1. SGSSI-20.PlantillaLaboratorio06 (S.8.3)

Práctica de SSL y algunas funciones relacionadas con integridad y confidencialidad en la red

1. Tecnologías utilizadas

Linux MX y la versión 1.1.1

1.1. Instalación de OpenSSL

He descargado el source pero al no ser suficiente el comando make he tenido que rebuscar algo[1] y siguiendo los pasos que recomenda una pagina de internet (primero había que configurar mediante el ./config atributos para luego poder hacer el make.

2. Generación de certificado autofirmado con OpenSSL

2.1. Crear la clave privada y pública

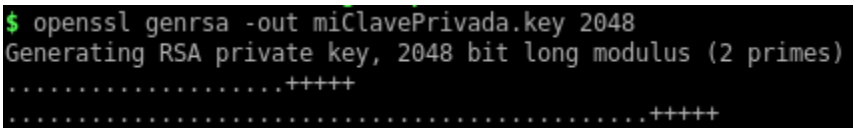

Imagen 1. Generación de clave privada

*Resultado **parcial** de clave privada en texto plano, miClavePrivada.key:*


```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyY8k+w6wBp8P8pwfajrYuz6XxdYrak3HmR+g0ToFjQvYnHVL
xenK572DCcpBDamRl1G8ILtNmgfZBAMSXja(...)1XJj5nYt0RTug8Ar8nom/XWkhwrHU
6B6Q0V46pEJ97BX10ZfDjmsNHtjBTvQCrlP(...)AIRi89EA2i1l5zbdiCXFrH2wPo8Ci
dKGYa6ghdD3GdYSCmTgBrBXJGDohJNiKoffVqsQKBgQDHll1Oh5QiBuZNBwACIPgNHsXp
vRf2HM9WEYlGlEBPrzrddmk/tBsqzpkcxyjXdjPLHfvRDe+MC7TOw+EDfjfWXkqX51o/
f6uMUT056AXBNUwr4HpI76Kg0sU4UyC09vuXv+ky0aZNLtefIkMkL+oF8ZtGNofBWFxyH
50x+yXQ==
-----END RSA PRIVATE KEY-----
```

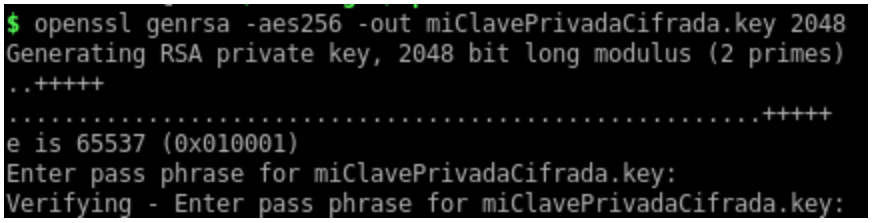

Imagen 2. Generación de clave privada protegida con contraseña

Resultado de clave privada cifrada:


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

Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,6EC02F0EBFCA1B600B520B8B08907944

+Fgq0tqlJkFm8nv0xTKyuC4apd/rn3s6pdKvU7NCE+miIXSkDq6BYjR9xd+JL98b
hB+si6WRIfOZ1rfrMRBv8vkzCEcraoFSbiKKdPdC4iXLj+JH0QPOajRZXFwtt8Vi
+8GFa/Jbds8zJvkIwIqb9Su0sp9m5hzSKDb+UIONCx2RYREDIasmRQE9Iv8ZisQO
r6Rs0vLYMz2f5jdXrO/kgCcxCPI/42HTMIDpcyldZvTqycUKHKImhFYKcEE1nKuL
3anUVryWK/ujRl9phGO9jv2RhjEtVhR0nIXbDbVI9bixNDvnPgXOmTOlBnJ9CK59
A/uKJ3+KxEUWahAGxO36ZqYtG09hnaHFScrndFz4j6gqN1jiif2yYhISZs96QgRs
GIG55tVf8+0mUWXlIRcHnSbzKPJPlg8KH1Cr42cEy+F8lVx+NNc/NkVktNQJA5Wg
p6jPjwQQ4OZNUagJNRoXpqK9mW+qVuNy9JODmWTRWZdHbe+zlUu54Ng/yA1QhMh3
SrzqmbpvDaqJQ3mHtIZM2ZLT5CZelofZaYMm0ibYWkxgaKxs6pY1sRRaW6fT1/K9
XZy6w9IvURoQpJXlwZPOovyd6DzFYrB3LPv6KmvXGNr3zaH2/7eolRl5b15UNFSu
2H7UXQkjAzBN5eJV59Yuxf7mpn4EsyEvxxLO+N+NhstUbWyy/y0An3DmEEgeUcbE
uyEY3cxbA2o+aCgpnlKMGBa3ptvW9pRGI1D0JCl35AZ/SgaTJEWMCSN0STGpnXoE
rYVsZ8ty+vVEcWeYLcLuPYDj9GUva/95MpugOja/rgy44QOrURFj4T5cJ6w1kaQz
NIxNWYnQZm4dXEYXY5asNNzOwF8uhOuyPTrT7KX1CiA4ZIjum0mJn72C0v3PrvsD
Q3zyjiKojCYUEEe5Ss5S4bXWdMG+S8CSWudIOiNjo4Jmd7TXk7n8iMNqj+lcQ+Jy
P0TpNnkDrHVZ3AZfJmCxV8fR97D7ruGIZwSMGQOmiJYz3NKDZTw2uLG1DwaxO8jV
XrSIRxl/xnIV2DzSlrgB1xw/NLdRy93WSuHetDzgI+3UwkF+9y51eg39WRZNmA2o
7rRWrbem0CEVH+UcSRWY03nZCoqBvvawrT7recxJ2FgqKaWXjwmgDcb4KLPXlqZe
4jFoG1FxqEPLuzwe7MVJDyNWuRzYc5p/YDYCfF1kUMHDZs2k2eMtUqA75jUY9MOi
QVyatf7WLrfDthenSSjczZ2kCCAebOdpSQoKf7THfo67K3N4doSPX7y/PeujgB//
bR4qzrIt9FDYxyGxqSenhxfSuKp+NpmzpFhvZ9dEtQVNBh+ouOBN8d5cH8aZLTOk
DULoES6sBmS0LoXlgJKtc9ODzX2jTlE+5K6gLUCG2NxlDIXNii2Q1B0rA5QDAn7R
1MLdavBRWCSIyQzbC/WNtWe/G5A8xiyyxl2HGcH8cy3spZrUSwOoueLrg1Tsf0zX
0UVoZ4teeg1LpLxO3Nr06mNh6L/Scv3Q0KfzfkvJ9ofXaR/tvNhAPXFALSdGkVb+
HOU2DlxQu2aYfOefND5AKMZe84hAFN2gd/VjxwSScYCjQY3Td1mNW90KHfNtvAxz
-----END RSA PRIVATE KEY-----
```

$openssl rsa -in miClavePrivadaCifrada.key -out miClavePrivadaPlano.key

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

MIIEowIBAAKCAQEAvbUbsgAnOlrdieRmPnof3yT7+q4qMDF3XUrqKslQEQcsE5Ml
BeGY/e735itrVDbE4r6oOK0qbWZuspoOUb0pESPSC+vmFgCqHRhLWT8KEN+mQFKk
lsNzCwJ09hho6HD8JCCFGTmyTOt8Yy7THp2RPT/lzZ9IoRhJ2btR3Qjb8rVkeB0i
b2GHDBWq1Zbj/SDUhheyGM1EG4mApeRSnIkGyxkGgH+3NvDreVuwd7z3I6E+CyJK
XlQlB09Q0PqDSzZktqTgNFPrm/juBdjD5nf1f3Nm7FT8P0nI5yvSqDsYGjhBD0l1
zRsXmYf4ahLL9gVP9Gt95bAujukqwB+rrYxwVwIDAQABAoIBAH/rv+EneUxAOWLi
QI+gih1OMxu2lXwp3vNpsL1pQjQ5Qd9xOWXd2exhV4g9fwIqbFj5dzXAjvt2Nu74
Mu+rPiXwoZKoX1421H8KAsULXR5DsTdugs2mvcyOu4+2pgcXKO6zfwyjezejEx1O
Vc4vMeC7VZpx7eezGRlY1rrVXnsp7Hfn9WZnSKY+ILTDxsj7xeyeWC68RMEE5D0c
kTsQvy0Sm0PFHRAjW1ZrgEGJXMyVffaNMi2rJ6DAUQzQOa/xPmualgm+EX3PPV42
fo2colbrG9OYn6mxtmp9tEuEuH5tEnsi2Hb1ARttGu7NcMKuuz/sKqoz5FnyDi7y
S7rAGwECgYEA39U0PoeKhZnElKXieZp/LRxPRBdhd5IzJRVxnIMNgbyqdh+aDwyZ
NkzoXY77PFUFacXn/mB88z26LcsgjHJO3zKENjJvYMl48bzFLxtOKCu2DF5dy9uz
hprJq1cP28K9NrvrnBtsQxbLfanVufB3bDHLVg13vZiFDyRdWSG4iiMCgYEA2Phv
Be5Y3Wflh7XjhqxlItKt5MD6bFf45jYqtBvhghpgzE9I05rcjbmqP44NvgRCygFR
DBFR+S4CN+TY/+35O/D7ZQYKM1mh78mcOETLub/rZyrbpGtFnwG/N8MHQAfsY/+j
zssAQTq6rn5h9k7HjXoaEddNTdjJdbGhW15Xwj0CgYAr5q9GjGMY7R3nYdnXq/vB
p0nMuyE8yIoLffc4kWO2zIBKhsw6o2fxhIgWwZJ5NNvI8S4dcGNRegvoK20I3uql
UE0qLB44R4vXLgUmxh5ANsKQDnorH75IalefqYXMvpdKAvWlOqOzTOdAkG0A+S8T
I3kUObQAlceTPrioYLrHLQKBgQDDSSBMm1Havgfm1Tyb25EP/cZMbbE4URoSwtA+
2hVoD6vuWLI421sGKQVmPMp7q8Qdo3+6N+CrQdD3VABIon3AiM8NB5mozFUnyTPV
pX4kiuwrKHUXEQJR8rWUT/K3nCoVe2OJ3kc1btHV+qTbl96epTbPthS7K5NwXlfY
MBsXFQKBgBVzCNYoa+UHMRgqPr5UuMd6tDVsCyFqjCNhmzt2dfbmS771XZ+oZ67I
aemJBB1S6caiabVt21z77hIQe6ZMObdMV47aaI+IUjsbxx5azktYVVtEbrDurFW0
QOLMFj5sBD4MRsNLeGgtrBxMNwYeRS94FHFVy39PTRU2u02IH/YQ
-----END RSA PRIVATE KEY-----
```

Para extraer la clave pública del archivo escribiremos el siguiente comando:

$openssl rsa -in miClavePrivada.key -out clavePublica.pem -outform PEM -pubout

```
-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyY8k+w6wBp8P8pwfajrY
uz6XxdYrak3HmR+g0ToFjQvYnHVLxenK572DCcpBDamRl1G8ILtNmgfZBAMSXja9
qAgcQqibvntBRolr1Cl65E6bi4NqxxmN8FBxwDzn8O6bRdBJY6rEBqSqzEKaiGe8
5UVaFFS/TcMnUP+I2viDwQFaVsYpcYbLTxlMFvFxjICnkgbtfDAEmfnroHbsYqlo
2fh9nnQKw4RWwCt8opzFNa6H0ryzjHDRWGuTgWU9wmX3dJa4Re8hj6A7hh9FGtRu
g4kJh/CpQ6mZawdlXYCBdvGlvwUcnXCpbjn05ekmU72TRd8KRk8BOYlXQsOCTz3s
UwIDAQAB

-----END PUBLIC KEY-----
```

2.2. Crear la CSR o *Certificate Signing Request*

```
$ openssl req -new -key miClavePrivadaCifrada.key -out server.csr
Enter pass phrase for miClavePrivadaCifrada.key:
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]:EH
State or Province Name (full name) [Some-State]:Gipuzkoa
Locality Name (eg, city) []:Donostia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EHU
Organizational Unit Name (eg, section) []:SGSSI
Common Name (e.g. server FQDN or YOUR name) []:SGSSI
Email Address []:sgssi@ehu.eus

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

Imagen 3. Generación de CSR

$openssl req -new -key miClavePrivada.key -out server.csr

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7zCCAdcCAQAwfzELMAkGA1UEBhMCRUgxETAPBgNVBAgMCEdpcHV6a29hMREw
DwYDVQQHDAhEb25vc3RpYTEMMAoGA1UECgwDRUhVMQ4wDAYDVQQLDAVTR1NTSTEO
MAwGA1UEAwwFU0dTU0kxHDAaBgkqhkiG9w0BCQEWDXNnc3NpQGVodS5ldXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9tRuyACc6Wt2J5GY+eh/fJPv6
riowMXddSuoqyVARBywTkyUF4Zj97vfmK2tUNsTivqg4rSptZm6ymg5RvSkRI9IL
6+YWAKodGEtZPwoQ36ZAUqSWw3MLAnT2GGjocPwkIIUZObJM63xjLtMenZE9P+XN
n0ihGEnZu1HdCNvytWR4HSJvYYcMFarVluP9INSGF7IYzUQbiYCl5FKciQbLGQaA
f7c28Ot5W7B3vPcjoT4LIkpeVCUHT1DQ+oNLNmS2pOA0U+ub+O4F2MPmd/V/c2bs
VPw/ScjnK9KoOxgaOEEPSXXNGxeZh/hqEsv2BU/0a33lsC6O6SrAH6utjHBXAgMB
AAGgKzASBgkqhkiG9w0BCQIxBQwDRUhVMBUGCSqGSIb3DQEJBzEIDAZwYXRhdGEw
DQYJKoZIhvcNAQELBQADggEBAFkuOQnLfo3fLUp5eWF/ygHFis9+ZkcMXBGuOeve
MYeLhWHyEdLkdd8ln4zTpnWFCFdKuzk8UAy1xGfRFg+v4ovrPQRkZxKoazGkAxdX
0jf5YCpAm5ehx/mIdpzuh0rHD/1Vx/ed3+kcSmv1BPWRaf4qkmp/NznVKrYjVImd
19wmRD6WfIlEWXreX2tX9aFtMkCooxLzE9/nvZr85OTAqGuO4UGqUxAPqD+sNbyU
fh6PCcvQdUizKhnZ/0VnttuC/ffL1VxRXZPFm7Vn+zG1jKmIbqRk+mY5tcPEFiHx
xpG8H5yZrsMRux10JzifQ0XFl1Y7A6MJV5UECh7RAfYgdRU=
-----END CERTIFICATE REQUEST-----
```

2.3. Generar el certificado SSL

```
$ openssl x509 -req -days 365 -in server.csr -signkey miClavePrivadaCifrada.key -out miCertificado.crt
Signature ok
subject=C = EH, ST = Gipuzkoa, L = Donostia, O = EHU, OU = SGSSI, CN = SGSSI, emailAddress = sgssi@ehu.eus
Getting Private key
Enter pass phrase for miClavePrivadaCifrada.key:
```

Imagen 4. Generación del certificado SSL

$openssl x509 -req -days 365 -in server.csr -signkey miClavePrivada.key -out miCertificado.crt


```
-----BEGIN CERTIFICATE-----
MIIDhTCCAm0CFFDO9bvWiMeUdgC/iG6p0KRLWbF2MA0GCSqGSIb3DQEBCwUAMH8x
CzAJBgNVBAYTAkVIMREwDwYDVQQIDAhHaXB1emtvYTERMA8GA1UEBwwIRG9ub3N0
aWExDDAKBgNVBAoMA0VIVTEOMAwGA1UECwwFU0dTU0kxDjAMBgNVBAMMBVNHU1NJ
MRwwGgYJKoZIhvcNAQkBFg1zZ3NzaUBlaHUuZXVzMB4XDTIwMTAzMDA5MTIxNloX
DTIxMTAzMDA5MTIxNlowfzELMAkGA1UEBhMCRUgxETAPBgNVBAgMCEdpcHV6a29h
MREwDwYDVQQHDAhEb25vc3RpYTEMMAoGA1UECgwDRUhVMQ4wDAYDVQQLDAVTR1NT
STEOMAwGA1UEAwwFU0dTU0kxHDAaBgkqhkiG9w0BCQEWDXNnc3NpQGVodS5ldXMw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9tRuyACc6Wt2J5GY+eh/f
JPv6riowMXddSuoqyVARBywTkyUF4Zj97vfmK2tUNsTivqg4rSptZm6ymg5RvSkR
I9IL6+YWAKodGEtZPwoQ36ZAUqSWw3MLAnT2GGjocPwkIIUZObJM63xjLtMenZE9
P+XNn0ihGEnZu1HdCNvytWR4HSJvYYcMFarVluP9INSGF7IYzUQbiYCl5FKciQbL
GQaAf7c28Ot5W7B3vPcjoT4LIkpeVCUHT1DQ+oNLNmS2pOA0U+ub+O4F2MPmd/V/
c2bsVPw/ScjnK9KoOxgaOEEPSXXNGxeZh/hqEsv2BU/0a33lsC6O6SrAH6utjHBX
AgMBAAEwDQYJKoZIhvcNAQELBQADggEBACTkuFa0CbKPt2qsfdZzn828uSdEMkB3
feM49u7WXDAoTNoRz13qphAiaGVj6z9bZje+AAIsOBsD/klOhYMtVjUTynQ2U1wo
e+nUZQViy/UxkVqqPGUHBRwAMN8ovtPwtgkK4doYgiLskK9TUOv2wjDKlwP7HLPe
ENcPKK0e7//016cLgsLw8PKio5EIlUhdgpUtTScA2lOIsTlJfaE9u6m1PoGG6fTx
Two+yKEWIRthmVFr96RTnqEjT6JIJn2jgAp0/dcmQ2jBxxmxNs3dhBTXbezoYKwD
bYh8OXB7xuk/yVSBUgsgeSx+Z11C1atss1c/xeECDC+zy6/vzqzSQOY=
-----END CERTIFICATE-----
```

3. (7. Otras aplicaciones con nuestro par de claves)

3.1 (7.1. Cifrar/Descifrar archivos)

Damos por sentado que ya tenemos nuestros par de claves

----Para cifrar----

1) Generar una clave aleatoria para cifrar el archivos

$openssl rand -out claveAleatoria.txt -base64 48

BLjPAMB1HLu3qmOWcaIML5y33e04LiWWwBsqMP6lLg9HNWcWXbL2dEr0Euy1XZ6V

2) Ciframos el archivo con la clave aleatoria

$openssl enc -aes-256-cbc -pass file:claveAleatoria.txt ...

```
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ openssl enc -aes-256-cbc -pass file:claveAleatoria.txt -in proba1.txt -out proba1.txt.encrypted
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ cat proba1.txt.encrypted
Salted__*@{g@d#▒Z@V~@@@zF@i.5$@\z@1@@@u@@@予KDarthDorron@tux:~/Deskargak/openssl-1.1.1h
$
```

Imagen 14. Archivo pdf cifrado

3) Ciframos la clave aleatoria con la clave pública de nuestro amigo

$openssl rsautl -encrypt -in claveAleatoria.txt -out claveAleatoria.enc -inkey clavePublica.pem...

----Para descifrar----

4) (nuestro amigo) Descifrar la clave aleatoria con la clave privada

$openssl rsautl -decrypt -inkey ...

```
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ openssl rsautl -decrypt -inkey ./miClavePrivada.key -in claveAleatoriaEncJon.enc -out claveAleatoriaDeVuelta.txt
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ cat claveAleatoriaDeVuelta.txt
/nTPqxKJEkN9X/p9+0wQgaGU37EimrJQXfObG406O1MTSVNoBDlNDCiUpPdvDOQ+
```

5) Descifrar el archivo con la clave aleatoria

$openssl enc -aes-256-cbc -d -pass file:claveAleatoriaDeVuelta.txt -in …

3.2 (7.2. Firmar archivos)

$openssl dgst -c -sign …

```
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ openssl dgst -c -sign miClavePrivada.key -out proba1.txt.sig proba1.txt
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ cat proba1.txt.
proba1.txt.encrypted  proba1.txt.sig
```

Para verificar el archivo nuestro amigo tiene que escribir el siguiente comando:

$openssl dgst -c -verify clavePublica.pem -signature ...

```
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ openssl dgst -c -verify EnekoclavePublica.pem -signature tablonSgssi16.pdf.sig tablonSgssi16.pdf
Verified OK
```

```
DarthDorron@tux:~/Deskargak/openssl-1.1.1h
$ openssl dgst -c -verify EnekoclavePublica.pem -signature tablonSgssi1.pdf.sig tablonSgssi.pdf
Verification Failure
```

4. Resumen y conclusiones

Sin ánimo de ofender a nadie es el laboratorio que más me ha gustado de todos los realizados, muy bien explicado. Lo unico para el cifrado mensajes sería interesante el uso de thunderbird+enigmail.

5. Fuentes de Información utilizadas

[1] https://www.howtoforge.com/tutorial/how-to-install-openssl-from-source-on-linux/