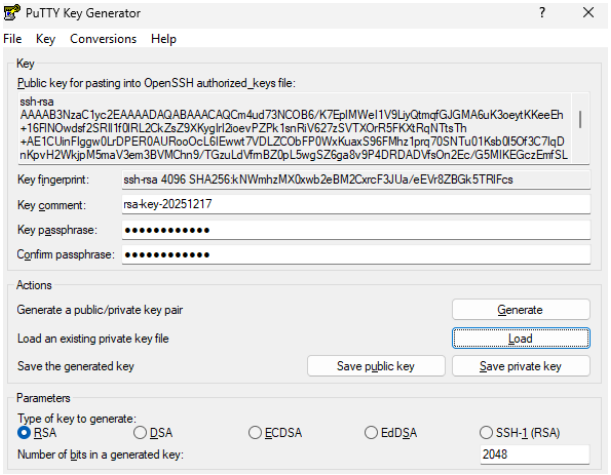
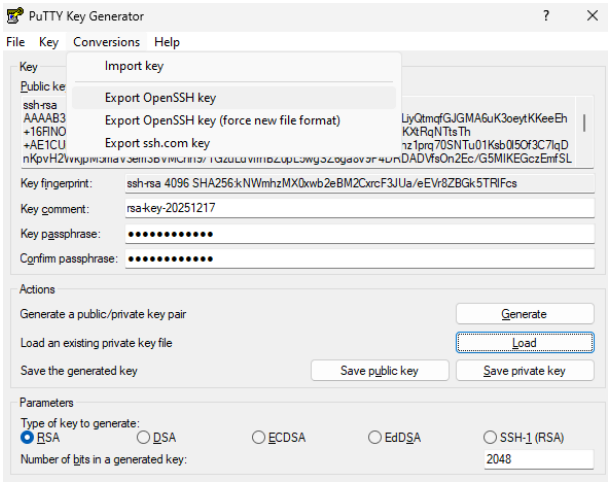
Practica 3 – Ejercicio 4

Usando PuttyGen genere una pareja de claves pública/privada de tipo SSH-1(RSA) de 4096 bits y proteja la clave privada con la frase "HolaCaracola". El formato de la clave generada es SSH2. Usando openssl u otra herramienta similar convertir la clave pública a formato PKCS#12. Como resultado del trabajo copie los textos de la clave pública / privada y añada el fichero .pfx generado.

Se ha generado la clave en formato SSH2 – RSA en el generador de claves de PuTTY





Posteriormente se ha exportado la clave a una clave con formato "OpenSSH key" la cual ha sido guardada como **clave_privada.pem.**

```
C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptografía>openssl req -new -key "C:\Users\Jorge\Desktop\UNIZAR\C
urso 2025-26\Cuatri I\criptografía\clave_privada.pem" -out "C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptog
rafía\certificado.csr
Enter pass phrase for C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptografÝa\clave_privada.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]:Zaragoza
Locality Name (eg, city) []:Zaragoza
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNIZAR
Organizational Unit Name (eg, section) []:UNIZAR - EUPLA
Common Name (e.g. server FQDN or YOUR name) []:Jorge
Email Address []:903700@unizar.es

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

C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptografía>
```

Para continuar se genera una solicitud de firma de solicitud siguiendo los pasos mostrados en la imagen superior; el resultado de este proceso es un archivo CSR el cual usa la clave privada exportada para crear una solicitud formal de certificado.

```
C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptografía>openssl x509 -req -days 365 -in certificado.csr -signk
ey clave_privada.pem -out certificado.crt
Enter pass phrase for clave_privada.pem:

Certificate request self-signature ok
subject=C=ES, ST=Zaragoza, L=Zaragoza, O=UNIZAR, OU=UNIZAR - EUPLA, CN=Jorge, emailAddress=903700@unizar.es
```

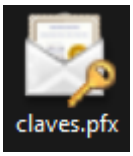
Una vez completado el paso anterior se crea el certificado auto firmado, al final de este profeso, obtendremos un archivo CRT (proveniente de la transformación directa del archivo CSR).

```
C:\Users\Jorge\Desktop\UNIZAR\Curso 2025-26\Cuatri I\criptografía>openssl pkcs12 -export -inkey clave_privada.pem -in ce
rtificado.crt -out claves.pfx
Enter pass phrase for clave_privada.pem:

Enter Export Password:

Verifying - Enter Export Password:
```

Para finalizar se realiza la exportación a formato PKCS#12, obteniendo así el archivo PFX que empaqueta la clave privada y el certificado público en un único archivo protegido.

El siguiente archivo 

guarda el resultado final del ejercicio:

Resultado del archivo .pfx obtenido mediante el comando <*openssl pkcs12 -info -in claves.pfx -nokeys*>

MAC: sha256, Iteration 2048

MAC length: 32, salt length: 16

PKCS7 Encrypted data: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256

Certificate bag

Bag Attributes

localKeyID: A2 17 6F 70 7D EB B5 A0 77 47 2B A8 0F 10 59 25 2D 99 05 8D

subject=C=ES, ST=Zaragoza, L=Zaragoza, O=UNIZAR, OU=UNIZAR - EUPLA, CN=Jorge, emailAddress=903700@unizar.es

issuer=C=ES, ST=Zaragoza, L=Zaragoza, O=UNIZAR, OU=UNIZAR - EUPLA, CN=Jorge, emailAddress=903700@unizar.es

-----BEGIN CERTIFICATE-----

MIIFzTCCA7WgAwIBAgIUa4FVN7Oqu6v1ytoYC9HPoWriS8kwDQYJKoZIhvcNAQEL

BQAwgY4xCzAJBgNVBAYTAkVTMREwDwYDVQQIDAhaYXJhZ296YTERMA8GA1UEBwwI

WmFyYWdvemExDzANBgNVBAoMBlVOSVpBUjEXMBUGA1UECwwOVU5JWkFSIC0gRVVQ

TEExDjAMBgNVBAMMBUpvcmdlMR8wHQYJKoZIhvcNAQkBFhA5MDM3MDBAdW5pemFy

LmVzMB4XDTI1MTIxOTE5NDYzN1oXDTI2MTIxOTE5NDYzN1owgY4xCzAJBgNVBAYT

AkVTMREwDwYDVQQIDAhaYXJhZ296YTERMA8GA1UEBwwIWmFyYWdvemExDzANBgNV

BAoMBlVOSVpBUjEXMBUGA1UECwwOVU5JWkFSIC0gRVVQTEExDjAMBgNVBAMMBUpv

cmdlMR8wHQYJKoZIhvcNAQkBFhA5MDM3MDBAdW5pemFyLmVzMIICIjANBgkqhkiG

9w0BAQEFAAOCAg8AMIICCgKCAgEApuLne9zQjgevyuxKZTFniNVfS4skLZqnxiRj

AOrit6HsrSinnhIftehZTTsHbH9kkSJdX9JUS9gpGbGfVysoCKyNoqHrz2T5NbJ0

Yletu80lU1zq0eRSl7UajU7bE4fgBNQlIpxSIIMNC6wzxEdAFEaKDnC+iBMMLe1Q

y2QjmxT9FsSrmsUvehTIc9aa6u9EjU7tNSrG9JeTn9wuyKg5yqbx9lpI6TOZmld3

ptwVTAoZ/f0xs7i3VX65wWdKS+clEmeoGvL/T+A0QwA1X7Dp9hHPxuTCChBnMxJn

0iyfXQxAtPlgLr1sBhF6iwUtg4TN7qwx2zvaU956XEJhr1y62KSU/emaTpayYJtR

3EBmOrdRAgf1Irv5pf2SwM8T3LElL1LHX6lUBvlFEs91gUHVlTdy4pWxN+fgg4sE

hKjDMYGxRf5YOPODV3wToJdVi08PSfA05i+vaVYEC7JvmeF5F8AexO7l5CO3aiQw

YKM0fGXtFLv1dVBvyPwEOSf7c12iknq7FCi09B/6y97pmclvO6P3cpZuOp0ImjgF

4AQtkV6y9MIzwMjekLo4oH3Ko1F/066P/C0z+WLbtPJP9mN21qnUgzme5mPGzvJC

wfElH075i2Yio0mQf+6lE02zCeDu47YWGJkp6lEi+dZRyHzgFtYdPP7L+RRUHThm

TcjOmHMCAwEAAaMhMB8wHQYDVR0OBBYEFKYpWEEWOGKHx8ABhfzRXiTU0dNLMA0G

CSqGSIb3DQEBCwUAA4ICAQBfK7o5qJUenk3t4tw0cLoFWaf+XtubT/1C7SqJbm4Z

1TvRpevg7cqAXcVPZvNzpTr+gS8YxnsA76xaLNpablrRv2n1VO0nYGc9NTUvKtrR

zMrcGoCJZCOL/itlwoqwjzleC9ptIO3alknB4akCXVKPQ/rOd3MASoiXdhZ/2GRk

7CmpFomVT2cD5mVNDjC4gcdrDix5E/4Otw4K7WvT0n7heMcLFTS0UKl7dGAmVlyb

WD5INGn8wssupqT07Q3smvsfCOlXaHYvQWZlRAlJnygNIgtPPoeNJyqyAvsLdjjq

a7mqau6SvTjGbOchMmoq0QnD1tPwbjqmWS2qOTfTIHv52FoGAt3NdgQcSp3PoaoC

o72DdRhCfO0FOYbNL23prXaV6/8yJuRoxKO7AZaMWbO7rETUKl61hXXxc3ERlQ3s

tH8v5piiOU3aokNWk6FaBRH5HOZJAry5EAFYt+flCMTJ7Z5TLg2u5G02aGtEnG++

dOfgBjTxhEI8DEWX8tKu11d4ihj9vjMVDgoHHfo8FaXeN+tItBGAtFp/CyYxHPmn

Uo6W9yYYwQ7UbORWUfXKXlxqu1ugxi3hzqDLGMaRD/w9nUkFk/YXAIn2Zfjo2Mkx

2ID5h4w8JNV/AymboSsHyiG8s3eFq2DY+Nw6sDFooqckN0C4zInfXJfZSuNJ/2f8

/Q==

-----END CERTIFICATE-----

PKCS7 Data

Shrouded Keybag: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256

Texto de clave pública

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20251217"

AAAAB3NzaC1yc2EAAAADAQABAAACAQCm4ud73NCOB6/K7EplMWeI1V9LiyQtmqfG

JGMA6uK3oeytKKeeEh+16FlNOwdsf2SRIl1f0lRL2CkZsZ9XKyglrI2ioevPZPk1

snRiV627zSVTXOrR5FKXtRqNTtsTh+AE1CUinFIggw0LrDPER0AURooOcL6IEwwt

7VDLZCObFP0WxKuaxS96FMhz1prq70SNTu01Ksb0l5Of3C7IqDnKpvH2WkjpM5ma

V3em3BVMChn9/TGzuLdVfrnBZ0pL5wgSZ6ga8v9P4DRDADVfsOn2Ec/G5MIKEGcz

EmfSLJ9dDEC08iAuvWwGEXqLBS2DhM3urDHbO9pT3npcQmGvXLrYpJT96ZpOlrJg

m1HcQGY6t1ECB/Uiu/ml/ZLAzxPcsSUvUsdfqVQG+UUSz3WBQdWVN3LilbE35+CD

iwSEqMMxgbFF/lg484NXfBOgl1WLTw9J8DTmL69pVgQLsm+Z4XkXwB7E7uXkl7dq

JDBgozR8Ze0Uu/V1UG/l/AQ5J/tzXaKSersUKLT0H/rL3umZyW87o/dylm46nQia

OAXgBC2RXrL0wjPAyN6QujigfcqjUX/Tro/8LTP5Ytu08k/2Y3bWqdSDOZ7mY8bO

8kLB8SUfTvmLZiKjSZB/7qUTTbMJ4O7jthYYmSnqUSL51lHlfOAW1h08/sv5FFQd

OGZNyM6Ycw==

---- END SSH2 PUBLIC KEY ----

Texto de clave privada

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

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,FB097DF3D0B3EF97

7UUWOBemC3TaqPwQsECiFYbzprVkeeayerEbTKkYlei/IKy7CUAwPVhAgF84vISh

X8xm/KWO3GsKwdyoiwPR/zf9n0KVuvAA/M3h2GDjO96Xy1SN5/8+q3G40MGiD4Hm

XNFmkjJnCCeTnA6H1Zud8UUEWFTGpVWbFW8gyY24FIWQQqt3eVG9apLFVNPKqBHP

8TZcyjDNb3+ohzCGThxrQ2IhP7Bp9CfZCuiCbQdD70BYRFXcHcbHk6KMcSnw8FVy

36lV1NwidglMX5XXWYV7qgFbMcAxSlK3APPxaV9LURMKQzHBTmR8BDRix1HR3Fu6

i9ibjKRu95TID1iH/qHV6MN3N9yN5zDc/kwL9IZwTvRnFz/amY3OSN2TRbDYyDy6

AOeHpmZEjWJNkvLXzX+CEBkjlZI6bGJ1lPWwJeGj4K0I4/x2N8C5Pz57WBp6Zmge

xLjr2fd6Bxz9Y91AK2r2AMTm9moGhUNnuDiWOzSWjFz59d3jTKEJSzVLmPcGklyO

bI81hCviuIOa6QULZevpepYDEV9n76WfdzvfmROQOa1Y+NrWw76AO+RTqgCRwJDX

RUDRFqJph36E+YnqjVTltQ8gL+hvTziwg9QhGR8VfyrNV6e4TEqGy7M+X1oPZPR1

hN8cMTWx30gE7sWlB9VSOxMlHCFAkm5RjK6EO+SJeWLlTakaKtZTWm4ZdLRVW/oI

YbjcAlz61lVpAPgKYRWdbHJJ2ZuepuUUWztu5JlxYb5kUDDc0HUm+Ju6FVVaWQCR

vuCeB7Ct91neya0SdgXXm3u+uV5G3Su7HazLhdR9OofHiMBb2LjQmRSdzRprMOpN

abmR/8KL2ekxyaikA0db7yFICZhzNEIJzenErWRaKu1q9TBtSXSTKaDbxPidmiDl

Eo3GYJ+hQvlThLSOtrDjVdXM1wSjLkVFmDYGMg7Dz3y1yAG/AcwMaymtblE5FpCi
bwy7Lehc9SBVmfaJTJ5V4in+pam8Y+/J9t5bVAT+NRojhY5qrQ7T7pq19juwporW
qR6PoaQaFZW9LBxgivOTBUZmZJhWHkYzSqRlrHq7gGSEUdnB9h81kKYusQWrrwTW
zfWFnu/8OPFk6hpwo1Mm4Jt4ST3MLpsIe7ALT0OBMRwdcsNeBrT0wlGAM73iMvZW
GF/WcEfAJszBQoxl7EGqTPfY+6HunyCzfrsuftslhRSql89DIIg7OOv9mHMr5M8w
PRVEwNdEqjjei+Sch/P+OTB+IiCSPqIydr2yt/goW/AaUFHaqnY9DgVL9Q0V6JYy
m1ktD5hkqwPrcyElwqLFLyKRBG4A/h65x7fAFyRB+pCSZ4VGlMrx3/uP7+leRHjq
ZVqm5XVFL1v1aaT0WxxDv0DcHGUdPvbuhLpA/GzpU3hPLdRxlHGgGPK3jgrUJDvx
hqXK0oi1tEGQEgLkM632J2icG1pxd0qajrdkVdGQWdEBcYLEuyCkzKX+3JScbSOs
VdnRnqXxPgjltcbzpsYLvpT8NGfWFWcSh0fDf6ph9j36siiUUHgGnlTnuKU5eSA6
mg2ZU22ZNMdznLN/G6rDXUkGVwqRrVtCp9YlA81DeqLgznygfwWtcceH3I/edcIA
ZKxt3/66ZRFCxlMDFKJLuZi9WRql1VMMIwTyrKyYYp1yhps5nHB97qPc38nIL0SY
ltt7PTdizo6fTvjQaH3XnfaI9U2B+pGFF1V7MgbjLVNINUDym5irgVasEzRaxtQx
IMog9FRm8FRW+12ws2QZyP47Wy2tHUcyeQzUosRpEKfArVVb3SwoVArcJek6KieF
nDEUaMHhMhh10A15LCNUOdkJOrVSx9T4PIBUZdHxbL8iBuyYlXJ2ZNpbpzP1kL8A
se6d+NDS/v4JjV92rzzidAY4gWdiUrK6vJ0bfxywBbwrkx/I4Bkh/+Z95LXWAqtr
XXLkUziuO0ULYHQgXZspdtuR3eXFKkGdRST965aecAk8pRWHC97CocYU4XutuOlc
6MiDeBj/iFBvjlwOdHAoQKplLP75++RkFJPG9r4hQyQgzsCDS8yvj43ztKjGq95E
peUh4Zqypwh0QMIHrwRKUdz5G3ZSnM+Bj2o2LYr1TqzWqksRsVrJA4FGslkgNtLH
hw7Q3vkTd++AV9ks4qzJjoxrSN1wuUbDhMHKoEya52S3cpSSxLrKZBqw66t+EOSs
4MlNRQNLmaDfhhPhc5shpyCM+3xb6bazdvhUGyEqDhpHUJ6XiVtSRmOpqRoAqTP8
xm16tHpiBGFmnpclv7QeYesAjWvw5SrHW/HH2zyvJGgFo3rQp9uCaUYkxvnBvk1R
ZPiF+xExGEOb73/ws1FCDStD6u/OjCKMysIREuqOAqRgSBffBElv8fPPCrWznj/A
7+mFL8WAah3mjULvgzQBSnpDk2G+lmbXmGbUNJlfeLowzWX4oQVNeLGm2Cof/Ty6
53QQ0u/bTerTa9o/s0CZbLlfbu5mDz/0EBh0RKefhQrlcx0V9MXsQYDzTunEMk2X
VEY1ckKjYiTNGuW5oZtvsrt33aWg9g3jc3KAP5YTFGfkrXYQs8cbkNxjyUDeG5bC
c2TfvyLHSQTQsuWxPFI3BOA7UWbdjCp2ZRnfeZn6Y6a++O4Rcl8ruQtayFuFHcB3
BHFavf/FHAlO6Jj0XXdfgycl9gFa1nKwOTvv1fAzknEJPgNO/CXS1plnSsVVxVUW
iX9G/BbdmeBHFC1sFlj2m6RbS7wq30rdANWFMN0N29PT8kEFsIgwOhEJ7KErvlTb
sRi7K7oN9nYKA4SkrUigGeVQmlso3QxEytDJiHoA97VWzCX22+5P/FDF1eoLXKo/
ik5AuFsCBloM5g5STyvvDiSELhuxuw2rZ6kqa9ArjNdV067ystVZH+PbObJZmt9S
Dmu8u3cvshiDfKSjpSMjaMdFS/7jTukvGEuqZausqso8ZALefdJVt3VOoOZo6gkb
Mv/0FVxRsmsJ3H13bolTmjbjtY31otdwLeDTMAm/wmtdR/NWqdsVnDB4Tz7gNrok
ANqa0/KV5EWrD4CB1SsMH1euHn/iquqp8I+D80LnxXn+ika3YJVCDu/hhaNHINEb
4cpN2gseVDTamb7hYxT3RZq7FLFsyugmfjtp5AMYDLceVvhWWNWqYcSxQyuPackb
-----END RSA PRIVATE KEY-----