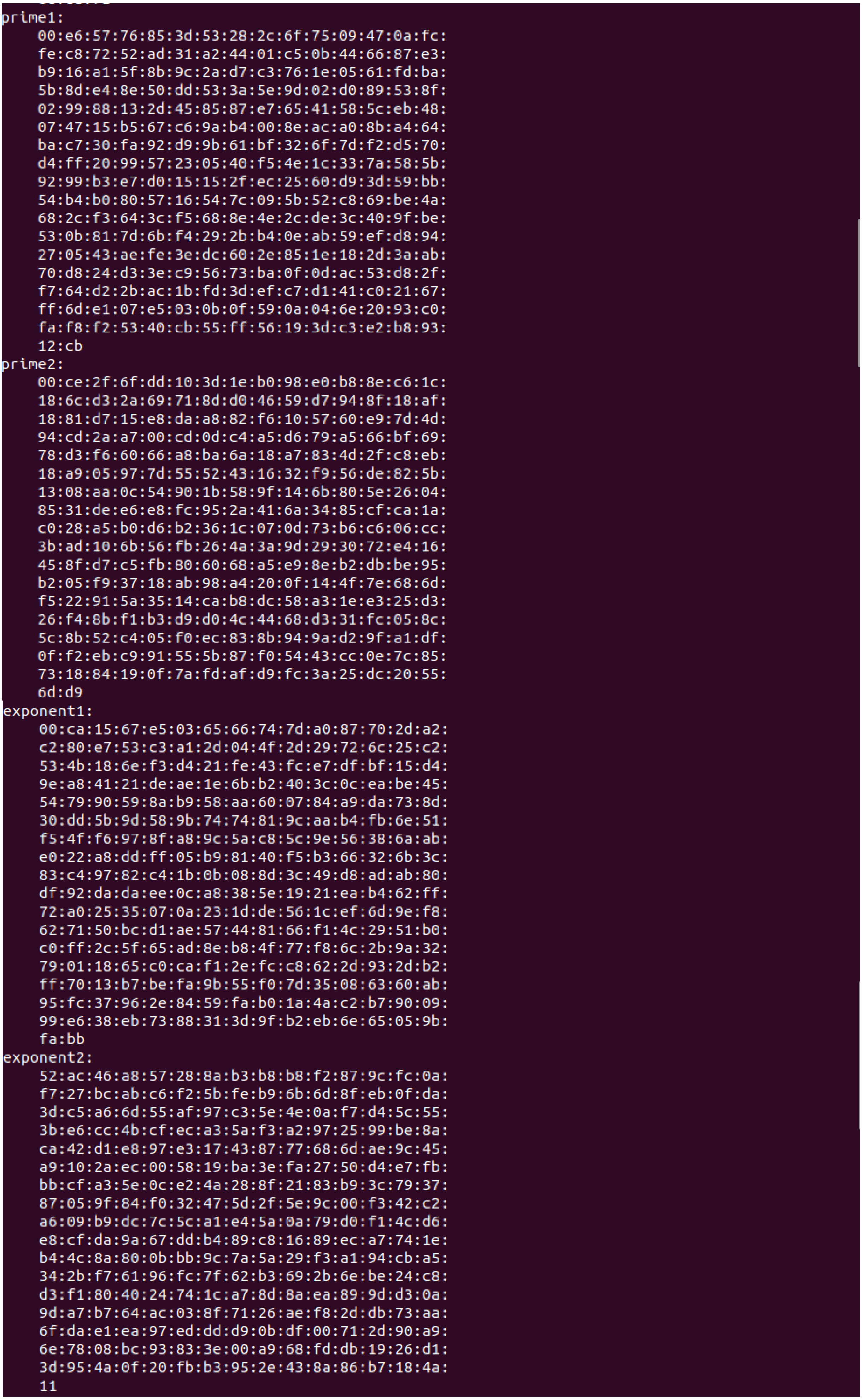


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ mkdir private
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ openssl genrsa -aes256
 -out private/cakey.pem 4096
Generating RSA private key, 4096 bit long modulus
.++
....++
e is 65537 (0x10001)
Enter pass phrase for private/cakey.pem:
Verifying - Enter pass phrase for private/cakey.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

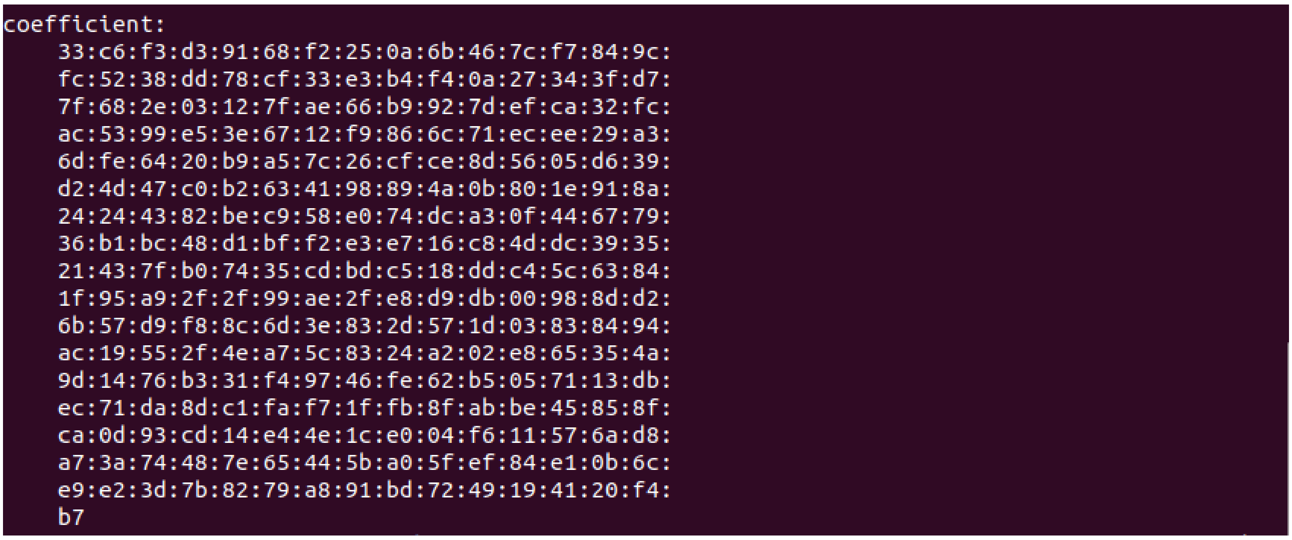
Muestro los datos:



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz/private$ open
ssl rsa -in cakey.pem -text -noout
Enter pass phrase for cakey.pem:
Private-Key: (4096 bit)
modulus:
    00:b9:85:10:14:ce:50:b9:11:d8:35:9f:b7:3c:53:
    94:73:b3:e9:84:34:b3:43:9d:54:c7:39:f1:95:dd:
    72:a5:d5:de:07:8f:b0:14:9f:04:ba:a0:08:3f:e4:
    d7:92:ce:73:c6:42:84:a5:2f:cc:d4:d1:78:c4:9c:
    e0:ed:6f:95:b6:d7:3f:ec:ea:03:6f:79:35:07:bd:
    45:fc:d3:10:61:46:76:4d:3c:b0:a2:13:d1:e9:07:
    fa:68:16:4d:bc:b3:00:0e:39:38:ec:5a:a4:e2:73:
    d8:ac:ff:a5:5b:19:85:d3:9f:67:55:9b:31:87:c2:
    78:6b:47:56:e0:43:6b:bc:14:99:c2:b8:dc:d6:a1:
    42:83:9d:e4:0f:17:48:6c:28:36:c0:ef:7f:26:01:
    60:66:4c:10:42:87:33:44:ab:10:75:72:86:fc:a4:
    3d:11:c6:91:0f:cf:b9:b0:2d:86:5b:07:51:52:e7:
    9a:d7:6f:b1:6e:61:0e:5d:81:6d:fe:2c:a8:5e:4c:
    6f:6f:a2:26:4c:92:8c:17:f5:d8:7d:71:35:70:ee:
    d0:dd:6b:0f:8b:4e:92:cc:52:a2:19:21:45:85:42:
    9f:58:74:41:84:71:30:ef:91:02:39:e5:f2:e8:6a:
    d7:0d:17:bd:c9:f7:20:4e:5a:45:86:86:a9:df:17:
    56:82:8e:49:00:d6:dd:aa:ba:33:67:d5:b9:c4:37:
    22:b4:c7:dc:e8:59:0d:ad:06:d8:38:36:0e:79:cf:
    97:e2:0a:ea:f5:d5:93:8f:7e:2f:80:a6:76:d4:08:
    76:38:49:60:58:f0:b6:5a:83:42:af:d5:2d:92:e8:
    e8:75:a0:ce:1a:f0:df:44:c6:9b:13:5a:30:f8:43:
    3f:66:b2:38:97:e0:b8:65:b7:9c:2d:77:75:f1:cb:
    14:05:6e:ac:b4:a8:cf:a4:dd:93:d8:11:70:30:d8:
    49:b1:37:6b:4a:f0:d7:2d:95:5e:76:d4:ee:ed:23:
    b3:ef:0d:9a:da:5d:eb:82:9c:bd:d9:55:7a:72:c8:
    77:f7:cf:d5:0d:23:f2:9b:d1:a5:69:33:da:2a:a1:
    a6:f1:97:e7:51:2b:7d:fc:5a:29:de:a3:97:35:3b:
    ad:28:70:dc:db:09:84:9b:34:8b:44:75:73:7f:a2:
    76:65:3f:3c:3c:06:01:e3:36:13:f6:99:f4:9c:a9:
    27:d2:34:c8:e0:c1:31:71:dc:fa:13:7f:49:60:79:
    6e:a8:4a:b7:49:99:b9:34:f4:f0:bb:af:47:5f:16:
    7a:5e:34:dc:2f:ed:59:07:ec:bb:f2:4c:01:65:a8:
    2e:3a:de:5c:44:fc:00:f0:99:22:09:35:bc:67:b1:
    12:5d:13
publicExponent: 65537 (0x10001)
privateExponent:
    00:8b:c0:82:19:ba:45:b2:f4:8f:53:ed:e9:e1:a6:
    f0:88:ac:79:f7:9e:9f:80:0a:cf:e7:78:6d:d5:c0:
    48:f2:46:06:88:d9:a4:02:14:bc:42:3d:f5:98:f4:
    31:b4:a4:93:30:41:c1:9c:92:42:91:fa:ee:27:e6:
    29:c6:93:2d:4b:dc:20:8a:be:ca:31:ba:33:c9:8d:
    ba:60:37:3a:fa:9c:52:d7:e2:25:09:23:37:18:7d:
    6b:13:e7:e1:4d:89:e6:3b:d0:bd:61:c6:f2:b8:a8:
    1e:0c:4c:54:6b:28:f1:d8:36:17:68:b4:8c:fe:40:
    ef:e7:98:89:08:4d:a1:a5:c0:3b:08:25:ac:2e:7e:
    b2:15:65:e6:7b:bb:c5:51:bc:85:6a:97:bf:c7:88:
    77:ee:f7:d3:b3:da:17:33:de:4d:7a:bb:f8:95:ee:
    bf:16:59:e7:c2:ea:6f:6e:19:0d:42:1b:64:16:b8:
    e3:ba:f0:a7:cf:87:8b:83:c2:d1:72:0c:80:14:f1:
    2d:6d:01:d0:2a:14:a7:36:11:7b:b1:1b:8b:ef:73:
    e7:a1:34:5a:34:4d:cf:65:dd:c5:c0:7a:80:dd:5f:
    0f:9c:59:8f:55:4e:d3:57:54:7c:41:d3:48:45:ee:
    dd:eb:3d:fc:39:5d:51:57:d4:c6:d5:0d:32:80:1d:
    1b:8b:da:fe:4e:61:8a:80:72:6c:19:6a:d4:01:21:
    9a:92:b9:f0:18:db:a2:4e:57:87:57:9c:88:0e:f8:
    40:af:60:17:83:40:24:9e:51:74:39:31:a6:cb:c7:
    06:d1:66:e4:76:9a:04:32:45:7d:80:86:30:67:99:
    13:ba:fd:d6:3e:34:54:57:98:34:e4:23:d9:30:00:
    45:76:34:1a:4e:f6:f5:ab:3d:14:04:e1:7e:98:7d:
    a0:f7:79:4b:68:c1:ec:a0:14:a3:f0:ac:fb:e1:70:
    80:00:c2:94:86:ce:d2:ab:28:b1:61:e2:44:69:73:
    b0:ce:c1:1d:fa:7c:14:eb:1a:90:5e:17:75:02:d1:
    60:96:f9:a4:6e:84:57:40:46:4b:73:d7:01:01:79:
    90:9b:e3:3d:f4:d5:55:53:28:a4:46:1b:6e:4b:b4:
    ca:c6:4b:bf:2b:57:26:f1:e0:dd:db:6a:4c:3b:05:
    97:cc:cb:b5:70:e2:a6:60:20:5b:4e:fd:4e:e4:93:
    83:ef:bc:a4:94:a5:e8:29:0b:3f:3a:be:7e:d6:b7:
    03:02:6a:6c:1f:0f:d7:89:9a:cd:0b:23:1b:12:9d:
    c1:63:db:79:6c:66:e6:f1:a1:e5:bb:3c:91:60:3d:
    d4:5f:41:e6:cf:6e:a6:18:38:5f:8c:86:6d:5f:c5:
    de:da:f1
```

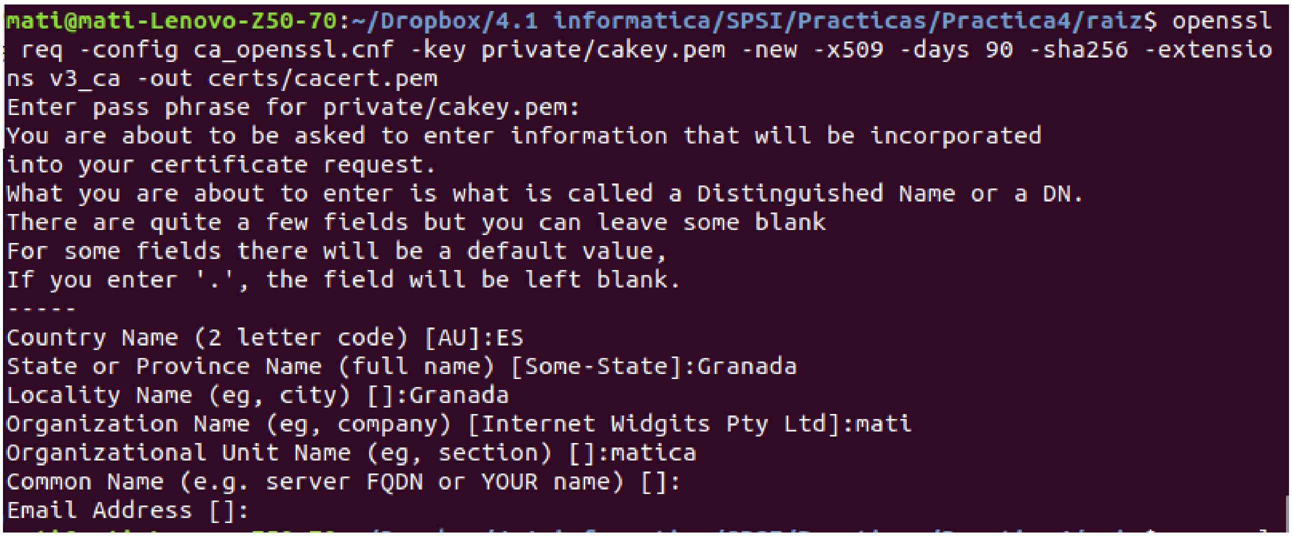


```
prime1:
    00:e6:57:76:85:3d:53:28:2c:6f:75:09:47:0a:fc:
    fe:c8:72:52:ad:31:a2:44:01:c5:0b:44:66:87:e3:
    b9:16:a1:5f:8b:9c:2a:d7:c3:76:1e:05:61:fd:ba:
    5b:8d:e4:8e:50:dd:53:3a:5e:9d:02:d0:89:53:8f:
    02:99:88:13:2d:45:85:87:e7:65:41:58:5c:eb:48:
    07:47:15:b5:67:c6:9a:b4:00:8e:ac:a0:8b:a4:64:
    ba:c7:30:fa:92:d9:9b:61:bf:32:6f:7d:f2:d5:70:
    d4:ff:20:99:57:23:05:40:f5:4e:1c:33:7a:58:5b:
    92:99:b3:e7:d0:15:15:2f:ec:25:60:d9:3d:59:bb:
    54:b4:b0:80:57:16:54:7c:09:5b:52:c8:69:be:4a:
    68:2c:f3:64:3c:f5:68:8e:4e:2c:de:3c:40:9f:be:
    53:0b:81:7d:6b:f4:29:2b:b4:0e:ab:59:ef:d8:94:
    27:05:43:ae:fe:3e:dc:60:2e:85:1e:18:2d:3a:ab:
    70:d8:24:d3:3e:c9:56:73:ba:0f:0d:ac:53:d8:2f:
    f7:64:d2:2b:ac:1b:fd:3d:ef:c7:d1:41:c0:21:67:
    ff:6d:e1:07:e5:03:0b:0f:59:0a:04:6e:20:93:c0:
    fa:f8:f2:53:40:cb:55:ff:56:19:3d:c3:e2:b8:93:
    12:cb
prime2:
    00:ce:2f:6f:dd:10:3d:1e:b0:98:e0:b8:8e:c6:1c:
    18:6c:d3:2a:69:71:8d:d0:46:59:d7:94:8f:18:af:
    18:81:d7:15:e8:da:a8:82:f6:10:57:60:e9:7d:4d:
    94:cd:2a:a7:00:cd:0d:c4:a5:d6:79:a5:66:bf:69:
    78:d3:f6:60:66:a8:ba:6a:18:a7:83:4d:2f:c8:eb:
    18:a9:05:97:7d:55:52:43:16:32:f9:56:de:82:5b:
    13:08:aa:0c:54:90:1b:58:9f:14:6b:80:5e:26:04:
    85:31:de:e6:e8:fc:95:2a:41:6a:34:85:cf:ca:1a:
    c0:28:a5:b0:d6:b2:36:1c:07:0d:73:b6:c6:06:cc:
    3b:ad:10:6b:56:fb:26:4a:3a:9d:29:30:72:e4:16:
    45:8f:d7:c5:fb:80:60:68:a5:e9:8e:b2:db:be:95:
    b2:05:f9:37:18:ab:98:a4:20:0f:14:4f:7e:68:6d:
    f5:22:91:5a:35:14:ca:b8:dc:58:a3:1e:e3:25:d3:
    26:f4:8b:f1:b3:d9:d0:4c:44:68:d3:31:fc:05:8c:
    5c:8b:52:c4:05:f0:ec:83:8b:94:9a:d2:9f:a1:df:
    0f:f2:eb:c9:91:55:5b:87:f0:54:43:cc:0e:7c:85:
    73:18:84:19:0f:7a:fd:af:d9:fc:3a:25:dc:20:55:
    6d:d9
exponent1:
    00:ca:15:67:e5:03:65:66:74:7d:a0:87:70:2d:a2:
    c2:80:e7:53:c3:a1:2d:04:4f:2d:29:72:6c:25:c2:
    53:4b:18:6e:f3:d4:21:fe:43:fc:e7:df:bf:15:d4:
    9e:a8:41:21:de:ae:1e:6b:b2:40:3c:0c:ea:be:45:
    54:79:90:59:8a:b9:58:aa:60:07:84:a9:da:73:8d:
    30:dd:5b:9d:58:9b:74:74:81:9c:aa:b4:fb:6e:51:
    f5:4f:f6:97:8f:a8:9c:5a:c8:5c:9e:56:38:6a:ab:
    e0:22:a8:dd:ff:05:b9:81:40:f5:b3:66:32:6b:3c:
    83:c4:97:82:c4:1b:0b:08:8d:3c:49:d8:ad:ab:80:
    df:92:da:da:ee:0c:a8:38:5e:19:21:ea:b4:62:ff:
    72:a0:25:35:07:0a:23:1d:de:56:1c:ef:6d:9e:f8:
    62:71:50:bc:d1:ae:57:44:81:66:f1:4c:29:51:b0:
    c0:ff:2c:5f:65:ad:8e:b8:4f:77:f8:6c:2b:9a:32:
    79:01:18:65:c0:ca:f1:2e:fc:c8:62:2d:93:2d:b2:
    ff:70:13:b7:be:fa:9b:55:f0:7d:35:08:63:60:ab:
    95:fc:37:96:2e:84:59:fa:b0:1a:4a:c2:b7:90:09:
    99:e6:38:eb:73:88:31:3d:9f:b2:eb:6e:65:05:9b:
    fa:bb
exponent2:
    52:ac:46:a8:57:28:8a:b3:b8:b8:f2:87:9c:fc:0a:
    f7:27:bc:ab:c6:f2:5b:fe:b9:6b:6d:8f:eb:0f:da:
    3d:c5:a6:6d:55:af:97:c3:5e:4e:0a:f7:d4:5c:55:
    3b:e6:cc:4b:cf:ec:a3:5a:f3:a2:97:25:99:be:8a:
    ca:42:d1:e8:97:e3:17:43:87:77:68:6d:ae:9c:45:
    a9:10:2a:ec:00:58:19:ba:3e:fa:27:50:d4:e7:fb:
    bb:cf:a3:5e:0c:e2:4a:28:8f:21:83:b9:3c:79:37:
    87:05:9f:84:f0:32:47:5d:2f:5e:9c:00:f3:42:c2:
    a6:09:b9:dc:7c:5c:a1:e4:5a:0a:79:d0:f1:4c:d6:
    e8:cf:da:9a:67:dd:b4:89:c8:16:89:ec:a7:74:1e:
    b4:4c:8a:80:0b:bb:9c:7a:5a:29:f3:a1:94:cb:a5:
    34:2b:f7:61:96:fc:7f:62:b3:69:2b:6e:be:24:c8:
    d3:f1:80:40:24:74:1c:a7:8d:8a:ea:89:9d:d3:0a:
    9d:a7:b7:64:ac:03:8f:71:26:ae:f8:2d:db:73:aa:
    6f:da:e1:ea:97:ed:dd:d9:0b:df:00:71:2d:90:a9:
    6e:78:08:bc:93:83:3e:00:a9:68:fd:db:19:26:d1:
    3d:95:4a:0f:20:fb:b3:95:2e:43:8a:86:b7:18:4a:
    11
```

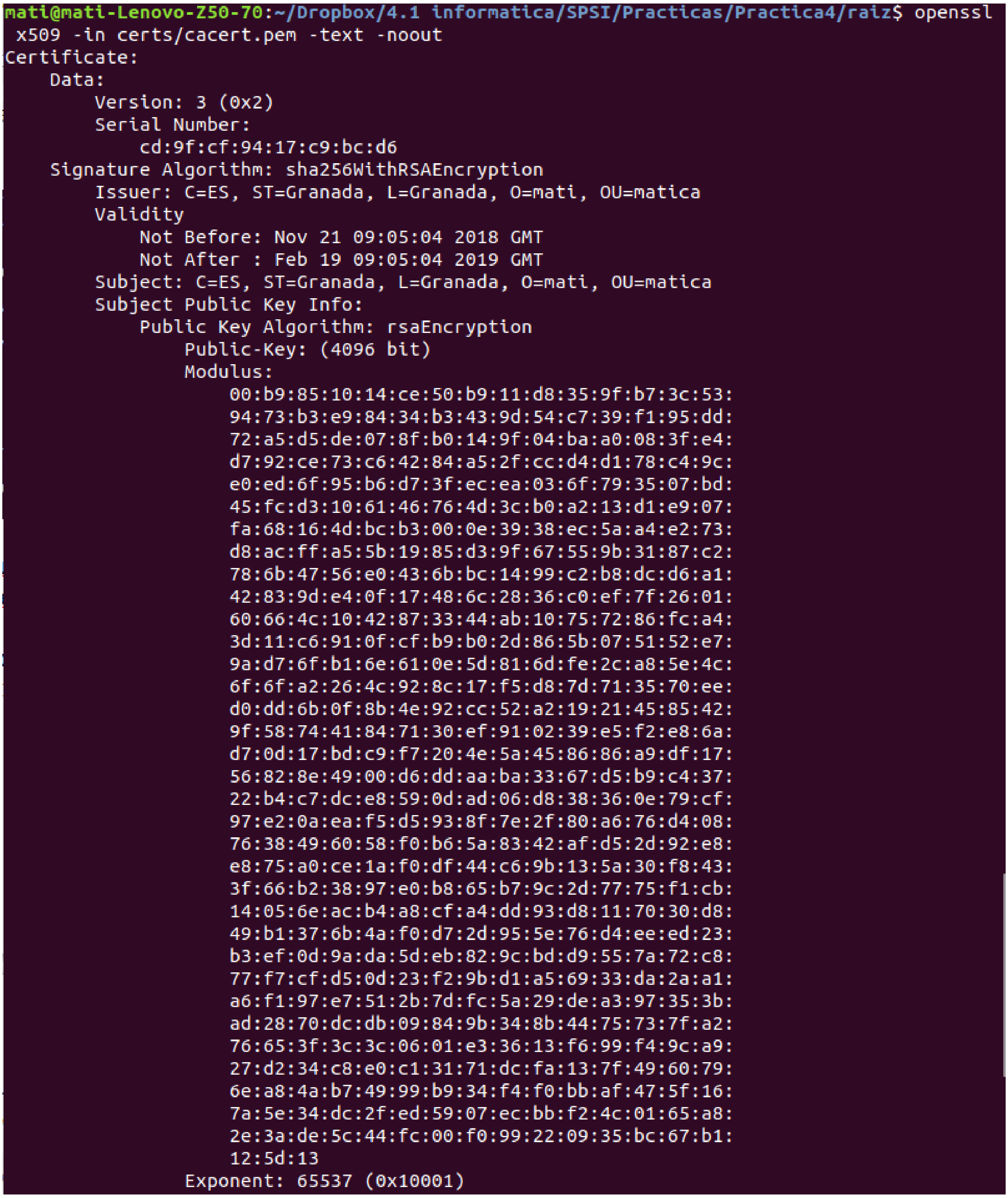


```
coefficient:
    33:c6:f3:d3:91:68:f2:25:0a:6b:46:7c:f7:84:9c:
    fc:52:38:dd:78:cf:33:e3:b4:f4:0a:27:34:3f:d7:
    7f:68:2e:03:12:7f:ae:66:b9:92:7d:ef:ca:32:fc:
    ac:53:99:e5:3e:67:12:f9:86:6c:71:ec:ee:29:a3:
    6d:fe:64:20:b9:a5:7c:26:cf:ce:8d:56:05:d6:39:
    d2:4d:47:c0:b2:63:41:98:89:4a:0b:80:1e:91:8a:
    24:24:43:82:be:c9:58:e0:74:dc:a3:0f:44:67:79:
    36:b1:bc:48:d1:bf:f2:e3:e7:16:c8:4d:dc:39:35:
    21:43:7f:b0:74:35:cd:bd:c5:18:dd:c4:5c:63:84:
    1f:95:a9:2f:2f:99:ae:2f:e8:d9:db:00:98:8d:d2:
    6b:57:d9:f8:8c:6d:3e:83:2d:57:1d:03:83:84:94:
    ac:19:55:2f:4e:a7:5c:83:24:a2:02:e8:65:35:4a:
    9d:14:76:b3:31:f4:97:46:fe:62:b5:05:71:13:db:
    ec:71:da:8d:c1:fa:f7:1f:fb:8f:ab:be:45:85:8f:
    ca:0d:93:cd:14:e4:4e:1c:e0:04:f6:11:57:6a:d8:
    a7:3a:74:48:7e:65:44:5b:a0:5f:ef:84:e1:0b:6c:
    e9:e2:3d:7b:82:79:a8:91:bd:72:49:19:41:20:f4:
    b7
```

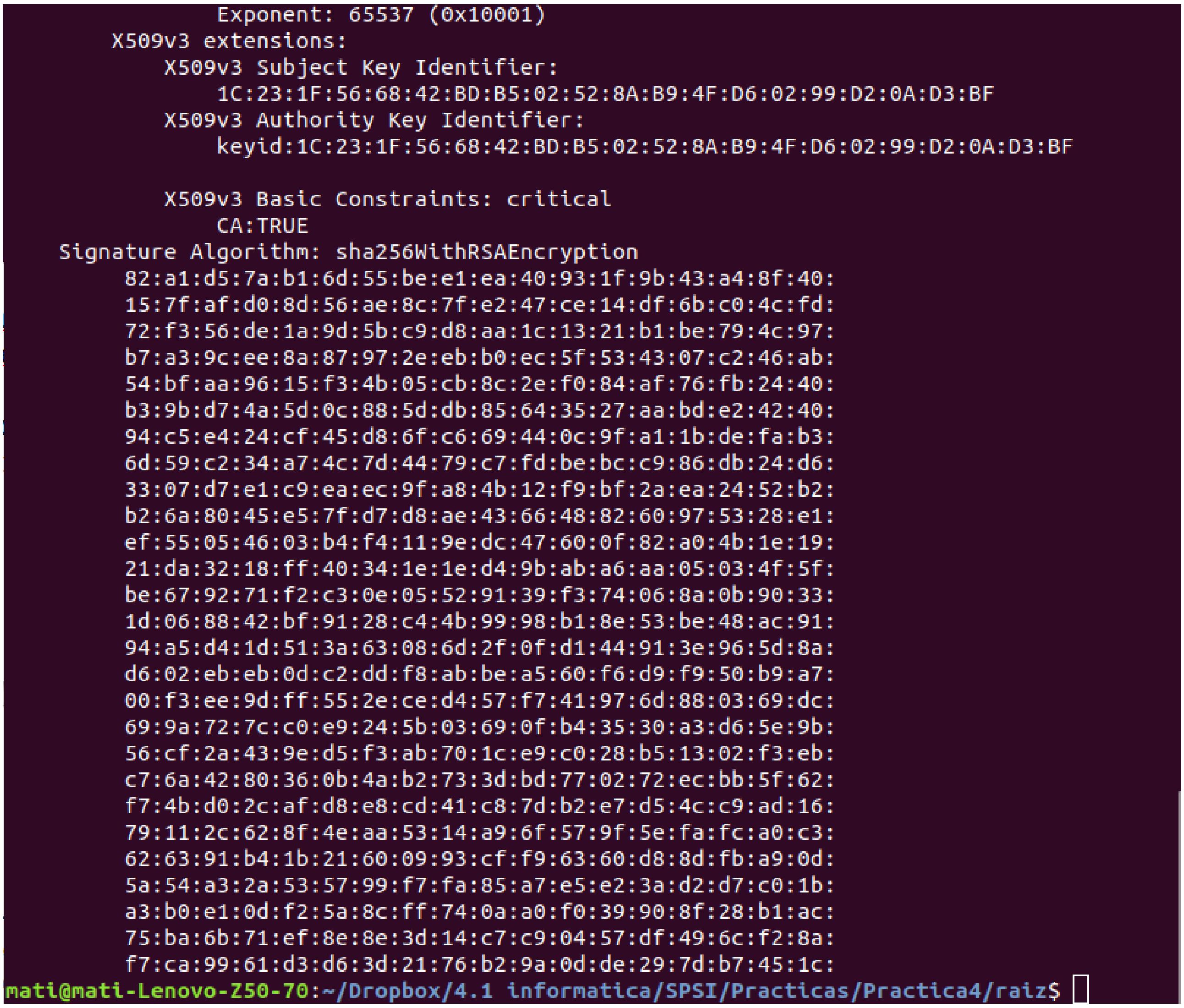
Usamos la clave raíz “cakey.pem” para crear un certificado raíz “certificate = $dir/cacert.pem   # The CA certificate”, le vamos a dar una fecha de caducidad de 3 meses, una vez que expire el certificado raíz, todos los certificados firmados por la entidad emisora no serán válidos:



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ openssl
 req -config ca_openssl.cnf -key private/cakey.pem -new -x509 -days 90 -sha256 -extensio
ns v3_ca -out certs/cacert.pem
Enter pass phrase for private/cakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:mati
Organizational Unit Name (eg, section) []:matica
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ openssl
 x509 -in certs/cacert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cd:9f:cf:94:17:c9:bc:d6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, L=Granada, O=mati, OU=matica
        Validity
            Not Before: Nov 21 09:05:04 2018 GMT
            Not After : Feb 19 09:05:04 2019 GMT
        Subject: C=ES, ST=Granada, L=Granada, O=mati, OU=matica
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b9:85:10:14:ce:50:b9:11:d8:35:9f:b7:3c:53:
                    94:73:b3:e9:84:34:b3:43:9d:54:c7:39:f1:95:dd:
                    72:a5:d5:de:07:8f:b0:14:9f:04:ba:a0:08:3f:e4:
                    d7:92:ce:73:c6:42:84:a5:2f:cc:d4:d1:78:c4:9c:
                    e0:ed:6f:95:b6:d7:3f:ec:ea:03:6f:79:35:07:bd:
                    45:fc:d3:10:61:46:76:4d:3c:b0:a2:13:d1:e9:07:
                    fa:68:16:4d:bc:b3:00:0e:39:38:ec:5a:a4:e2:73:
                    d8:ac:ff:a5:5b:19:85:d3:9f:67:55:9b:31:87:c2:
                    78:6b:47:56:e0:43:6b:bc:14:99:c2:b8:dc:d6:a1:
                    42:83:9d:e4:0f:17:48:6c:28:36:c0:ef:7f:26:01:
                    60:66:4c:10:42:87:33:44:ab:10:75:72:86:fc:a4:
                    3d:11:c6:91:0f:cf:b9:b0:2d:86:5b:07:51:52:e7:
                    9a:d7:6f:b1:6e:61:0e:5d:81:6d:fe:2c:a8:5e:4c:
                    6f:6f:a2:26:4c:92:8c:17:f5:d8:7d:71:35:70:ee:
                    d0:dd:6b:0f:8b:4e:92:cc:52:a2:19:21:45:85:42:
                    9f:58:74:41:84:71:30:ef:91:02:39:e5:f2:e8:6a:
                    d7:0d:17:bd:c9:f7:20:4e:5a:45:86:86:a9:df:17:
                    56:82:8e:49:00:d6:dd:aa:ba:33:67:d5:b9:c4:37:
                    22:b4:c7:dc:e8:59:0d:ad:06:d8:38:36:0e:79:cf:
                    97:e2:0a:ea:f5:d5:93:8f:7e:2f:80:a6:76:d4:08:
                    76:38:49:60:58:f0:b6:5a:83:42:af:d5:2d:92:e8:
                    e8:75:a0:ce:1a:f0:df:44:c6:9b:13:5a:30:f8:43:
                    3f:66:b2:38:97:e0:b8:65:b7:9c:2d:77:75:f1:cb:
                    14:05:6e:ac:b4:a8:cf:a4:dd:93:d8:11:70:30:d8:
                    49:b1:37:6b:4a:f0:d7:2d:95:5e:76:d4:ee:ed:23:
                    b3:ef:0d:9a:da:5d:eb:82:9c:bd:d9:55:7a:72:c8:
                    77:f7:cf:d5:0d:23:f2:9b:d1:a5:69:33:da:2a:a1:
                    a6:f1:97:e7:51:2b:7d:fc:5a:29:de:a3:97:35:3b:
                    ad:28:70:dc:db:09:84:9b:34:8b:44:75:73:7f:a2:
                    76:65:3f:3c:3c:06:01:e3:36:13:f6:99:f4:9c:a9:
                    27:d2:34:c8:e0:c1:31:71:dc:fa:13:7f:49:60:79:
                    6e:a8:4a:b7:49:99:b9:34:f4:f0:bb:af:47:5f:16:
                    7a:5e:34:dc:2f:ed:59:07:ec:bb:f2:4c:01:65:a8:
                    2e:3a:de:5c:44:fc:00:f0:99:22:09:35:bc:67:b1:
                    12:5d:13
                Exponent: 65537 (0x10001)
```

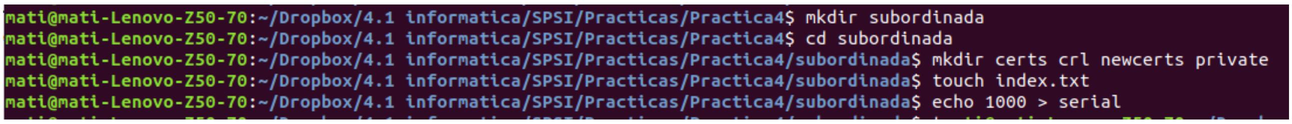


```
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                1C:23:1F:56:68:42:BD:B5:02:52:8A:B9:4F:D6:02:99:D2:0A:D3:BF
            X509v3 Authority Key Identifier:
                keyid:1C:23:1F:56:68:42:BD:B5:02:52:8A:B9:4F:D6:02:99:D2:0A:D3:BF

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         82:a1:d5:7a:b1:6d:55:be:e1:ea:40:93:1f:9b:43:a4:8f:40:
         15:7f:af:d0:8d:56:ae:8c:7f:e2:47:ce:14:df:6b:c0:4c:fd:
         72:f3:56:de:1a:9d:5b:c9:d8:aa:1c:13:21:b1:be:79:4c:97:
         b7:a3:9c:ee:8a:87:97:2e:eb:b0:ec:5f:53:43:07:c2:46:ab:
         54:bf:aa:96:15:f3:4b:05:cb:8c:2e:f0:84:af:76:fb:24:40:
         b3:9b:d7:4a:5d:0c:88:5d:db:85:64:35:27:aa:bd:e2:42:40:
         94:c5:e4:24:cf:45:d8:6f:c6:69:44:0c:9f:a1:1b:de:fa:b3:
         6d:59:c2:34:a7:4c:7d:44:79:c7:fd:be:bc:c9:86:db:24:d6:
         33:07:d7:e1:c9:ea:ec:9f:a8:4b:12:f9:bf:2a:ea:24:52:b2:
         b2:6a:80:45:e5:7f:d7:d8:ae:43:66:48:82:60:97:53:28:e1:
         ef:55:05:46:03:b4:f4:11:9e:dc:47:60:0f:82:a0:4b:1e:19:
         21:da:32:18:ff:40:34:1e:1e:d4:9b:ab:a6:aa:05:03:4f:5f:
         be:67:92:71:f2:c3:0e:05:52:91:39:f3:74:06:8a:0b:90:33:
         1d:06:88:42:bf:91:28:c4:4b:99:98:b1:8e:53:be:48:ac:91:
         94:a5:d4:1d:51:3a:63:08:6d:2f:0f:d1:44:91:3e:96:5d:8a:
         d6:02:eb:eb:0d:c2:dd:f8:ab:be:a5:60:f6:d9:f9:50:b9:a7:
         00:f3:ee:9d:ff:55:2e:ce:d4:57:f7:41:97:6d:88:03:69:dc:
         69:9a:72:7c:c0:e9:24:5b:03:69:0f:b4:35:30:a3:d6:5e:9b:
         56:cf:2a:43:9e:d5:f3:ab:70:1c:e9:c0:28:b5:13:02:f3:eb:
         c7:6a:42:80:36:0b:4a:b2:73:3d:bd:77:02:72:ec:bb:5f:62:
         f7:4b:d0:2c:af:d8:e8:cd:41:c8:7d:b2:e7:d5:4c:c9:ad:16:
         79:11:2c:62:8f:4e:aa:53:14:a9:6f:57:9f:5e:fa:fc:a0:c3:
         62:63:91:b4:1b:21:60:09:93:cf:f9:63:60:d8:8d:fb:a9:0d:
         5a:54:a3:2a:53:57:99:f7:fa:85:a7:e5:e2:3a:d2:d7:c0:1b:
         a3:b0:e1:0d:f2:5a:8c:ff:74:0a:a0:f0:39:90:8f:28:b1:ac:
         75:ba:6b:71:ef:8e:8e:3d:14:c7:c9:04:57:df:49:6c:f2:8a:
         f7:ca:99:61:d3:d6:3d:21:76:b2:9a:0d:de:29:7d:b7:45:1c:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ 
```

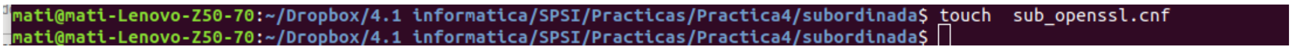
*** (1 punto) Cread una autoridad certificadora subordinada a la anterior. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.**

Preparamos el escenario:

```
mkdir subordinada
cd subordinada
mkdir certs crl newcerts private
touch index.txt
echo 1000 > serial
touch  sub_openssl.cnf
```

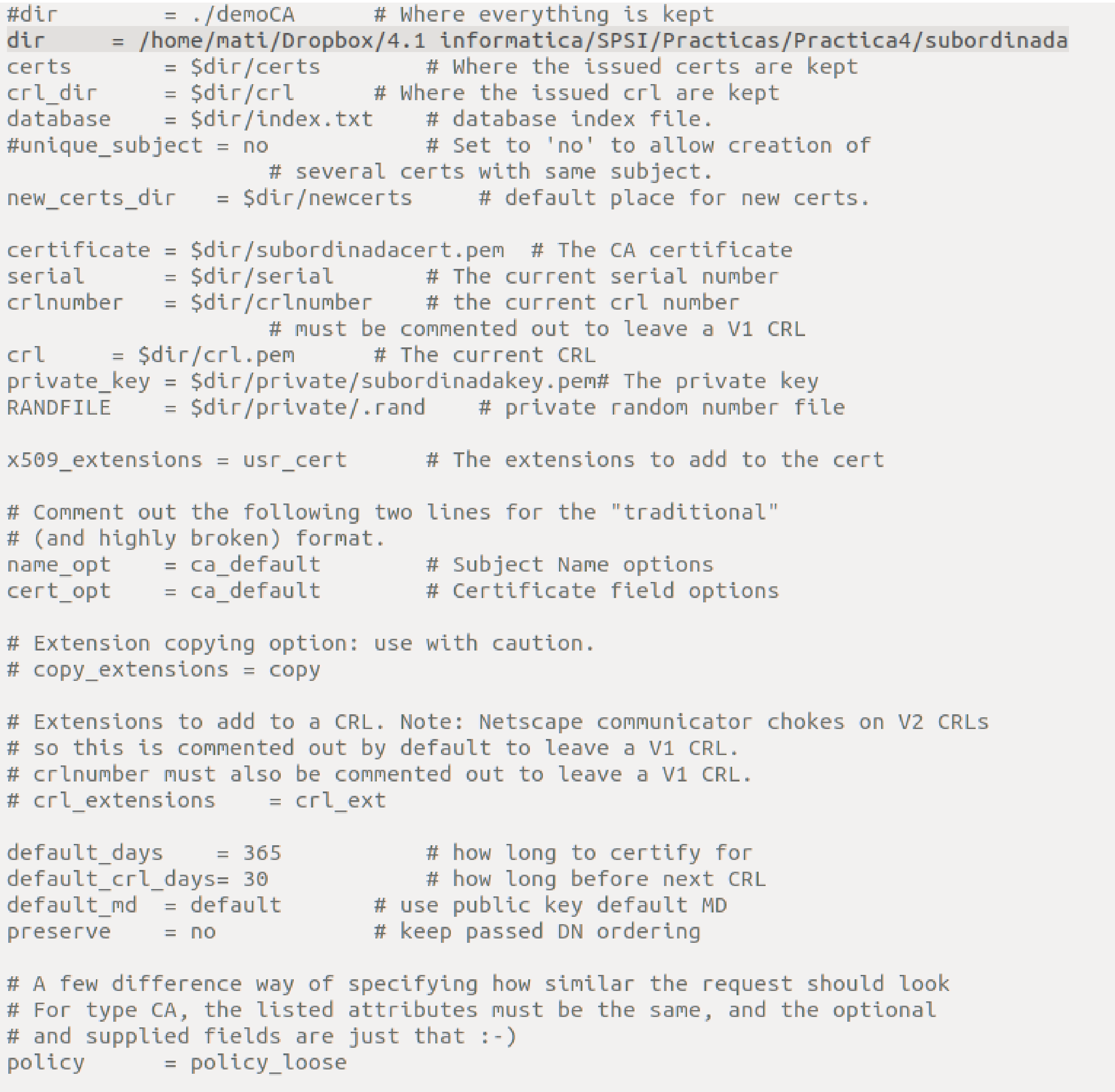


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4$ mkdir subordinada
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4$ cd subordinada
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ mkdir certs crl newcerts private
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ touch index.txt
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ echo 1000 > serial
```



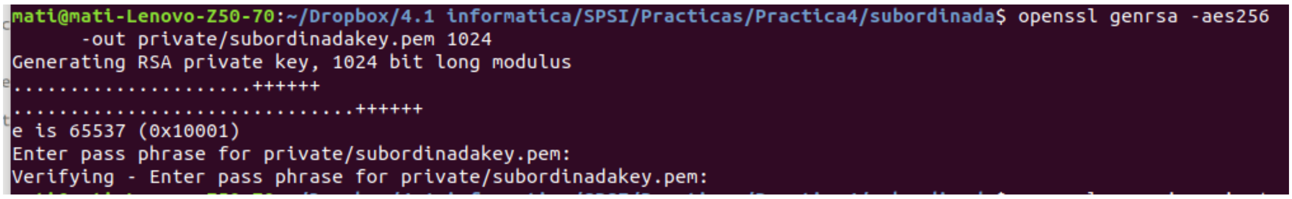
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ touch  sub_openssl.cnf
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ 
```

Del archivo sub_openssl.cnf cambiamos:
dir= /home/mati/.../Practica4/subordinada
certificate = $dir/subordinadacert.pem
private_key   = $dir/private/subordinadakey.pem
policy   = policy_loose



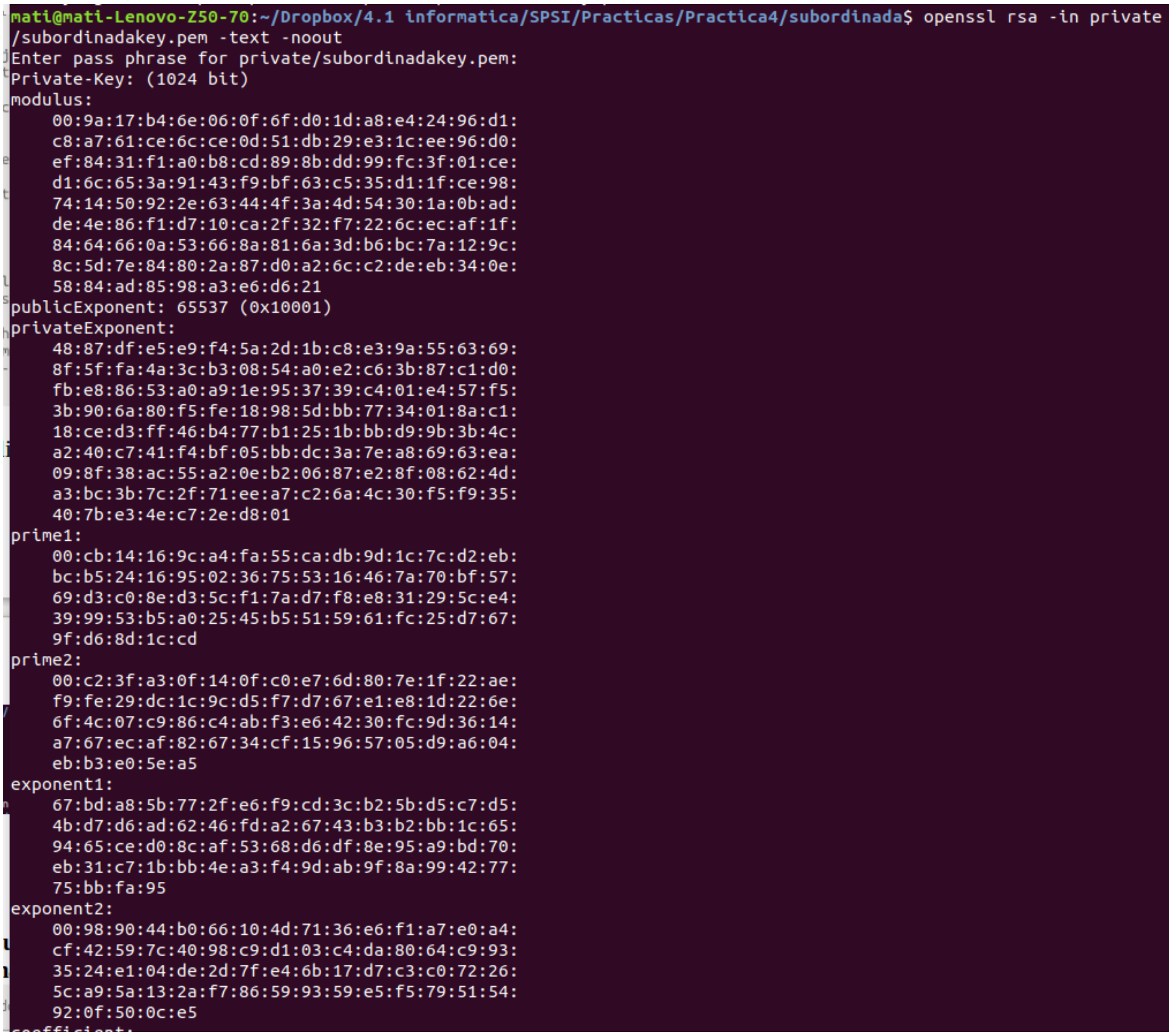
```
#dir		= ./demoCA		# Where everything is kept
dir	= /home/mati/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada
certs		= $dir/certs		# Where the issued certs are kept
crl_dir		= $dir/crl		# Where the issued crl are kept
database	= $dir/index.txt	# database index file.
#unique_subject	= no			# Set to 'no' to allow creation of
					# several certs with same subject.
new_certs_dir	= $dir/newcerts		# default place for new certs.

certificate	= $dir/subordinadacert.pem 	# The CA certificate
serial		= $dir/serial 		# The current serial number
crlnumber	= $dir/crlnumber	# the current crl number
					# must be commented out to leave a V1 CRL
crl		= $dir/crl.pem 		# The current CRL
private_key	= $dir/private/subordinadakey.pem# The private key
RANDFILE	= $dir/private/.rand	# private random number file

x509_extensions	= usr_cert		# The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt 	= ca_default		# Subject Name options
cert_opt 	= ca_default		# Certificate field options

# Extension copying option: use with caution.
# copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions	= crl_ext

default_days	= 365			# how long to certify for
default_crl_days= 30			# how long before next CRL
default_md	= default		# use public key default MD
preserve	= no			# keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy		= policy_loose
```

Creamos la clave primada subordinada:

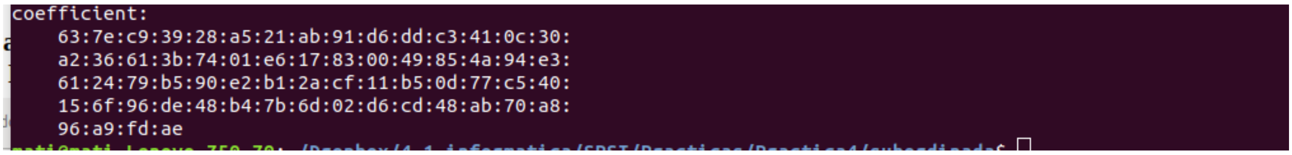


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ openssl genrsa -aes256
     -out private/subordinadakey.pem 1024
Generating RSA private key, 1024 bit long modulus
.....................++++++
..............................++++++
e is 65537 (0x10001)
Enter pass phrase for private/subordinadakey.pem:
Verifying - Enter pass phrase for private/subordinadakey.pem:
```

Muestro los datos de la clave creada:

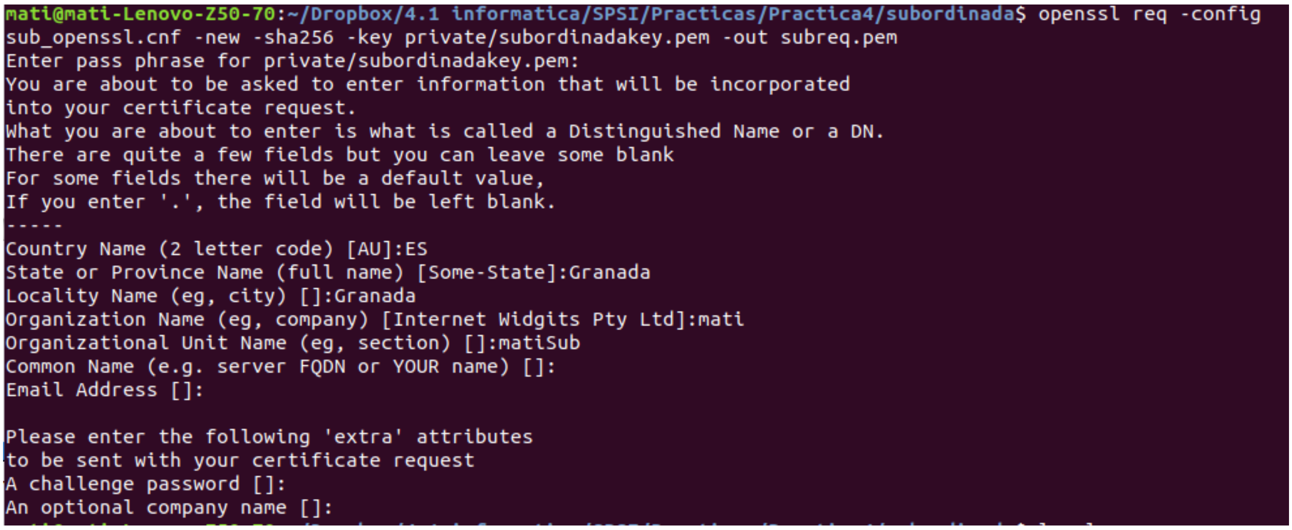


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ openssl rsa -in private
/subordinadakey.pem -text -noout
Enter pass phrase for private/subordinadakey.pem:
Private-Key: (1024 bit)
modulus:
    00:9a:17:b4:6e:06:0f:6f:d0:1d:a8:e4:24:96:d1:
    c8:a7:61:ce:6c:ce:0d:51:db:29:e3:1c:ee:96:d0:
    ef:84:31:f1:a0:b8:cd:89:8b:dd:99:fc:3f:01:ce:
    d1:6c:65:3a:91:43:f9:bf:63:c5:35:d1:1f:ce:98:
    74:14:50:92:2e:63:44:4f:3a:4d:54:30:1a:0b:ad:
    de:4e:86:f1:d7:10:ca:2f:32:f7:22:6c:ec:af:1f:
    84:64:66:0a:53:66:8a:81:6a:3d:b6:bc:7a:12:9c:
    8c:5d:7e:84:80:2a:87:d0:a2:6c:c2:de:eb:34:0e:
    58:84:ad:85:98:a3:e6:d6:21
publicExponent: 65537 (0x10001)
privateExponent:
    48:87:df:e5:e9:f4:5a:2d:1b:c8:e3:9a:55:63:69:
    8f:5f:fa:4a:3c:b3:08:54:a0:e2:c6:3b:87:c1:d0:
    fb:e8:86:53:a0:a9:1e:95:37:39:c4:01:e4:57:f5:
    3b:90:6a:80:f5:fe:18:98:5d:bb:77:34:01:8a:c1:
    18:ce:d3:ff:46:b4:77:b1:25:1b:bb:d9:9b:3b:4c:
    a2:40:c7:41:f4:bf:05:bb:dc:3a:7e:a8:69:63:ea:
    09:8f:38:ac:55:a2:0e:b2:06:87:e2:8f:08:62:4d:
    a3:bc:3b:7c:2f:71:ee:a7:c2:6a:4c:30:f5:f9:35:
    40:7b:e3:4e:c7:2e:d8:01
prime1:
    00:cb:14:16:9c:a4:fa:55:ca:db:9d:1c:7c:d2:eb:
    bc:b5:24:16:95:02:36:75:53:16:46:7a:70:bf:57:
    69:d3:c0:8e:d3:5c:f1:7a:d7:f8:e8:31:29:5c:e4:
    39:99:53:b5:a0:25:45:b5:51:59:61:fc:25:d7:67:
    9f:d6:8d:1c:cd
prime2:
    00:c2:3f:a3:0f:14:0f:c0:e7:6d:80:7e:1f:22:ae:
    f9:fe:29:dc:1c:9c:d5:f7:d7:67:e1:e8:1d:22:6e:
    6f:4c:07:c9:86:c4:ab:f3:e6:42:30:fc:9d:36:14:
    a7:67:ec:af:82:67:34:cf:15:96:57:05:d9:a6:04:
    eb:b3:e0:5e:a5
exponent1:
    67:bd:a8:5b:77:2f:e6:f9:cd:3c:b2:5b:d5:c7:d5:
    4b:d7:d6:ad:62:46:fd:a2:67:43:b3:b2:bb:1c:65:
    94:65:ce:d0:8c:af:53:68:d6:df:8e:95:a9:bd:70:
    eb:31:c7:1b:bb:4e:a3:f4:9d:ab:9f:8a:99:42:77:
    75:bb:fa:95
exponent2:
    00:98:90:44:b0:66:10:4d:71:36:e6:f1:a7:e0:a4:
    cf:42:59:7c:40:98:c9:d1:03:c4:da:80:64:c9:93:
    35:24:e1:04:de:2d:7f:e4:6b:17:d7:c3:c0:72:26:
    5c:a9:5a:13:2a:f7:86:59:93:59:e5:f5:79:51:54:
    92:0f:50:0c:e5
```



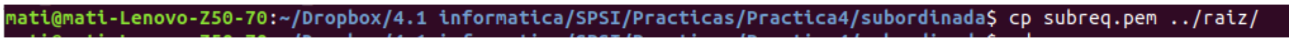
```
coefficient:
    63:7e:c9:39:28:a5:21:ab:91:d6:dd:c3:41:0c:30:
    a2:36:61:3b:74:01:e6:17:83:00:49:85:4a:94:e3:
    61:24:79:b5:90:e2:b1:2a:cf:11:b5:0d:77:c5:40:
    15:6f:96:de:48:b4:7b:6d:02:d6:cd:48:ab:70:a8:
    96:a9:fd:ae
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ 
```

Creo el certificado subordinado:



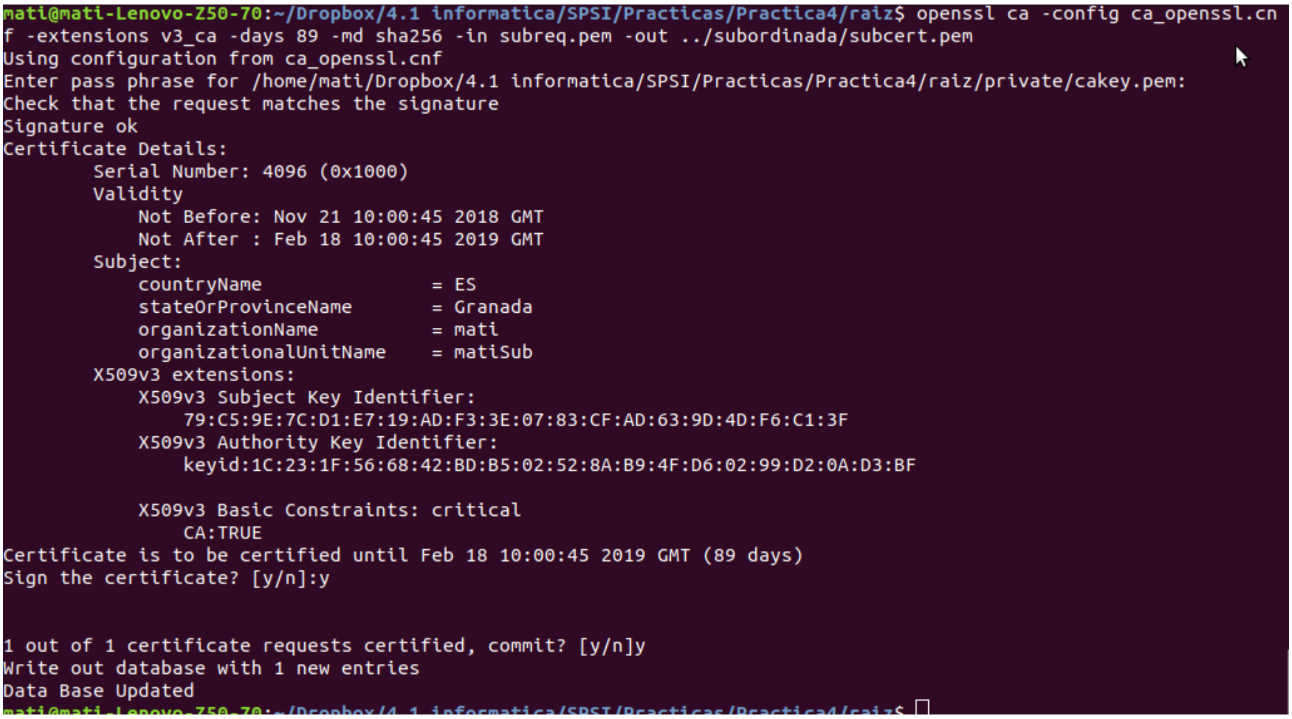
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ openssl req -config
sub_openssl.cnf -new -sha256 -key private/subordinadakey.pem -out subreq.pem
Enter pass phrase for private/subordinadakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:mati
Organizational Unit Name (eg, section) []:matiSub
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Copio el certificado subordinado en la carpeta raíz para firmarlo con el certificado raiz:



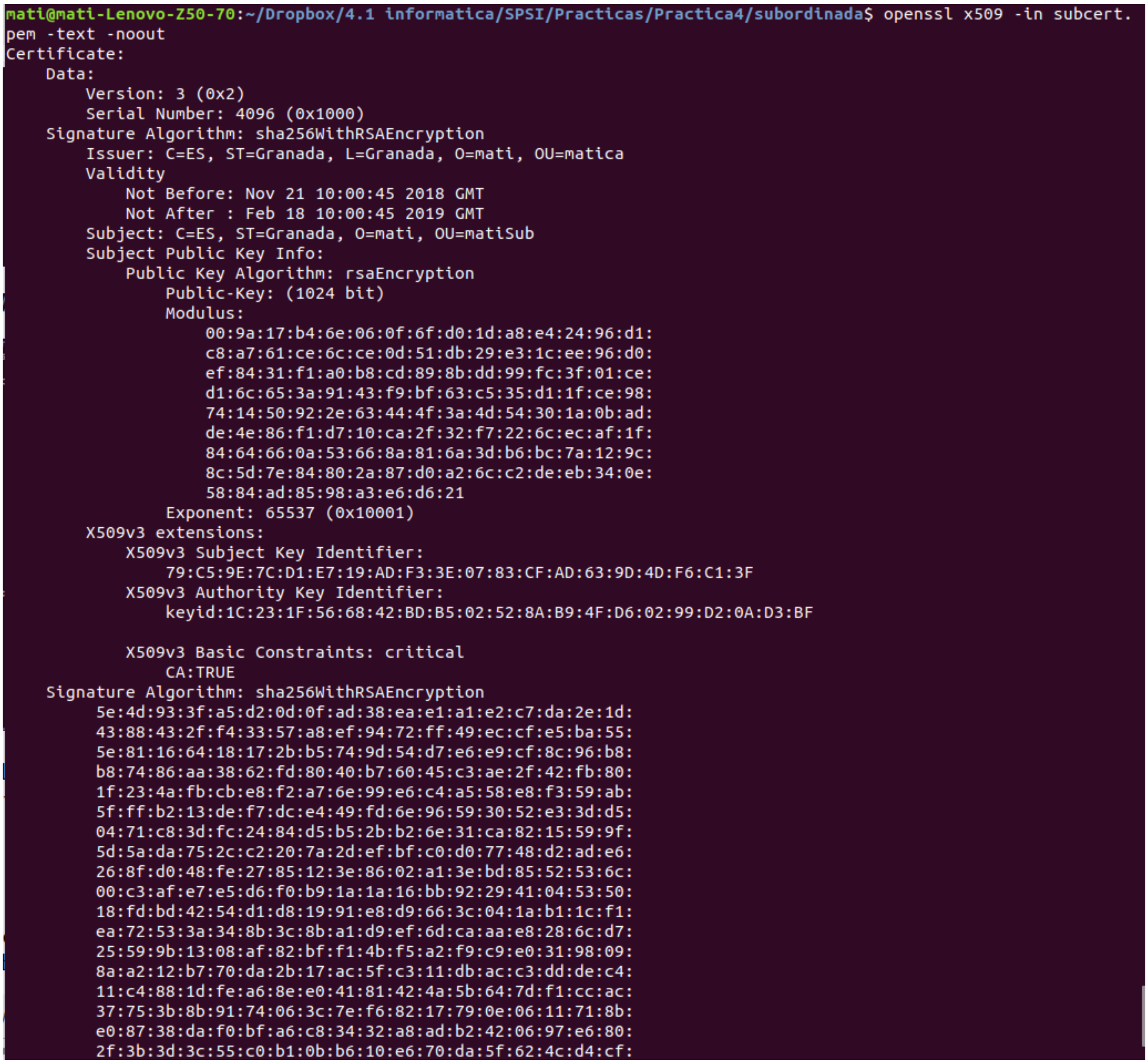
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ cp subreq.pem ../raiz/
```

Usamos la entidad emisora raíz para firmar el certificado subordinado:



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$ openssl ca -config ca_openssl.cn
f -extensions v3_ca -days 89 -md sha256 -in subreq.pem -out ../subordinada/subcert.pem
Using configuration from ca_openssl.cnf
Enter pass phrase for /home/mati/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 21 10:00:45 2018 GMT
            Not After : Feb 18 10:00:45 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = mati
            organizationalUnitName    = matiSub
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3F
            X509v3 Authority Key Identifier:
                keyid:1C:23:1F:56:68:42:BD:B5:02:52:8A:B9:4F:D6:02:99:D2:0A:D3:BF

            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Feb 18 10:00:45 2019 GMT (89 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

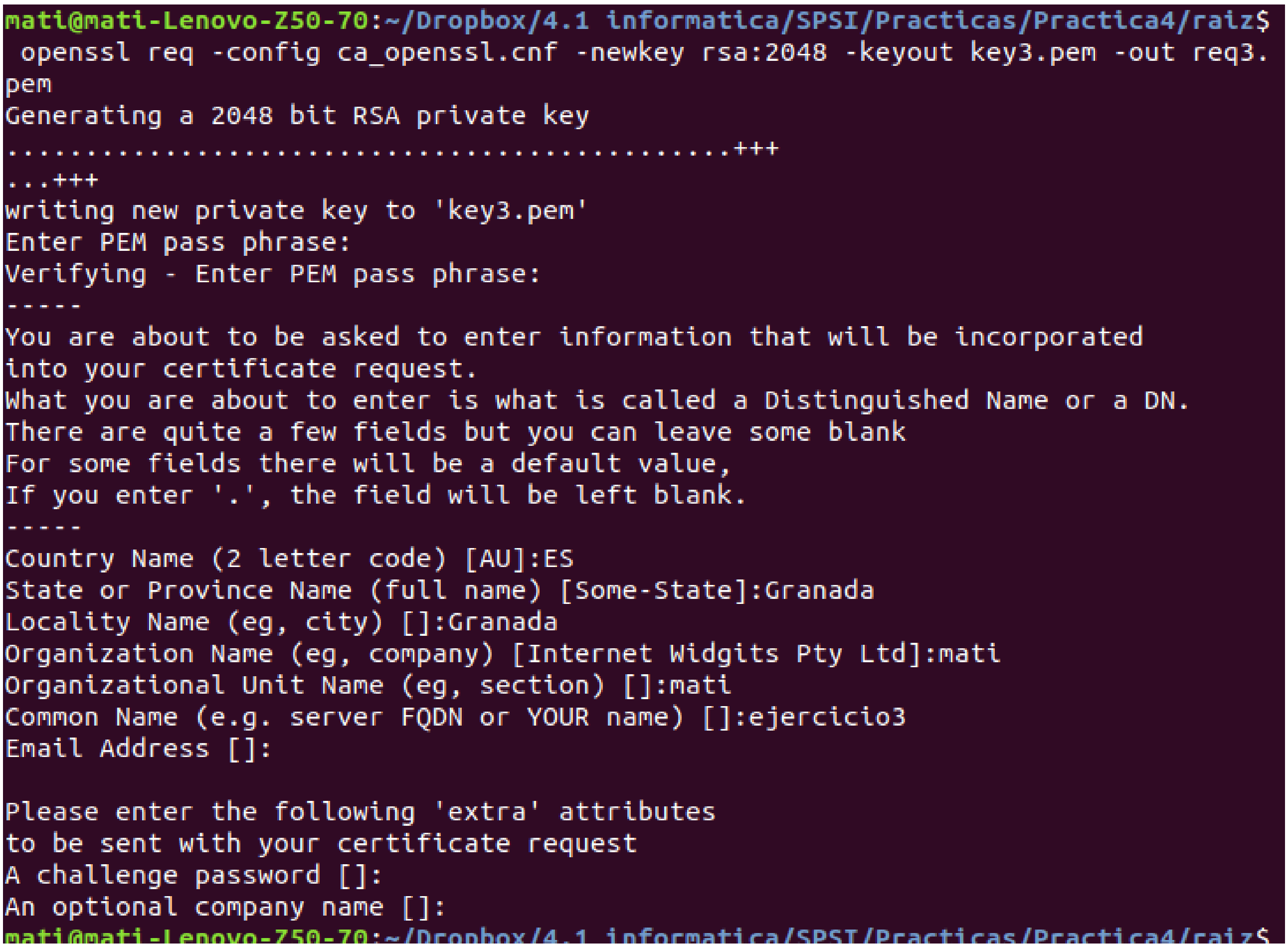
Muestro los valores del certificado subordinado generado.



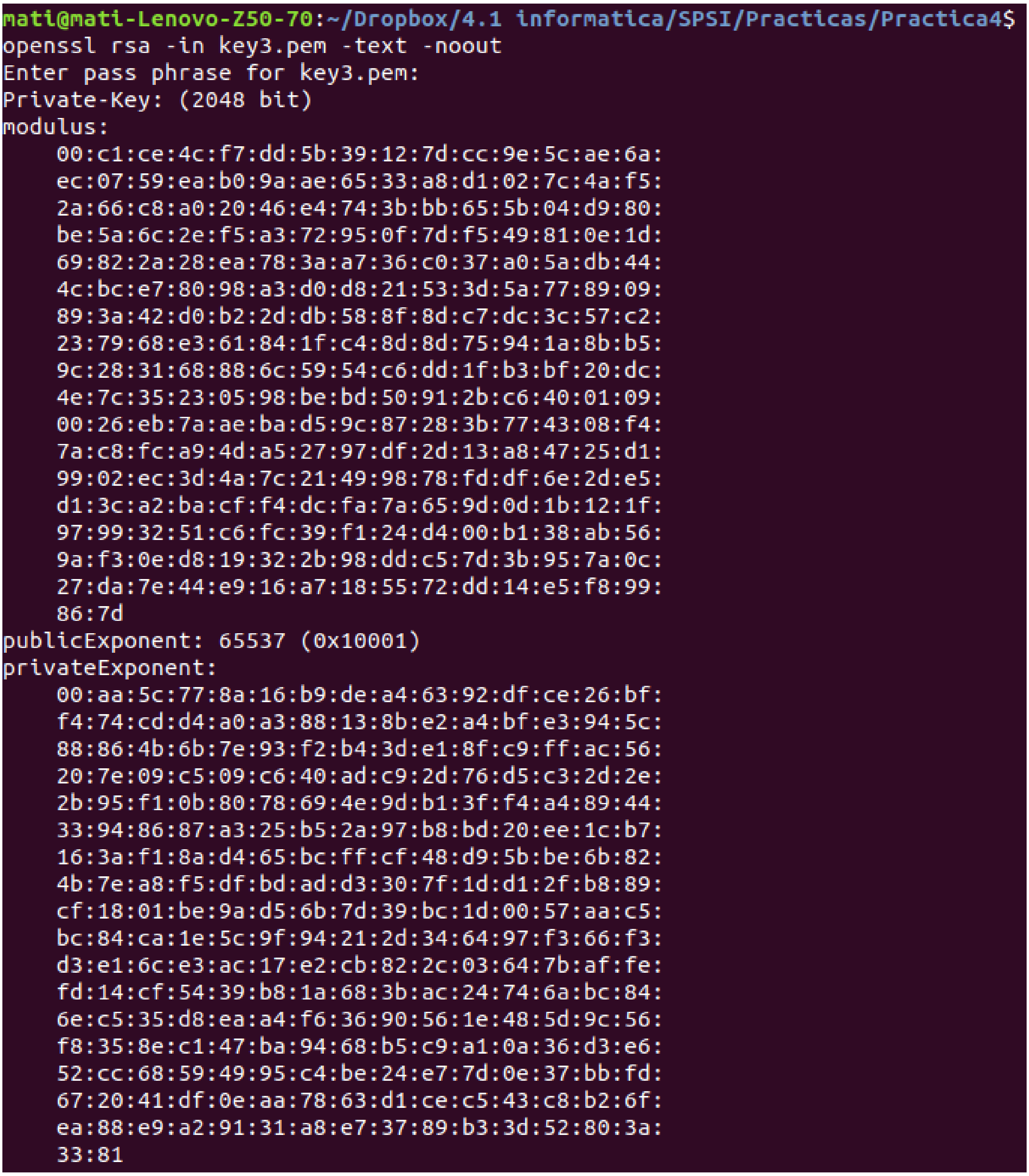
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/subordinada$ openssl x509 -in subcert.
pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, L=Granada, O=mati, OU=matica
        Validity
            Not Before: Nov 21 10:00:45 2018 GMT
            Not After : Feb 18 10:00:45 2019 GMT
        Subject: C=ES, ST=Granada, O=mati, OU=matiSub
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9a:17:b4:6e:06:0f:6f:d0:1d:a8:e4:24:96:d1:
                    c8:a7:61:ce:6c:ce:0d:51:db:29:e3:1c:ee:96:d0:
                    ef:84:31:f1:a0:b8:cd:89:8b:dd:99:fc:3f:01:ce:
                    d1:6c:65:3a:91:43:f9:bf:63:c5:35:d1:1f:ce:98:
                    74:14:50:92:2e:63:44:4f:3a:4d:54:30:1a:0b:ad:
                    de:4e:86:f1:d7:10:ca:2f:32:f7:22:6c:ec:af:1f:
                    84:64:66:0a:53:66:8a:81:6a:3d:b6:bc:7a:12:9c:
                    8c:5d:7e:84:80:2a:87:d0:a2:6c:c2:de:eb:34:0e:
                    58:84:ad:85:98:a3:e6:d6:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3F
            X509v3 Authority Key Identifier:
                keyid:1C:23:1F:56:68:42:BD:B5:02:52:8A:B9:4F:D6:02:99:D2:0A:D3:BF

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         5e:4d:93:3f:a5:d2:0d:0f:ad:38:ea:e1:a1:e2:c7:da:2e:1d:
         43:88:43:2f:f4:33:57:a8:ef:94:72:ff:49:ec:cf:e5:ba:55:
         5e:81:16:64:18:17:2b:b5:74:9d:54:d7:e6:e9:cf:8c:96:b8:
         b8:74:86:aa:38:62:fd:80:40:b7:60:45:c3:ae:2f:42:fb:80:
         1f:23:4a:fb:cb:e8:f2:a7:6e:99:e6:c4:a5:58:e8:f3:59:ab:
         5f:ff:b2:13:de:f7:dc:e4:49:fd:6e:96:59:30:52:e3:3d:d5:
         04:71:c8:3d:fc:24:84:d5:b5:2b:b2:6e:31:ca:82:15:59:9f:
         5d:5a:da:75:2c:c2:20:7a:2d:ef:bf:c0:d0:77:48:d2:ad:e6:
         26:8f:d0:48:fe:27:85:12:3e:86:02:a1:3e:bd:85:52:53:6c:
         00:c3:af:e7:e5:d6:f0:b9:1a:1a:16:bb:92:29:41:04:53:50:
         18:fd:bd:42:54:d1:d8:19:91:e8:d9:66:3c:04:1a:b1:1c:f1:
         ea:72:53:3a:34:8b:3c:8b:a1:d9:ef:6d:ca:aa:e8:28:6c:d7:
         25:59:9b:13:08:af:82:bf:f1:4b:f5:a2:f9:c9:e0:31:98:09:
         8a:a2:12:b7:70:da:2b:17:ac:5f:c3:11:db:ac:c3:dd:de:c4:
         11:c4:88:1d:fe:a6:8e:e0:41:81:42:4a:5b:64:7d:f1:cc:ac:
         37:75:3b:8b:91:74:06:3c:7e:f6:82:17:79:0e:06:11:71:8b:
         e0:87:38:da:f0:bf:a6:c8:34:32:a8:ad:b2:42:06:97:e6:80:
         2f:3b:3d:3c:55:c0:b1:0b:b6:10:e6:70:da:5f:62:4c:d4:cf:
```

* (1,5 puntos) Cread una solicitud de certificado que incluya la generación de claves en la misma. Mostrad los valores junto con el archivo.

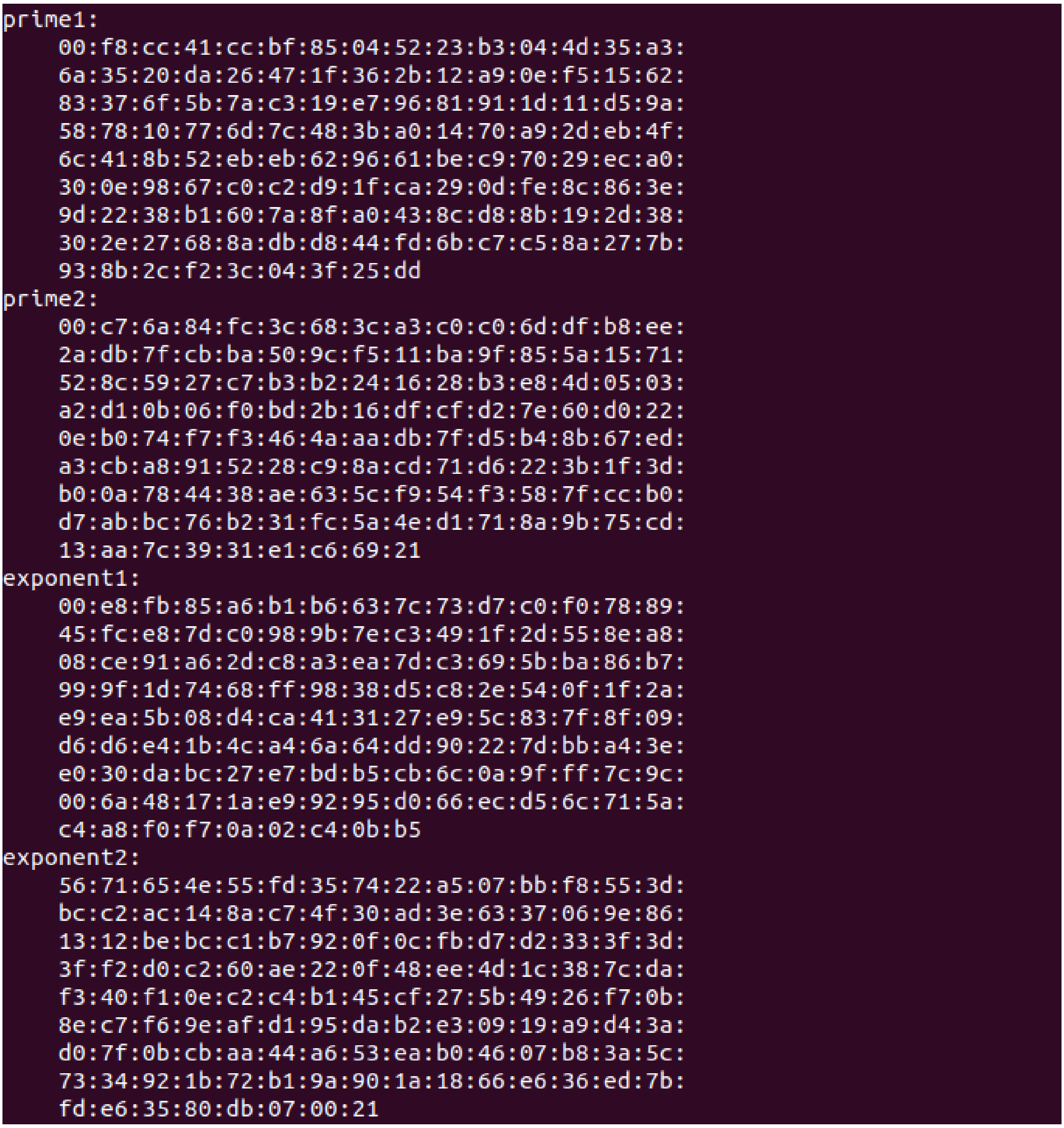
Para este ejercicio se crea la clave privada y se genera la solicitud de certificado a partir de ella.
La clave generada es key3.pem
La solicitud del certificado lo guardamos en req3.pem
Generado en el directorio de la practica 4, en raiz.
openssl req -config ca_openssl.cnf -newkey rsa:2048 -keyout key3.pem -out req3.pem



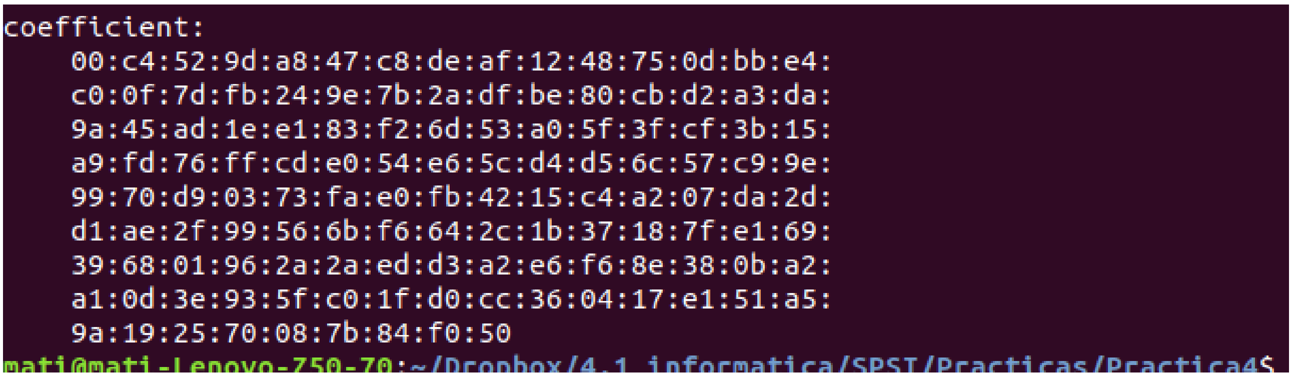
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl req -config ca_openssl.cnf -newkey rsa:2048 -keyout key3.pem -out req3.
pem
Generating a 2048 bit RSA private key
...............................................+++
...+++
writing new private key to 'key3.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:mati
Organizational Unit Name (eg, section) []:mati
Common Name (e.g. server FQDN or YOUR name) []:ejercicio3
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```



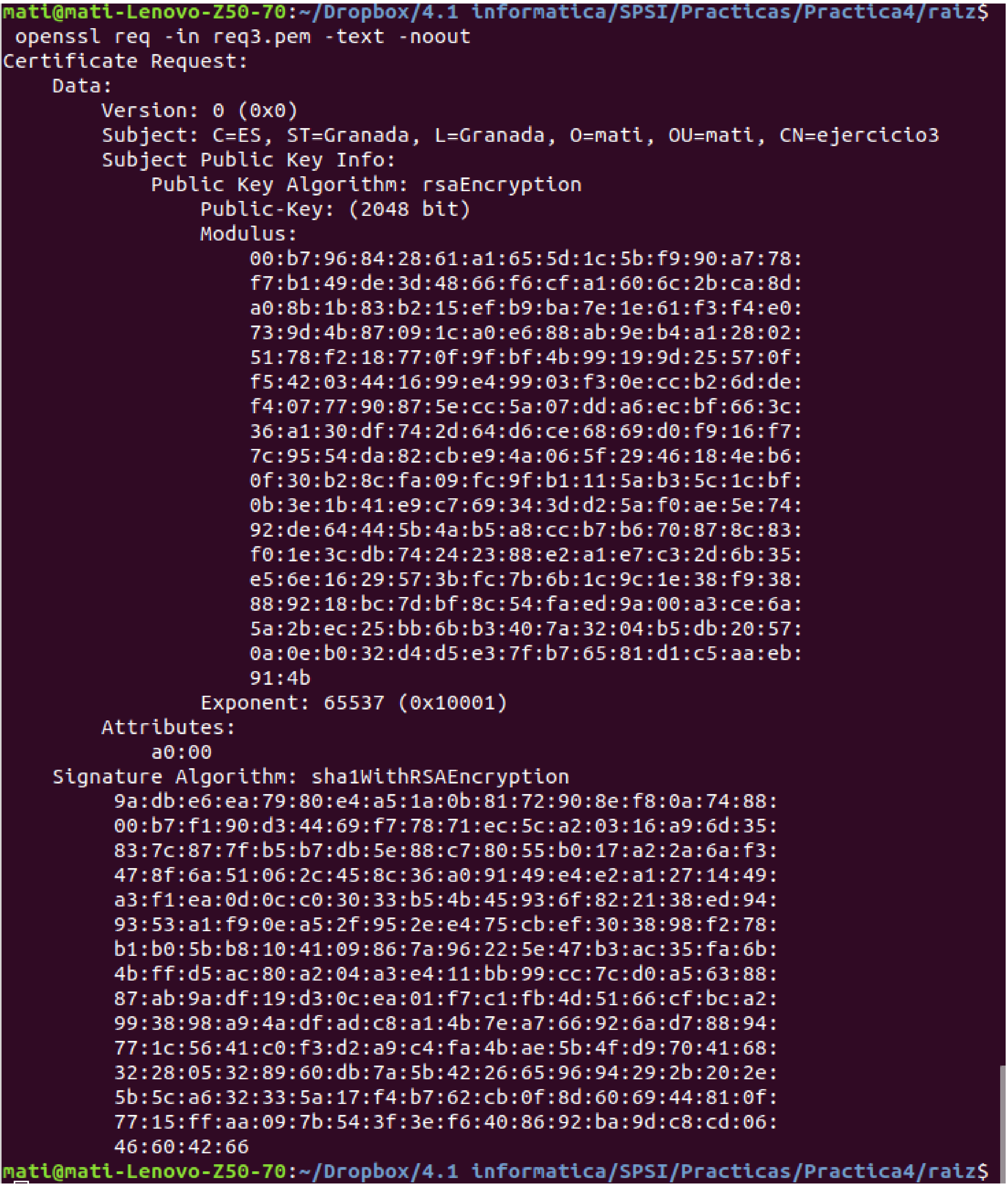
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4$
openssl rsa -in key3.pem -text -noout
Enter pass phrase for key3.pem:
Private-Key: (2048 bit)
modulus:
    00:c1:ce:4c:f7:dd:5b:39:12:7d:cc:9e:5c:ae:6a:
    ec:07:59:ea:b0:9a:ae:65:33:a8:d1:02:7c:4a:f5:
    2a:66:c8:a0:20:46:e4:74:3b:bb:65:5b:04:d9:80:
    be:5a:6c:2e:f5:a3:72:95:0f:7d:f5:49:81:0e:1d:
    69:82:2a:28:ea:78:3a:a7:36:c0:37:a0:5a:db:44:
    4c:bc:e7:80:98:a3:d0:d8:21:53:3d:5a:77:89:09:
    89:3a:42:d0:b2:2d:db:58:8f:8d:c7:dc:3c:57:c2:
    23:79:68:e3:61:84:1f:c4:8d:8d:75:94:1a:8b:b5:
    9c:28:31:68:88:6c:59:54:c6:dd:1f:b3:bf:20:dc:
    4e:7c:35:23:05:98:be:bd:50:91:2b:c6:40:01:09:
    00:26:eb:7a:ae:ba:d5:9c:87:28:3b:77:43:08:f4:
    7a:c8:fc:a9:4d:a5:27:97:df:2d:13:a8:47:25:d1:
    99:02:ec:3d:4a:7c:21:49:98:78:fd:df:6e:2d:e5:
    d1:3c:a2:ba:cf:f4:dc:fa:7a:65:9d:0d:1b:12:1f:
    97:99:32:51:c6:fc:39:f1:24:d4:00:b1:38:ab:56:
    9a:f3:0e:d8:19:32:2b:98:dd:c5:7d:3b:95:7a:0c:
    27:da:7e:44:e9:16:a7:18:55:72:dd:14:e5:f8:99:
    86:7d
publicExponent: 65537 (0x10001)
privateExponent:
    00:aa:5c:77:8a:16:b9:de:a4:63:92:df:ce:26:bf:
    f4:74:cd:d4:a0:a3:88:13:8b:e2:a4:bf:e3:94:5c:
    88:86:4b:6b:7e:93:f2:b4:3d:e1:8f:c9:ff:ac:56:
    20:7e:09:c5:09:c6:40:ad:c9:2d:76:d5:c3:2d:2e:
    2b:95:f1:0b:80:78:69:4e:9d:b1:3f:f4:a4:89:44:
    33:94:86:87:a3:25:b5:2a:97:b8:bd:20:ee:1c:b7:
    16:3a:f1:8a:d4:65:bc:ff:cf:48:d9:5b:be:6b:82:
    4b:7e:a8:f5:df:bd:ad:d3:30:7f:1d:d1:2f:b8:89:
    cf:18:01:be:9a:d5:6b:7d:39:bc:1d:00:57:aa:c5:
    bc:84:ca:1e:5c:9f:94:21:2d:34:64:97:f3:66:f3:
    d3:e1:6c:e3:ac:17:e2:cb:82:2c:03:64:7b:af:fe:
    fd:14:cf:54:39:b8:1a:68:3b:ac:24:74:6a:bc:84:
    6e:c5:35:d8:ea:a4:f6:36:90:56:1e:48:5d:9c:56:
    f8:35:8e:c1:47:ba:94:68:b5:c9:a1:0a:36:d3:e6:
    52:cc:68:59:49:95:c4:be:24:e7:7d:0e:37:bb:fd:
    67:20:41:df:0e:aa:78:63:d1:ce:c5:43:c8:b2:6f:
    ea:88:e9:a2:91:31:a8:e7:37:89:b3:3d:52:80:3a:
    33:81
```



```
prime1:
    00:f8:cc:41:cc:bf:85:04:52:23:b3:04:4d:35:a3:
    6a:35:20:da:26:47:1f:36:2b:12:a9:0e:f5:15:62:
    83:37:6f:5b:7a:c3:19:e7:96:81:91:1d:11:d5:9a:
    58:78:10:77:6d:7c:48:3b:a0:14:70:a9:2d:eb:4f:
    6c:41:8b:52:eb:eb:62:96:61:be:c9:70:29:ec:a0:
    30:0e:98:67:c0:c2:d9:1f:ca:29:0d:fe:8c:86:3e:
    9d:22:38:b1:60:7a:8f:a0:43:8c:d8:8b:19:2d:38:
    30:2e:27:68:8a:db:d8:44:fd:6b:c7:c5:8a:27:7b:
    93:8b:2c:f2:3c:04:3f:25:dd
prime2:
    00:c7:6a:84:fc:3c:68:3c:a3:c0:c0:6d:df:b8:ee:
    2a:db:7f:cb:ba:50:9c:f5:11:ba:9f:85:5a:15:71:
    52:8c:59:27:c7:b3:b2:24:16:28:b3:e8:4d:05:03:
    a2:d1:0b:06:f0:bd:2b:16:df:cf:d2:7e:60:d0:22:
    0e:b0:74:f7:f3:46:4a:aa:db:7f:d5:b4:8b:67:ed:
    a3:cb:a8:91:52:28:c9:8a:cd:71:d6:22:3b:1f:3d:
    b0:0a:78:44:38:ae:63:5c:f9:54:f3:58:7f:cc:b0:
    d7:ab:bc:76:b2:31:fc:5a:4e:d1:71:8a:9b:75:cd:
    13:aa:7c:39:31:e1:c6:69:21
exponent1:
    00:e8:fb:85:a6:b1:b6:63:7c:73:d7:c0:f0:78:89:
    45:fc:e8:7d:c0:98:9b:7e:c3:49:1f:2d:55:8e:a8:
    08:ce:91:a6:2d:c8:a3:ea:7d:c3:69:5b:ba:86:b7:
    99:9f:1d:74:68:ff:98:38:d5:c8:2e:54:0f:1f:2a:
    e9:ea:5b:08:d4:ca:41:31:27:e9:5c:83:7f:8f:09:
    d6:d6:e4:1b:4c:a4:6a:64:dd:90:22:7d:bb:a4:3e:
    e0:30:da:bc:27:e7:bd:b5:cb:6c:0a:9f:ff:7c:9c:
    00:6a:48:17:1a:e9:92:95:d0:66:ec:d5:6c:71:5a:
    c4:a8:f0:f7:0a:02:c4:0b:b5
exponent2:
    56:71:65:4e:55:fd:35:74:22:a5:07:bb:f8:55:3d:
    bc:c2:ac:14:8a:c7:4f:30:ad:3e:63:37:06:9e:86:
    13:12:be:bc:c1:b7:92:0f:0c:fb:d7:d2:33:3f:3d:
    3f:f2:d0:c2:60:ae:22:0f:48:ee:4d:1c:38:7c:da:
    f3:40:f1:0e:c2:c4:b1:45:cf:27:5b:49:26:f7:0b:
    8e:c7:f6:9e:af:d1:95:da:b2:e3:09:19:a9:d4:3a:
    d0:7f:0b:cb:aa:44:a6:53:ea:b0:46:07:b8:3a:5c:
    73:34:92:1b:72:b1:9a:90:1a:18:66:e6:36:ed:7b:
    fd:e6:35:80:db:07:00:21
```



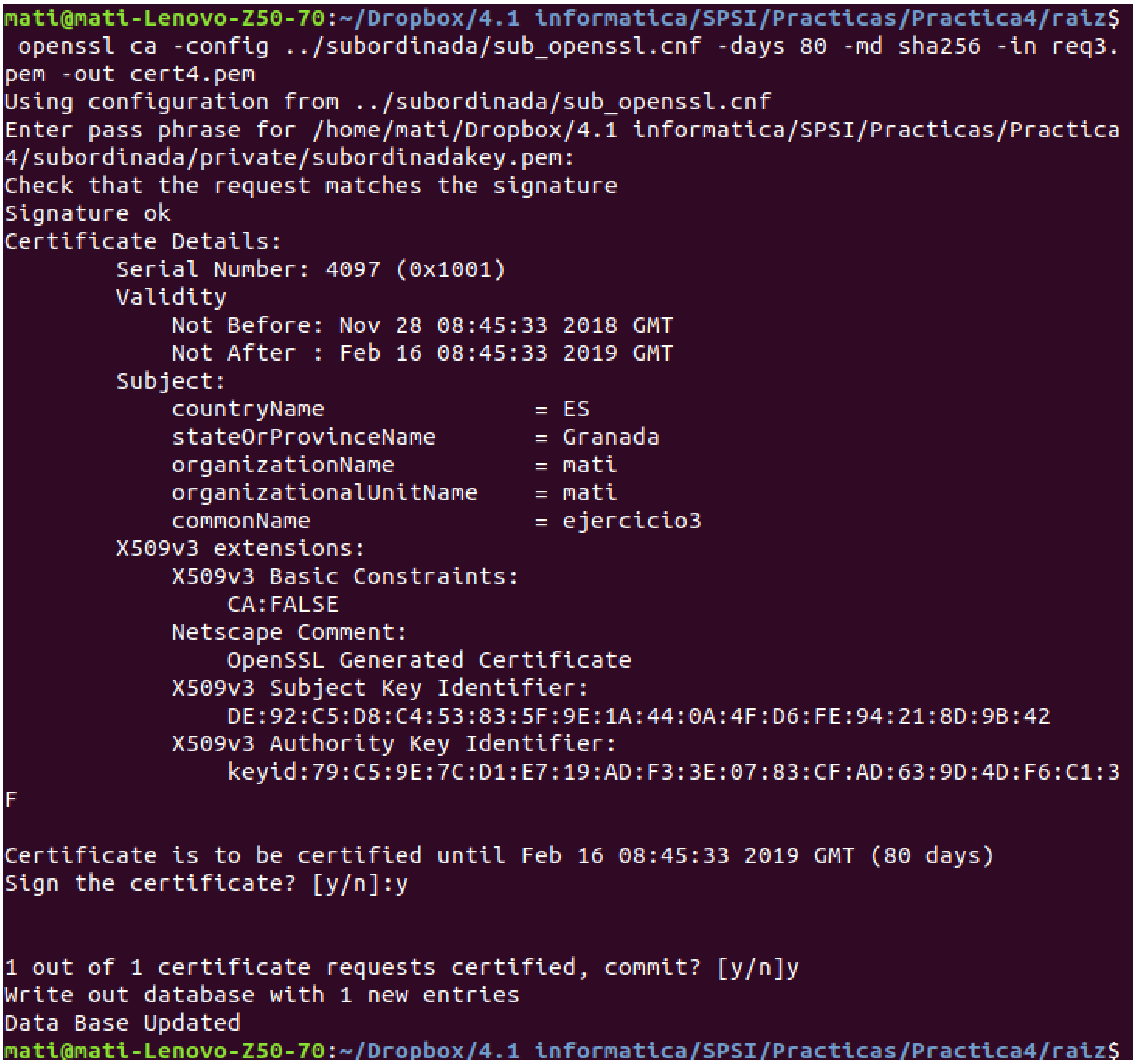
```
coefficient:
    00:c4:52:9d:a8:47:c8:de:af:12:48:75:0d:bb:e4:
    c0:0f:7d:fb:24:9e:7b:2a:df:be:80:cb:d2:a3:da:
    9a:45:ad:1e:e1:83:f2:6d:53:a0:5f:3f:cf:3b:15:
    a9:fd:76:ff:cd:e0:54:e6:5c:d4:d5:6c:57:c9:9e:
    99:70:d9:03:73:fa:e0:fb:42:15:c4:a2:07:da:2d:
    d1:ae:2f:99:56:6b:f6:64:2c:1b:37:18:7f:e1:69:
    39:68:01:96:2a:2a:ed:d3:a2:e6:f6:8e:38:0b:a2:
    a1:0d:3e:93:5f:c0:1f:d0:cc:36:04:17:e1:51:a5:
    9a:19:25:70:08:7b:84:f0:50
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4$
```



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl req -in req3.pem -text -noout
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, L=Granada, O=mati, OU=mati, CN=ejercicio3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b7:96:84:28:61:a1:65:5d:1c:5b:f9:90:a7:78:
                    f7:b1:49:de:3d:48:66:f6:cf:a1:60:6c:2b:ca:8d:
                    a0:8b:1b:83:b2:15:ef:b9:ba:7e:1e:61:f3:f4:e0:
                    73:9d:4b:87:09:1c:a0:e6:88:ab:9e:b4:a1:28:02:
                    51:78:f2:18:77:0f:9f:bf:4b:99:19:9d:25:57:0f:
                    f5:42:03:44:16:99:e4:99:03:f3:0e:cc:b2:6d:de:
                    f4:07:77:90:87:5e:cc:5a:07:dd:a6:ec:bf:66:3c:
                    36:a1:30:df:74:2d:64:d6:ce:68:69:d0:f9:16:f7:
                    7c:95:54:da:82:cb:e9:4a:06:5f:29:46:18:4e:b6:
                    0f:30:b2:8c:fa:09:fc:9f:b1:11:5a:b3:5c:1c:bf:
                    0b:3e:1b:41:e9:c7:69:34:3d:d2:5a:f0:ae:5e:74:
                    92:de:64:44:5b:4a:b5:a8:cc:b7:b6:70:87:8c:83:
                    f0:1e:3c:db:74:24:23:88:e2:a1:e7:c3:2d:6b:35:
                    e5:6e:16:29:57:3b:fc:7b:6b:1c:9c:1e:38:f9:38:
                    88:92:18:bc:7d:bf:8c:54:fa:ed:9a:00:a3:ce:6a:
                    5a:2b:ec:25:bb:6b:b3:40:7a:32:04:b5:db:20:57:
                    0a:0e:b0:32:d4:d5:e3:7f:b7:65:81:d1:c5:aa:eb:
                    91:4b
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
         9a:db:e6:ea:79:80:e4:a5:1a:0b:81:72:90:8e:f8:0a:74:88:
         00:b7:f1:90:d3:44:69:f7:78:71:ec:5c:a2:03:16:a9:6d:35:
         83:7c:87:7f:b5:b7:db:5e:88:c7:80:55:b0:17:a2:2a:6a:f3:
         47:8f:6a:51:06:2c:45:8c:36:a0:91:49:e4:e2:a1:27:14:49:
         a3:f1:ea:0d:0c:c0:30:33:b5:4b:45:93:6f:82:21:38:ed:94:
         93:53:a1:f9:0e:a5:2f:95:2e:e4:75:cb:ef:30:38:98:f2:78:
         b1:b0:5b:b8:10:41:09:86:7a:96:22:5e:47:b3:ac:35:fa:6b:
         4b:ff:d5:ac:80:a2:04:a3:e4:11:bb:99:cc:7c:d0:a5:63:88:
         87:ab:9a:df:19:d3:0c:ea:01:f7:c1:fb:4d:51:66:cf:bc:a2:
         99:38:98:a9:4a:df:ad:c8:a1:4b:7e:a7:66:92:6a:d7:88:94:
         77:1c:56:41:c0:f3:d2:a9:c4:fa:4b:ae:5b:4f:d9:70:41:68:
         32:28:05:32:89:60:db:7a:5b:42:26:65:96:94:29:2b:20:2e:
         5b:5c:a6:32:33:5a:17:f4:b7:62:cb:0f:8d:60:69:44:81:0f:
         77:15:ff:aa:09:7b:54:3f:3e:f6:40:86:92:ba:9d:c8:cd:06:
         46:60:42:66
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

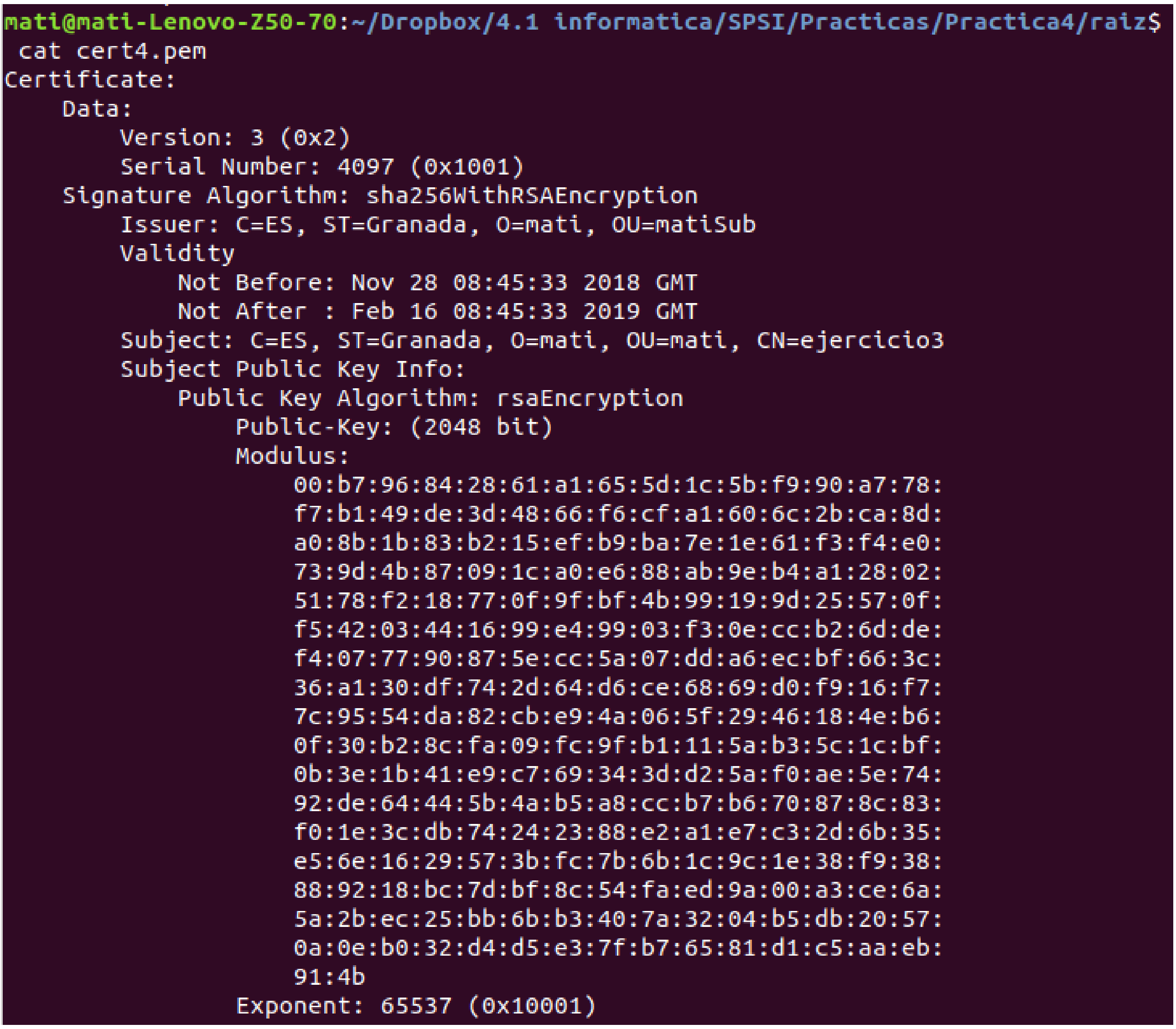
*** (1,5 puntos) Cread un certificado para la solicitud anterior empleando la CA subordinada. Mostrad el archivo y sus valores.**

Firmamos la solicitud anterior “rep3.pem”, con salida creamos un certificado al que llamamos “cert4.pem”, caducará en 80 días y usamos la opción -md el algoritmo sha256 para generar el certificado auto firmado.

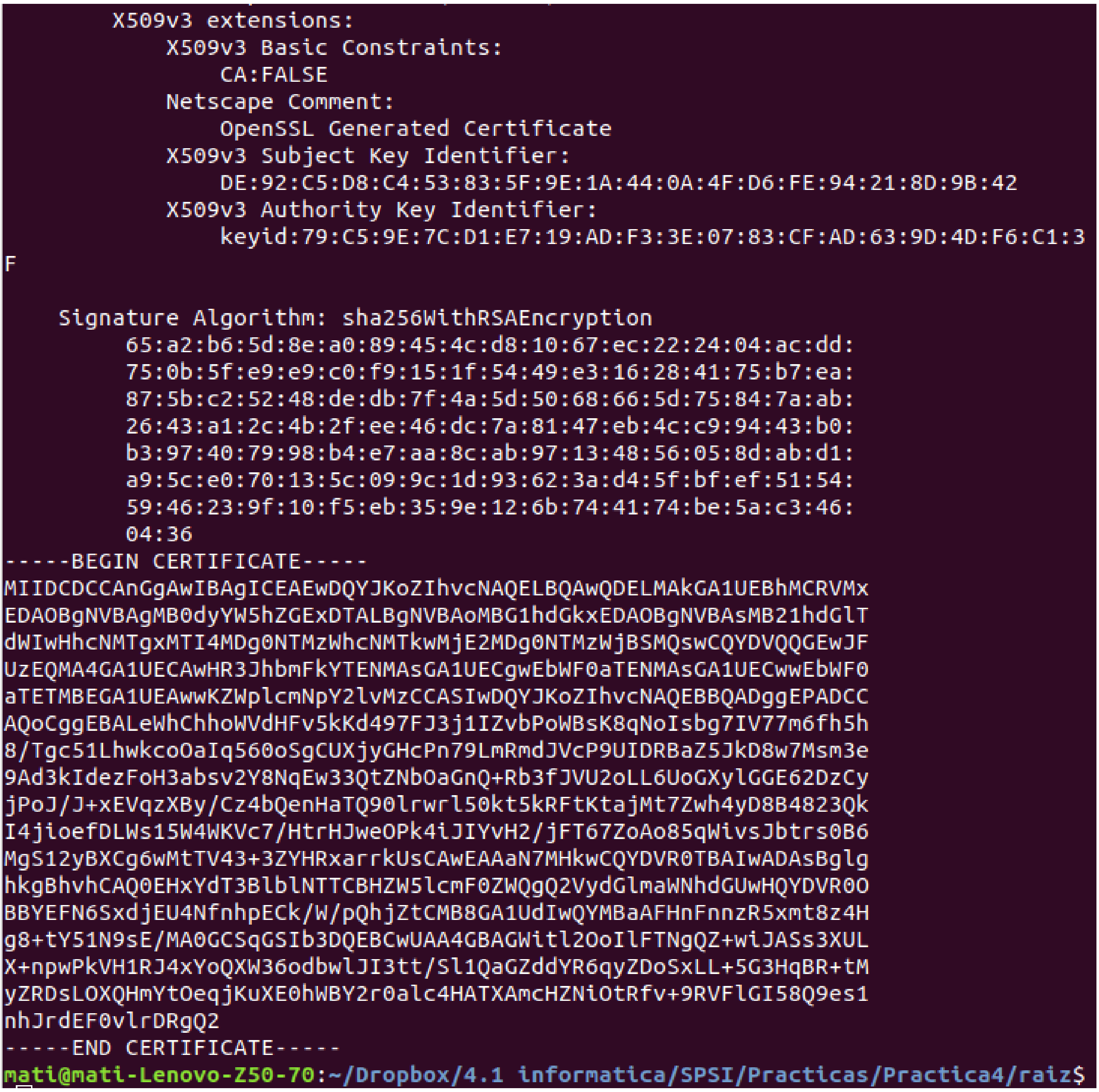


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl ca -config ../subordinada/sub_openssl.cnf -days 80 -md sha256 -in req3.
pem -out cert4.pem
Using configuration from ../subordinada/sub_openssl.cnf
Enter pass phrase for /home/mati/Dropbox/4.1 informatica/SPSI/Practicas/Practica
4/subordinada/private/subordinadakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Nov 28 08:45:33 2018 GMT
            Not After : Feb 16 08:45:33 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = mati
            organizationalUnitName    = mati
            commonName                = ejercicio3
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                DE:92:C5:D8:C4:53:83:5F:9E:1A:44:0A:4F:D6:FE:94:21:8D:9B:42
            X509v3 Authority Key Identifier:
                keyid:79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3
F

Certificate is to be certified until Feb 16 08:45:33 2019 GMT (80 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

Mostramos los valores:



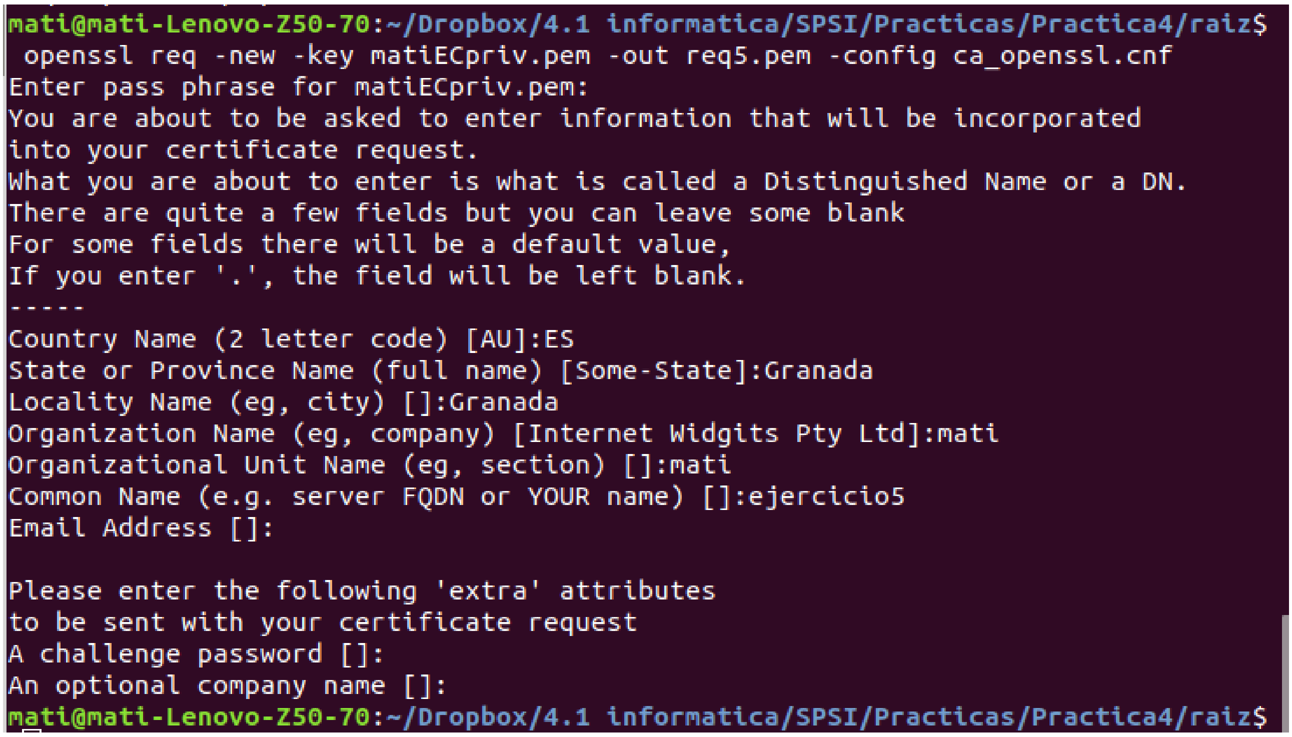
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 cat cert4.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=mati, OU=matiSub
        Validity
            Not Before: Nov 28 08:45:33 2018 GMT
            Not After : Feb 16 08:45:33 2019 GMT
        Subject: C=ES, ST=Granada, O=mati, OU=mati, CN=ejercicio3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b7:96:84:28:61:a1:65:5d:1c:5b:f9:90:a7:78:
                    f7:b1:49:de:3d:48:66:f6:cf:a1:60:6c:2b:ca:8d:
                    a0:8b:1b:83:b2:15:ef:b9:ba:7e:1e:61:f3:f4:e0:
                    73:9d:4b:87:09:1c:a0:e6:88:ab:9e:b4:a1:28:02:
                    51:78:f2:18:77:0f:9f:bf:4b:99:19:9d:25:57:0f:
                    f5:42:03:44:16:99:e4:99:03:f3:0e:cc:b2:6d:de:
                    f4:07:77:90:87:5e:cc:5a:07:dd:a6:ec:bf:66:3c:
                    36:a1:30:df:74:2d:64:d6:ce:68:69:d0:f9:16:f7:
                    7c:95:54:da:82:cb:e9:4a:06:5f:29:46:18:4e:b6:
                    0f:30:b2:8c:fa:09:fc:9f:b1:11:5a:b3:5c:1c:bf:
                    0b:3e:1b:41:e9:c7:69:34:3d:d2:5a:f0:ae:5e:74:
                    92:de:64:44:5b:4a:b5:a8:cc:b7:b6:70:87:8c:83:
                    f0:1e:3c:db:74:24:23:88:e2:a1:e7:c3:2d:6b:35:
                    e5:6e:16:29:57:3b:fc:7b:6b:1c:9c:1e:38:f9:38:
                    88:92:18:bc:7d:bf:8c:54:fa:ed:9a:00:a3:ce:6a:
                    5a:2b:ec:25:bb:6b:b3:40:7a:32:04:b5:db:20:57:
                    0a:0e:b0:32:d4:d5:e3:7f:b7:65:81:d1:c5:aa:eb:
                    91:4b
                Exponent: 65537 (0x10001)
```



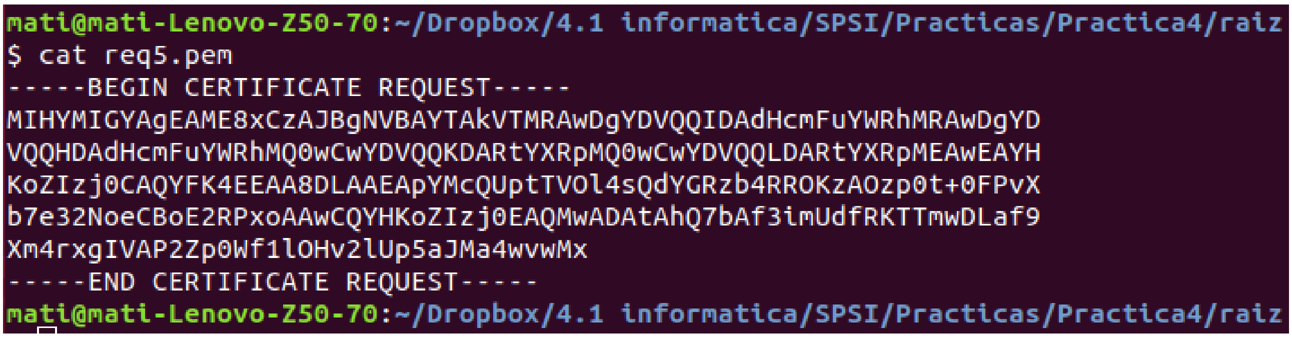
```
        X509v3 extensions:
            X509v3 Basic Constraints: 
                CA:FALSE
            Netscape Comment: 
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier: 
                DE:92:C5:D8:C4:53:83:5F:9E:1A:44:0A:4F:D6:FE:94:21:8D:9B:42
            X509v3 Authority Key Identifier: 
                keyid:79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3
F

    Signature Algorithm: sha256WithRSAEncryption
         65:a2:b6:5d:8e:a0:89:45:4c:d8:10:67:ec:22:24:04:ac:dd:
         75:0b:5f:e9:e9:c0:f9:15:1f:54:49:e3:16:28:41:75:b7:ea:
         87:5b:c2:52:48:de:db:7f:4a:5d:50:68:66:5d:75:84:7a:ab:
         26:43:a1:2c:4b:2f:ee:46:dc:7a:81:47:eb:4c:c9:94:43:b0:
         b3:97:40:79:98:b4:e7:aa:8c:ab:97:13:48:56:05:8d:ab:d1:
         a9:5c:e0:70:13:5c:09:9c:1d:93:62:3a:d4:5f:bf:ef:51:54:
         59:46:23:9f:10:f5:eb:35:9e:12:6b:74:41:74:be:5a:c3:46:
         04:36
-----BEGIN CERTIFICATE-----
MIIDCDCCAnGgAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwQDELMAkGA1UEBhMCRVMx
EDAOBgNVBAgMB0dyYW5hZGExDTALBgNVBAoMBG1hdGkxEDAOBgNVBAsMB21hdGlT
dWIwHhcNMTgxMTI4MDg0NTMzWhcNMTkwMjE2MDg0NTMzWjBSMQswCQYDVQQGEwJF
UzEQMA4GA1UECAwHR3JhbmFkYTENMAsGA1UECgwEbWF0aTENMAsGA1UECwwEbWF0
aTETMBEGA1UEAwwKZWplcmNpY2lvMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALeWhChhoWVdHFv5kKd497FJ3j1IZvbPoWBsK8qNoIsbg7IV77m6fh5h
8/Tgc51LhwkcoOaIq560oSgCUXjyGHcPn79LmRmdJVcP9UIDRBaZ5JkD8w7Msm3e
9Ad3kIdezFoH3absv2Y8NqEw33QtZNbOaGnQ+Rb3fJVU2oLL6UoGXylGGE62DzCy
jPoJ/J+xEVqzXBy/Cz4bQenHaTQ90lrwrl50kt5kRFtKtajMt7Zwh4yD8B4823Qk
I4jioefDLWs15W4WKVc7/HtrHJweOPk4iJIYvH2/jFT67ZoAo85qWivsJbtrs0B6
MgS12yBXCg6wMtTV43+3ZYHRxarrkUsCAwEAAaN7MHkwCQYDVR0TBAIwADAsBglg
hkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0O
BBYEFN6SxdjEU4NfnhpECk/W/pQhjZtCMB8GA1UdIwQYMBaAFHnFnnzR5xmt8z4H
g8+tY51N9sE/MA0GCSqGSIb3DQEBCwUAA4GBAGWitl2OoIlFTNgQZ+wiJASs3XUL
X+npwPkVH1RJ4xYoQXW36odbwlJI3tt/Sl1QaGZddYR6qyZDoSxLL+5G3HqBR+tM
yZRDsLOXQHmYtOeqjKuXE0hWBY2r0alc4HATXAmcHZNiOtRfv+9RVFlGI58Q9es1
nhJrdEF0vlrDRgQ2
-----END CERTIFICATE-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

*** (1,5 puntos) Cread una solicitud de certificado para cualquiera de las claves que habéis generado en las prácticas anteriores, excepto las RSA . Mostrad el archivo y el valor de la solicitud.**

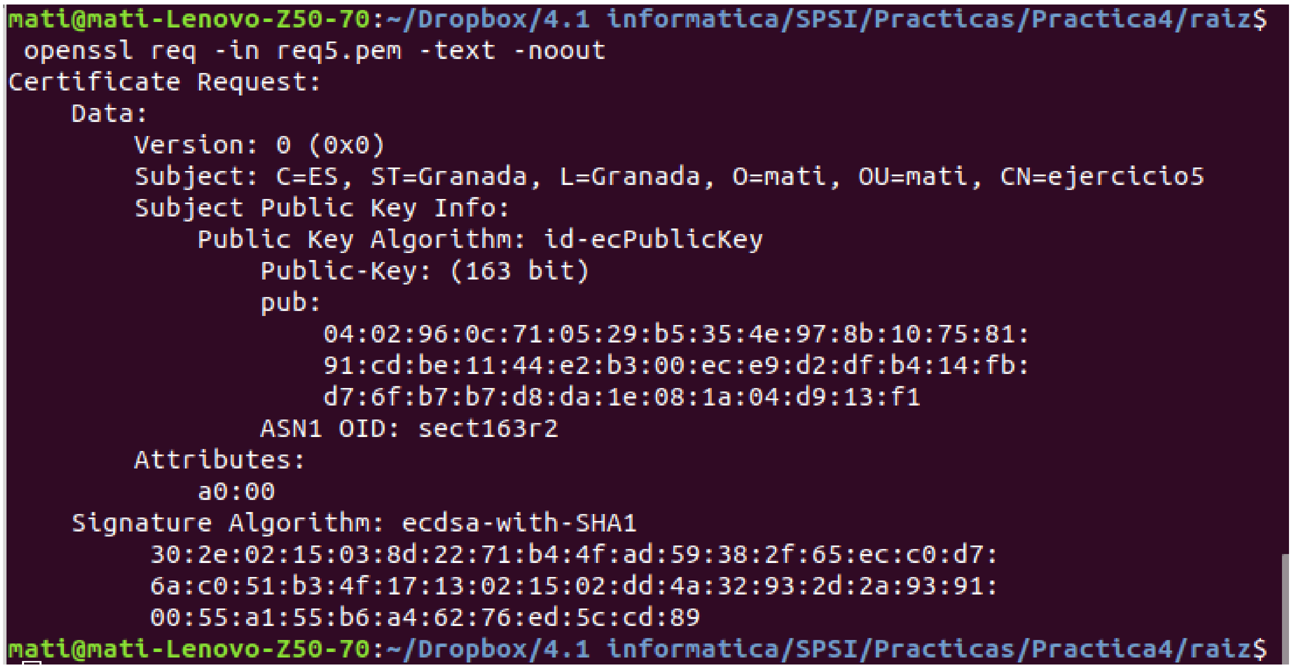
De la practica anterior traemos “matiECpriv.pem”. Usamos ca_openssl.cnf de nuestro certificado raiz. Archivo donde se guarda la solicitud “req5.pem”. El Common Name será “ejercicio5”.



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl req -new -key matiECpriv.pem -out req5.pem -config ca_openssl.cnf
Enter pass phrase for matiECpriv.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:mati
Organizational Unit Name (eg, section) []:mati
Common Name (e.g. server FQDN or YOUR name) []:ejercicio5
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```



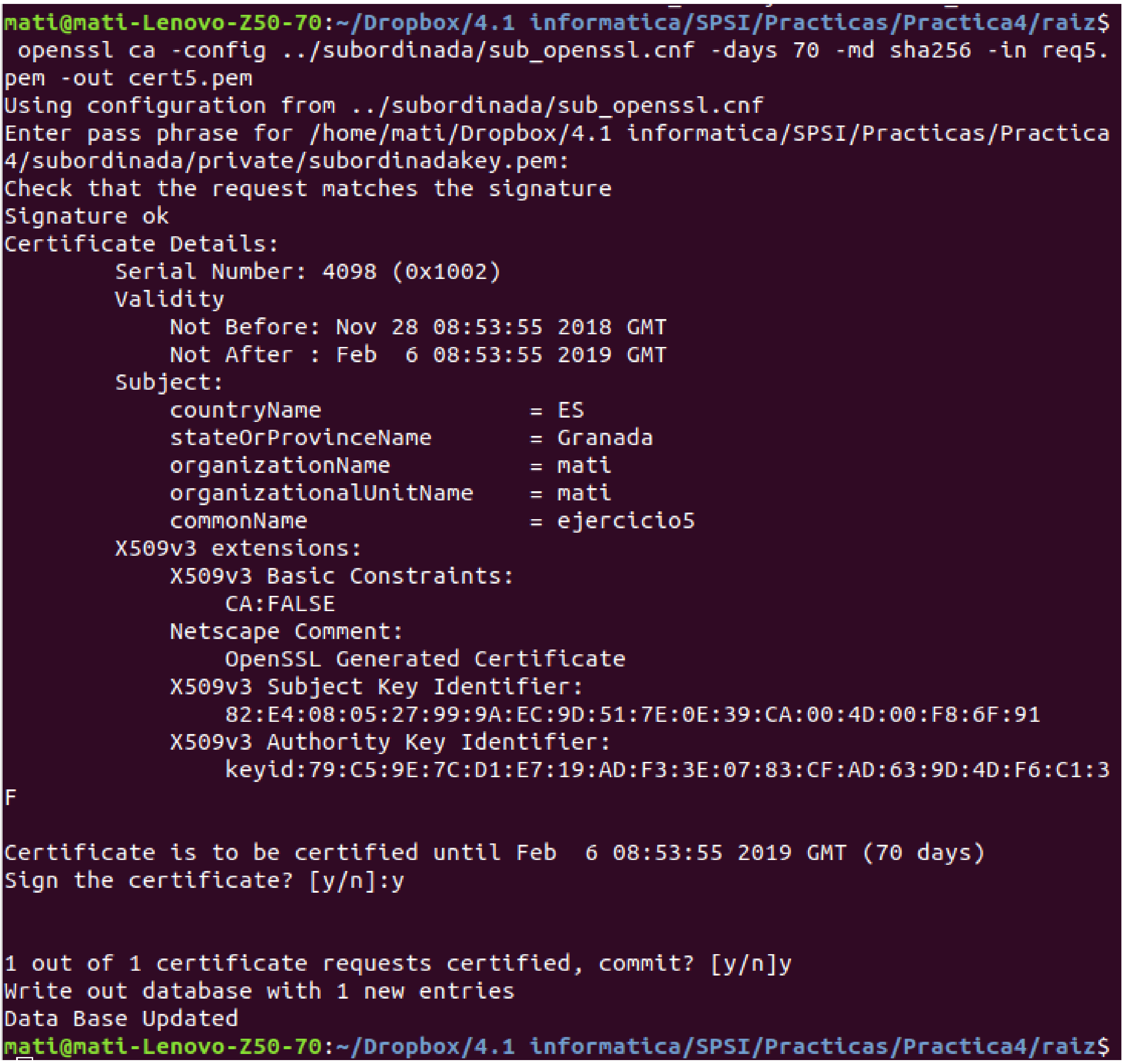
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz
$ cat req5.pem
-----BEGIN CERTIFICATE REQUEST-----
MIHYMIGYAgEAME8xCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMRAwDgYD
VQQHDAdHcmFuYWRhMQ0wCwYDVQQKDARtYXRpMQ0wCwYDVQQLDARtYXRpMEAwEAYH
KoZIzj0CAQYFK4EEAA8DLAAEApYMcQUptTVOl4sQdYGRzb4RROKzAOzp0t+0FPvX
b7e32NoeCBoE2RPxoAAwCQYHKoZIzj0EAQMwADAtAhQ7bAf3imUdfRKTTmwDLaf9
Xm4rxgIVAP2Zp0Wf1lOHv2lUp5aJMa4wvwMx
-----END CERTIFICATE REQUEST-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz
```



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl req -in req5.pem -text -noout
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, L=Granada, O=mati, OU=mati, CN=ejercicio5
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (163 bit)
                pub:
                    04:02:96:0c:71:05:29:b5:35:4e:97:8b:10:75:81:
                    91:cd:be:11:44:e2:b3:00:ec:e9:d2:df:b4:14:fb:
                    d7:6f:b7:b7:d8:da:1e:08:1a:04:d9:13:f1
                ASN1 OID: sect163r2
        Attributes:
            a0:00
    Signature Algorithm: ecdsa-with-SHA1
         30:2e:02:15:03:8d:22:71:b4:4f:ad:59:38:2f:65:ec:c0:d7:
         6a:c0:51:b3:4f:17:13:02:15:02:dd:4a:32:93:2d:2a:93:91:
         00:55:a1:55:b6:a4:62:76:ed:5c:cd:89
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

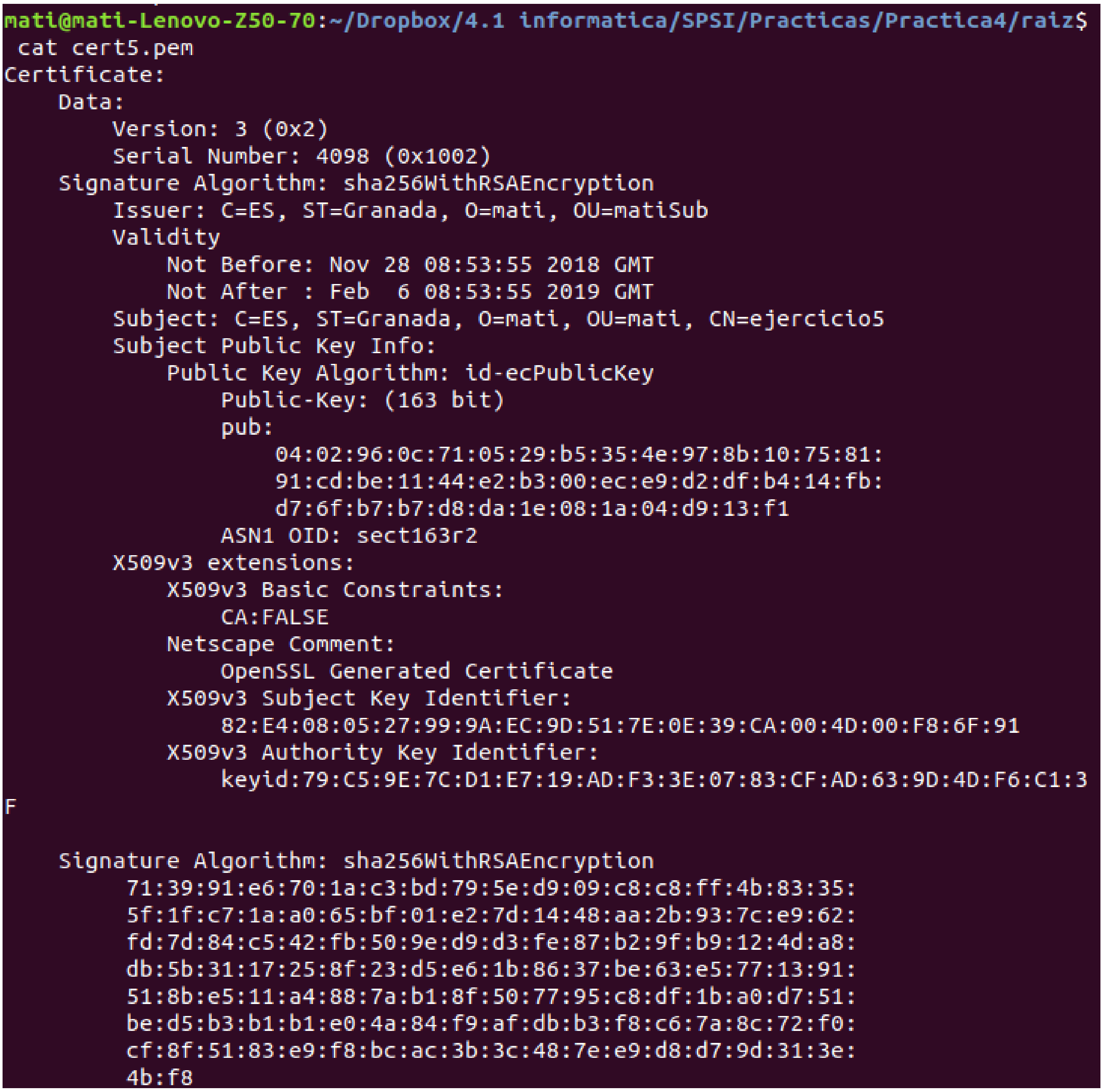
*** (1,5 puntos) Cread un certificado para la solicitud anterior utilizando la CA subordinada. Mostrad el archivo y los valores del certificado.**

Firmamos la solicitud anterior “rep5.pem”, con salida creamos un certificado al que llamamos “cert5.pem”, caducará en 80 días y usamos la opción -md el algoritmo sha256 para generar el certificado auto firmado.

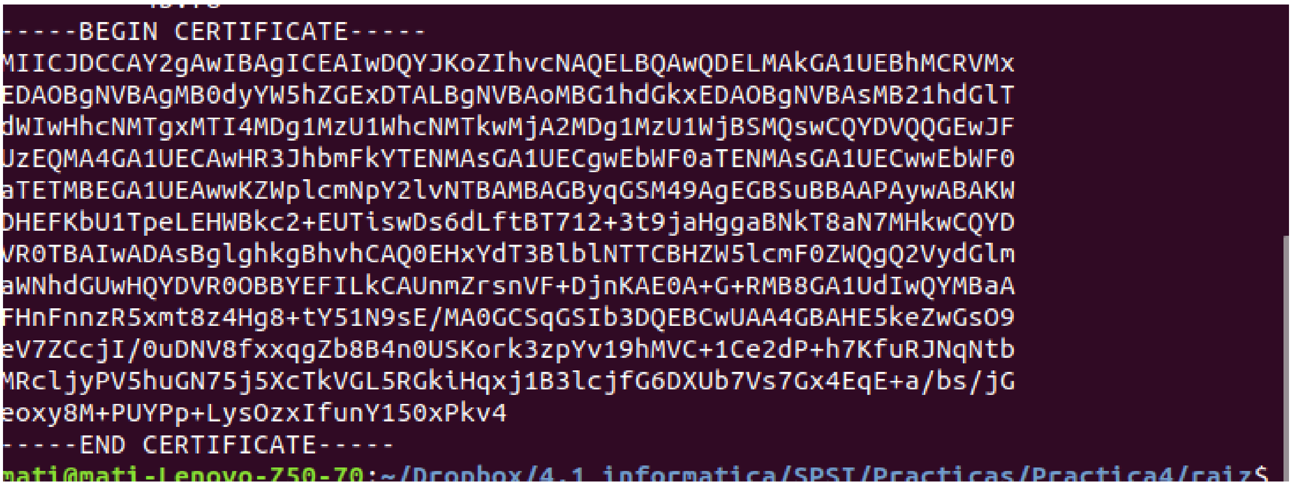


```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 openssl ca -config ../subordinada/sub_openssl.cnf -days 70 -md sha256 -in req5.
pem -out cert5.pem
Using configuration from ../subordinada/sub_openssl.cnf
Enter pass phrase for /home/mati/Dropbox/4.1 informatica/SPSI/Practicas/Practica
4/subordinada/private/subordinadakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4098 (0x1002)
        Validity
            Not Before: Nov 28 08:53:55 2018 GMT
            Not After : Feb  6 08:53:55 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = mati
            organizationalUnitName    = mati
            commonName                = ejercicio5
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                82:E4:08:05:27:99:9A:EC:9D:51:7E:0E:39:CA:00:4D:00:F8:6F:91
            X509v3 Authority Key Identifier:
                keyid:79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3
F

Certificate is to be certified until Feb  6 08:53:55 2019 GMT (70 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```

Mostramos los valores del certificado, al no poner la opcion -notext podemos ver toda la información con la orden “cat cert5.pem”, sino tendriamos que usar “openssl x509 -in cert5.pem -text -noout “



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
 cat cert5.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=mati, OU=matiSub
        Validity
            Not Before: Nov 28 08:53:55 2018 GMT
            Not After : Feb  6 08:53:55 2019 GMT
        Subject: C=ES, ST=Granada, O=mati, OU=mati, CN=ejercicio5
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (163 bit)
                pub:
                    04:02:96:0c:71:05:29:b5:35:4e:97:8b:10:75:81:
                    91:cd:be:11:44:e2:b3:00:ec:e9:d2:df:b4:14:fb:
                    d7:6f:b7:b7:d8:da:1e:08:1a:04:d9:13:f1
                ASN1 OID: sect163r2
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                82:E4:08:05:27:99:9A:EC:9D:51:7E:0E:39:CA:00:4D:00:F8:6F:91
            X509v3 Authority Key Identifier:
                keyid:79:C5:9E:7C:D1:E7:19:AD:F3:3E:07:83:CF:AD:63:9D:4D:F6:C1:3
F

    Signature Algorithm: sha256WithRSAEncryption
         71:39:91:e6:70:1a:c3:bd:79:5e:d9:09:c8:c8:ff:4b:83:35:
         5f:1f:c7:1a:a0:65:bf:01:e2:7d:14:48:aa:2b:93:7c:e9:62:
         fd:7d:84:c5:42:fb:50:9e:d9:d3:fe:87:b2:9f:b9:12:4d:a8:
         db:5b:31:17:25:8f:23:d5:e6:1b:86:37:be:63:e5:77:13:91:
         51:8b:e5:11:a4:88:7a:b1:8f:50:77:95:c8:df:1b:a0:d7:51:
         be:d5:b3:b1:b1:e0:4a:84:f9:af:db:b3:f8:c6:7a:8c:72:f0:
         cf:8f:51:83:e9:f8:bc:ac:3b:3c:48:7e:e9:d8:d7:9d:31:3e:
         4b:f8
```



```
-----BEGIN CERTIFICATE-----
MIICJDCCAY2gAwIBAgICEAIwDQYJKoZIhvcNAQELBQAwQDELMAkGA1UEBhMCRVMx
EDAOBgNVBAgMB0dyYW5hZGExDTALBgNVBAoMBG1hdGkxEDAOBgNVBAsMB21hdGlT
dWIwHhcNMTgxMTI4MDg1MzU1WhcNMTkwMjA2MDg1MzU1WjBSMQswCQYDVQQGEwJF
UzEQMA4GA1UECAwHR3JhbmFkYTENMAsGA1UECgwEbWF0aTENMAsGA1UECwwEbWF0
aTETMBEGA1UEAwwKZWplcmNpY2lvNTBAMBAGByqGSM49AgEGBSuBBAAPAywABAKW
DHEFKbU1TpeLEHWBkc2+EUTiswDs6dLftBT712+3t9jaHggaBNkT8aN7MHkwCQYD
VR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlm
aWNhdGUwHQYDVR0OBBYEFILkCAUnmZrsnVF+DjnKAE0A+G+RMB8GA1UdIwQYMBaA
FHnFnnzR5xmt8z4Hg8+tY51N9sE/MA0GCSqGSIb3DQEBCwUAA4GBAHE5keZwGsO9
eV7ZCcjI/0uDNV8fxxqgZb8B4n0USKork3zpYv19hMVC+1Ce2dP+h7KfuRJNqNtb
MRcljyPV5huGN75j5XcTkVGL5RGkiHqxj1B3lcjfG6DXUb7Vs7Gx4EqE+a/bs/jG
eoxy8M+PUYPp+LysOzxIfunY150xPkv4
-----END CERTIFICATE-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica4/raiz$
```