Exercici 1.- Generar les claus (0.5p)

1. Indiqueu les comandes que heu emprat per generar la llavor aleatòria i les claus, indicant el significat de cadascun dels paràmetres que heu fet servir.

openssl rand -base64 -out randFile.txt 512

Explicació d’instruccions llavor:

* openssl: cridem al paquet d’eines OpenSSL.
* rand: genera un numero aleatori utilitzant CSPRNG.
* -base64: codifica la informació seguint la especificació de base64.
* -out randFile: guardem la informació generada al randFile.
* 512: numero de bits o mida que es generen aleatòriament.

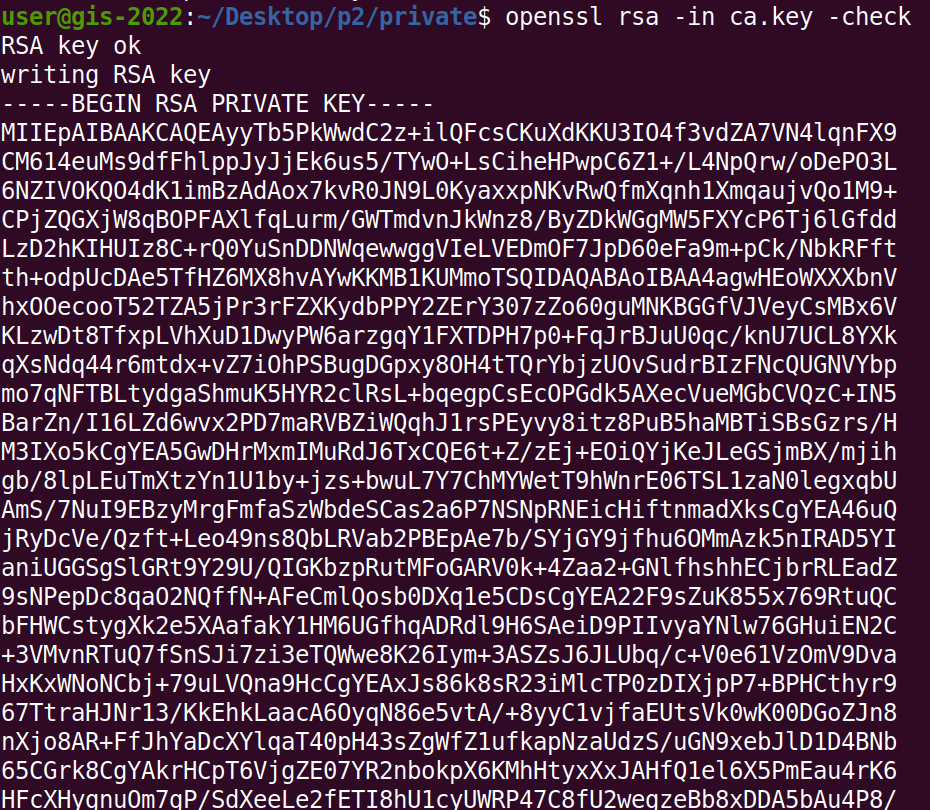
openssl genrsa -out ca.key -rand randFile.txt 2048

Explicació d’instruccions clau:

* genrsa: genera una RSA clau Privada.
* -out filename.key: la clau generada s’emmagatzema en filename.key
* -rand randFile.txt: utilitzem la llavor creada anteriorment per a generar els valors aleatoris.
* 2048: numero de bits o mida que es generen aleatòriament.

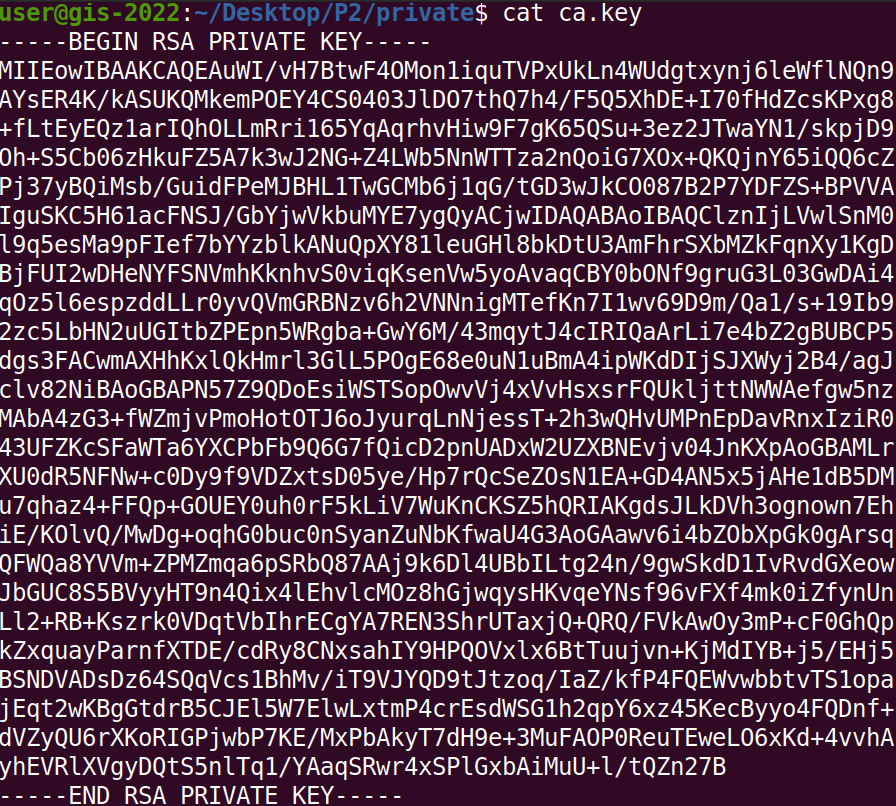
1. Verifiqueu que la clau generada és correcta emprant l’eina OpenSSL.

Verificació de la clau generada : openssl rsa -in ca.key -check

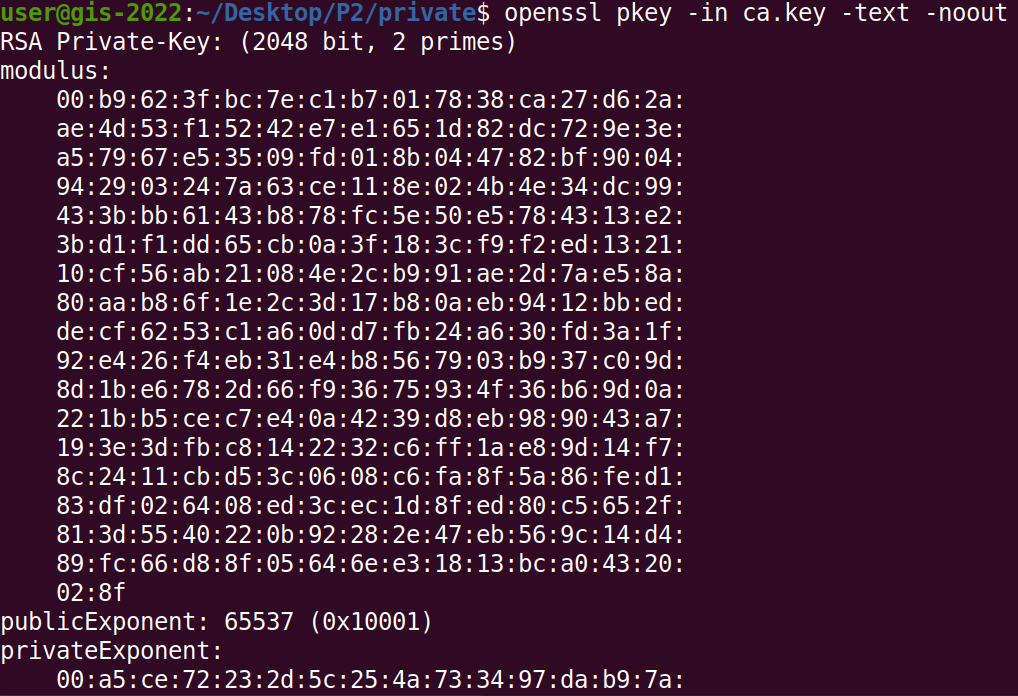


1. Visualitzeu el fitxer de claus que heu generat emprant l’eina OpenSSL i comenteu la informació que es mostra de la clau.

Inicialment tenim aquesta vista del fitxer de claus, que no ens aporta molta informació al estar codificat:



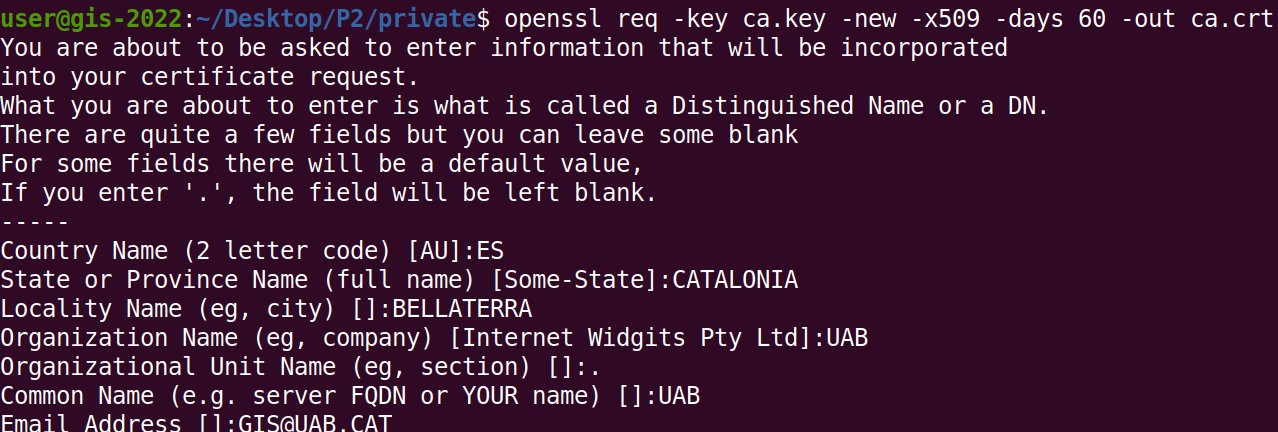
Amb l’ajuda de la instrucció pkey podem, extreure més informació :



Podem observar que tenim una RSA private key de 2048 bits, amb 2 primers. A mes a més, tenim la clau publica, el mòdul, el exponent privat. A la foto no he inclòs els dos primers, dos exponents i un coeficient, tots aquest se’ns donen codificats.

Exercici 2.- Crear un certificat auto-signat (0.5p)

1. Indiqueu les comandes que heu fet servir per generar el certificat, indicant el significat de cadascun dels paràmetres que heu fet servir.



Explicació d’instruccions generació de certificat:

* openssl: cridem al paquet d’eines OpenSSL.
* req: creació del procés per a un certificat.
* -key ca.key: utilitzem la clau creada anteriorment.
* -new: codifica la informació seguint la especificació de base64.
* -x509 randFile: informa a la instrucció req que volem crear un certificat auto-signat.
* -days 60: numero de dies de validesa del certificat.
* -out ca.crt: el certificat generat s’emmagatzema en ca.crt

1. Visualitzeu el certificat que heu generat i comenteu la informació que us mostra l’eina OpenSSL.

Podem veure diferents paràmetres d’informació del certificat: la versió del certificat, el numero de seqüencia que l’identifica, la signatura que té, les dades de validesa que conformen sent aquest 60 dies des de la data de creació. També tenim dades de qui ha creat aquest certificat, les que jo he emplenat en aquest cas. I per últim dades relacionades a la clau publica, quin tipus de encriptació porta aquesta clau pública, quants bits, mòdul ...

