

Práctica 3. Cifrado asimétrico con OpenSSL:

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante
alu0101364544@ull.edu.es



1. Generación de claves	2
1.1. Tenemos que generar tres claves privadas RSA de diferentes tamaños. Anota en un pequeño informe cual es la salida que obtienes en consola, el tiempo que tarda (puedes usar el comando time de Linux) y el valor de la clave pública e.	2
2. Almacenando las claves y generando claves públicas	5
2.1. Cifra una de las claves privadas anteriores con el triple DES.	5
2.2. Convierte una de las claves anteriores del formato PEM al formato DER.	6
2.3. Muestras las componentes de una clave privada en la consola.	6
2.4. Obtén la clave pública asociada a una de las claves privadas que generaste en el ejercicio anterior y almacénala en el fichero pubkey.mem	8
3. Cifrando	9
3.1. Usando la clave pública RSA que obtuviste en el ejercicio anterior (almacenada en pubkey.pem), cifra el fichero DancingMan.txt almacenando el resultado en el fichero cipher.txt en formato hexadecimal. Genera 1 también el fichero resultante en binario porque para descifrarlo posteriormente lo necesitarás con esa codificación.	9
3.2. Usando la clave privada correspondiente a la pública generada anteriormente descifra el contenido del fichero cipher.txt y almacena el resultado en el fichero plain.txt. Para poder hacerlo el fichero con el texto cifrado debe estar codificado en binario, no en hexadecimal.	11



El tiempo para la generación de una clave de 2048 bits es de 0.14s aproximadamente.

- Genera una segunda clave de 4096 bits indicando que la clave pública es la estándar y almacénala en un fichero distinto.

Unset

```
$ openssl genpkey -algorithm rsa -out  
clave_privada_rsa_4096.pem -outform PEM -pkeyopt  
rsa_keygen_bits:4096 -pkeyopt rsa_keygen_pubexp:65537
```

```
/mnt/d/0/1/2/3/4/5/Practicas-SSI/Practica_03 Cifrado asimetrico OpenSSL on main !7  
cat clave_privada_rsa_4096.pem  
-----BEGIN PRIVATE KEY-----  
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwggkoAgEAAoICAQCwzN1ZIjckYkdkK  
xJqV/4wtKmw7DLW92FsnYhR1cxGMFAUX+SAJoTGusQCLsdegB9SbqX/a7jQM0qAS  
e0J0U00z4k3rxb3KATKuPf846au2T9yNJVrEVqmwQDmhIHTTkgPSE3eK9Mp8/yYR  
v40yUQMAFGAZrGhmKWEFFTy0vIKqbXSXh+EhPw8jB0tMdlh1cJx336WGitTK3sUR  
8K4/wjBHiGP4SD4cQimr54UVUb3+fRCwxY0eN92HFEizXglUm6E32X88kGyKHMctq  
w10kr5nVZ0BgUe2ju5g5CDWgoN0SdhCdtLT70jarBV6cxYVMtxSKfGJ1ftSeV1sL  
vy07W0LZWNRrta/ORIw01Kr/qW1LTxsh14f/QAFIaHfbZYCrW8N02a6UGUn85Pn  
iLylLW2zGJzChaw2usiAne9K1WmM3V1KedHUQScPY4qs92Dxzg8TnHgtbMI05F0t  
IxAO17BrC5MEHtIrapV01rNmicrocyQHqQECdi+k8X5xyntcTjai02+I+VhpcmhVs  
1S20guRmUoA7955yCGkUwNT03siu8sP3HJ8DU4qzq4zgycemOZ0wmHuNxbnyeb  
7Jw/16FkME5/x5D7wH9uNE6mygzXuFvi109DKDdo81wqMTdGM9oj+wxnSf7153a  
ZwItQ+/drMYF8VoQ8cvFR9ydrDO+4QIDAQABAoICAAXsw6E0TPVDTtM72JF91hf  
I10mOpPzT3C4qrFZ6xVe6WHDiTxwbzYLu/kye0ejY4pY5o47a9afK1qbM1h1HcH2  
m+05M3hE2mY5Efvr+oEvv06+kG/1P1/whpiki5zLN6UAgB1pJaHtg661wrj1Zx  
1JXfqr+dbseEqdyiZt2Xv+/BD7gZwSPbH3iFm7vAh5nTzpwA5Iss5n1Iq8o6s3v+  
Qc5M+3nedL+MSW8yt10DN087m5R06ndXpG0YktQvyYZxVsQJrrS9UhtZh5v3Q+j  
/2ok7WQPBSr/h+6LXYU8HCfw0ZzksVTPYAGQc/xjaUaPzwvhdxYd7jyp5jaCQy3v  
mGsRf0CjaVqXHUsg0cvUyMudDOW11B9+dYZrcVukw97kpRVCPztVtCTUJ5DC+CA  
6KqF/xJZScUjawn4IK4eziqq8bWfWjn/4z2mp00xDPwxSu+wXvqkKXNwct09W  
Q73bconzriw766hvr4w0q7/b0AYSIMh0x8aDSipLAhDB46/TJCotukX06dUaZkv7  
Tq8Fk08WKFRI0029TnAm62FBs1J54S0spuGr5Z11NoFRNahLb8jNBNI8ZD1fSRbC  
ahP5J+05KogrNtRak5fwl9I42JWc/Wz3uwUJ37XggIdS3xTnnPPZDtZzcJ5ZE83iQ  
hDXJyFSY4J1VP/H/2b2SxAoIBAQC8Cfq12tRhglYD3FzFuOX1wPwm7NPNczg1JGkR9  
dcC6b14q1F0UwWbqH20ArDdXMapxbMnuSoV5+kVsQ4vqd8N/MoXU6j1iUTC67Y  
tYIKfIehzo4QjVa0gbQ9qieZC0V4BXA2TehDzc7Y/afjgDKiv/3btzGFyNqTE6sD  
5AsCDVda1g2vhljrmcJBZFaNEIf93gf4mzI9WYQp+Eq0B0V0Bx8QyG7Af9JfGm  
cea1eVjrXrajN01b0kXXRd9Bq04Kb9vuyXgG3HU9CBuSg6JhpyGBv//vnfeR7+J9  
G7C1ZjCaQZOGfyT6ILJbf48WdV2bmhD9jL7gh13c2LYF+vWpAoIBAQDswsn6fbkN  
AbTubEjStwVlaqc84CTEGYnkyeuY7FhnzltxtR2isb+liVeG7AFMWREAF7ifKtU  
sfqDZBDuShX0XrUzp0V2RY2Y8C41YUvYfjsa4B8p4pxvCyIKEZKJV+8r41rg0qp1  
W4S626xHBIqWRCQ0zeGJXFS0PS1EVQPKodEoiivqNTd4Ia/5RBE3TTh/+HqK8ju  
Rqh1Iop5+omKw13HUMeqKT8jjjc2K5Ua5G+YEmYbH0gAwxs161ejd518x0+/+ASi  
9vIeS4TYmiYoyMYExJ+s7I6INeFspwpmR5J05gv7V2PeZjb2hQmBRLqm7Mp8T8hr  
Wx90prBDKdJ5AoIBAQCvmdopjewC21sOZPhiaQm9kwdxdKT73z0sbuYPKj473tr  
17h2B9tYdHSE1k7v/I+hnHf8Nq0Yu+4bwLbwyABnvZ50aAooISK26spMz0ReCqFW  
9+Avk05Rr3a0x3wnK+mvRdTewa6P81hx2/LwukGniJhb31d6I5GH23rOkEVb4Q0  
MmchbXY1det6v45X4MmHtMDXdc0FeTgyhDUX1g911j12qpc5i7mFTLp4rhG3k1T4  
qQCCW1fXGQ4fyXY2XtC/+cxRae7MJHDpxiooIk6DKv70W0FT7Ps80pbd0hSd8fo  
sRf12QKd637kd6EWBnXLo1ayMYfnIDSjkzWLB3RAoIBAFJi9ednYQ+ypdt19Pcq  
Yel+t/9+ORdmJmzJMHsHarsdRu9YFqD8n2BExEW9I3Seh9ND5E2Wu6Cfny8Q49M  
jG1u91bW+J0HwYwPe61LWEO56sEoMYKArkrT5LLNkPqxvounJ1QNX4q6j3jAhBd2  
1oG/X4ipRjGf+OP/4cKYS811IsE82XBGuZW4ZGcKYuC/VnqEuy8MDZqBv0fDCul1  
f16galjWtWQ8d8hICDKih7KUegbZBekFwDFZ2RsaXLqXL1A+2sZ2XxuSfJuaQ7  
vxP2pNC8/GqUdbVRu/cUtdqMZOfclf1RzD0zf1yh7L7yZ3D7W9NvuGwGFjo3U92p  
UwECggEAKpfj1UfyU6t4sh31N7iwj1LiCBpF5Ud/ybducjbo1Tv1D0/neHdBzfv4  
AT+qaeV+mEB4oCE1vb7S037Q+uw3yhG5T6GzR9GUmqVz0QoYamTQvqV5SC+4UKV  
w8PVNqepRQSeE1gcHh9UmR+rMS0eHATVwFowZOFzS1S2aK3tEPdjbnuaalnsUM  
BUTSt/79cN6Ys9QDAiIy3W/1CugYQcoGLb/ACSbd062Cn0WdgaFxa4965Q/PBffBj  
7wXhInovJah+hK0YMDfw1+n6WBS2FGzgtSMEHJJEE8PHbuxsG/pCMDVXXyZV78k2  
go76WIB3+J7qWq8pgD2q70Wd2VjRQ==  
-----END PRIVATE KEY-----
```




2. Almacenando las claves y generando claves públicas

2.1. Cifra una de las claves privadas anteriores con el triple DES.

Unset

```
$ openssl enc -des3 -a -in clave_privada.pem -out  
triple_des_cipher.txt -pbkdf2
```

```
└─$ /mnt/d/.../Practicas-SSI/Practica 03 Cifrado asimetrico OpenSSL on main !7 ?1  
openssl enc -des3 -a -in clave_privada_rsa_2048.pem -out triple_des_cipher.txt -pbkdf2  
  
enter DES-EDE3-CBC encryption password:  
Verifying - enter DES-EDE3-CBC encryption password:  
  
└─$ /mnt/d/.../Practicas-SSI/Practica 03 Cifrado asimetrico OpenSSL on main !7 ?1  
cat triple_des_cipher.txt  
U2FsdGVkX1+TX66Pm53fZihBf00JVND11KXPqP8wAznXg7ft+wWPzXfjTdmTk6ZS  
m0NauqxtGnR5JXJttpuGREm1Wr3TTZN25vKwjGRanQi+YIenUJHhro/o4Xz008kj  
3sqCa2S3mL6NI6PWyEwsr9fmxX1ZDizWjx5G16KhsHBNAwB6SKIQQ5vfEmhSN5ro  
QbFSAjqsusahGA0hgbUPfffiAeSjB0Xysz3gQQMmzjkgKLCHN2qe8vtJC31Zx+tYu  
CuH7NP7o5/VxiwDZ31DhBpfviahk6Nr9c0/TUopVQQq/U4erAEiDQdBzXFA1qu0  
nktnRqOJzVPhMRS0/GrZ8MwLq4SI8I8WaaMuMHbyGGgpS7cGSpQcGN1QfjILxOA8  
DQ3HSQYkd0cNPQAL5ME7sBLp9BQo36Br75V3SRgqBD0UmdUfQJRpzwwP1LLVv4X  
/opZR/Kyp4fR2JBPUAzeZPRLCeUG9do631Hz/TPlvMr8MjCtH44seP0K4nelTH/t  
9eZIknrIpgxyj0kFeYMjUd2bWHMKxTfphMeON5U3sTB/v+50aIkgZq6LiSh7i5gP  
kpsBGszPYWAdrdI9wQIntQxeCLaw7nWdXFrUNJhbI0NB5/qMc4qY5MOCT0Xvtqb+  
cnGH/ZsVuRw8GNqrBwL8BtcwYTnJK/xbcVrEVivVFPT3ohdmo0qbjM9nbEX/5ILg  
zxaRBzFfhuDqahXjKZG1IRdZ31R7ixclD0DNn9F8nvFngEGeNFJtwkD+vlrIFCJ  
1+btw4/VN0R2QP65taUSDptMej3tzC9P4tGbIIyS8ymhSszwjIwwJcKYUsfliUH+  
0VfP0Hm5KgFpzBd/54ph2VYmy/gDIKe9845VindpnqwsKc3AyGQ0lu+8MU61y809  
x/J8Ka4nfcceq242hf1+lw8uMGs+DKdKga+PkI17HZHFbYQ00yQzA8hZT2kdyim  
rGzk/FyHLDm361cxTx/omfV4YNeLgw6xq2vzUQSKWNE8eyJ55HpDDQMplwnSKpmQ  
Gq2XJLltW4yd7Yp3fzG6xuXMF+wwPxejY8CaCN0RU+uFTjXdu3F53NknfSCUbnI  
PEPW0oNlNxBVZXC4NY8pxj4vgIzaSxLUxUmsVc6YyZnFkyBoIuEPLN0slrDl1tr  
RDJyLdr021yzgws6w/7kVg0/1+sOUXLhzVzUaFCQ6CIB5dj1jj4aqGIDKfKQWIC  
wwlm00dn60aDR/zD/XjpHSMETsNxrXPYvJ1d4M0PS911z5HB9uNFP2phSzC3TwN  
9bi01XliCudSD3nNvnHwRbheySQGJ7dwFDtAambA8lekDS9B1tXu16ejrroEtPFb  
1EqdpV+99Yd5QvzLqmDQ0Bdo143W5oYTGBlQSGtapnfUuVw/2HUHjZWfZzyovWz4  
TR17yF/kzwkgFc4cQUP+bC6+x0MVeE804mJumGdjSBOokuDFuQW7860hLITkxbUg  
2hEbRyF44kCFs9kAtvuMRno9kvFwyQsAA3pKYthkrh/aYD2zikEf6gOxtDOPOKh  
HZZHq26whd6RS9bG/pFgt3zhBMIdM15dvfzJjHErZ/+UilIrKYBGrrQbPYxgSsd/  
c80QVXKFYXVex6YXW8CPj+i1zc6FA3G+q0qIaYGN3bNotmU11+9o5sIsvXJf7gy  
tLeK8B1XF3zqwKemcStvWU1h9vBhTbVpa4zArWrJRzuZnKTC9TV3qyEV6nyWdC3U  
uNV7xLxdy7b1kfTw1zqgbfXoC0J9H5BzW/iKcLVlunbAcgT+nKHpAUC4USyr+ZCh  
6fb5tjCMspnk+eS/Vxi/dOAWXbcP4KZETG9+/RWHucv+sXVsE97ekhmFbCMVspkx  
zmpZpZRscvtv5weDr8CfN1vHm8fXK5G1ZAB6R86saBh8DLgtfiAjsdvWo4RdexS  
WpW01wOwFRnVnIrKOnqXG0tVExerQQGBqKFemit00GCD2adbgqVuQVRVrAgC9u7l  
r2E6EtQjJbodgeGhwf3K/ChiZ9sGM07cEZSh9SqsNwllKkL9rs94cFgyVi/YQ6NhL  
5u/cWy+odpIPVivc+DDT47t6MZ0Lqd4nLgZ3/mojVg+C86vPvJWH3qsWv3FhSKom  
yx2iS2qlEUBcxg9kdxaqulRD0Fn+Y3UKKkftqZaF4W1KGLkN9GkRd3DeLkfZpV1j  
mTrg5d+cnDNmrBf1SVTDnMQ2LegmOb78czK7sQ/dmjpg8mDnR1xKAQV30ThAgE/H  
jC7nirrR0neaoqC57fSvvhHqkeM0pprogfurYdTSLQIPXXVfCvY9X1RBWhKiW5g
```




```
$ openssl pkey -in clave_privada.pem -out clave_privada.der  
-outform der
```

2.3. Muestras las componentes de una clave privada en la consola.

```
$ openssl rsa -in clave_privada_rsa_1024.pem -text
Private-Key: (1024 bit, 2 primes)
modulus:
    00:db:62:82:f3:e7:55:43:0f:93:71:11:d5:b3:e3:
    02:66:d2:7d:65:9c:dd:29:e2:15:35:87:40:ee:32:
    23:f3:2e:77:79:5d:97:dc:5b:42:70:99:de:08:66:
    62:9d:89:e2:b8:26:6c:9c:79:b2:35:d3:6f:d0:17:
    5a:e3:f5:14:69:2e:e7:50:1c:11:06:af:23:4b:89:
```



```
06:d0:76:3e:10:15:fd:53:d6:d3:41:13:78:97:b4:
be:6c:22:6c:24:dd:4c:ec:3b:f9:ae:5a:b5:db:df:
76:3d:18:a3:88:5d:81:14:0c:c3:a8:5f:7d:a6:90:
3c:66:a9:81:d2:f9:f4:bf:65
publicExponent: 3 (0x3)
privateExponent:
00:92:41:ac:a2:9a:38:d7:5f:b7:a0:b6:8e:77:ec:
ac:44:8c:53:99:13:3e:1b:ec:0e:23:af:80:9e:cc:
17:f7:74:4f:a6:3e:65:3d:92:2c:4b:11:3e:b0:44:
41:be:5b:ec:7a:c4:48:68:51:21:79:37:9f:e0:0f:
91:ed:4e:0d:9a:38:64:27:56:34:10:a8:16:af:94:
e5:29:ce:b3:ae:dc:9b:29:f6:e6:ab:29:30:21:bc:
2d:9a:19:0d:50:ed:08:fb:de:37:6e:87:5e:ac:f3:
df:8a:5e:0a:c5:78:da:a1:b5:ff:48:aa:84:8c:92:
7f:93:dc:1c:54:ab:18:a4:ab
prime1:
00:f6:30:bf:c7:94:8e:30:71:46:a4:77:e0:1a:4d:
24:1a:87:82:c0:2d:37:e6:3d:18:31:2e:3d:85:d5:
a8:db:b6:2f:1b:43:b2:f4:73:34:cf:2b:cc:24:5a:
76:ef:77:be:c1:74:ae:3c:98:ac:02:28:71:99:9f:
73:16:8b:c0:a5
prime2:
00:e4:20:55:53:2e:5f:82:8f:fd:85:37:31:a5:e3:
65:b0:8d:12:24:4c:08:6f:73:4c:e9:4b:c7:77:02:
82:9e:09:43:53:62:d5:9b:34:a3:a2:7b:21:67:38:
e9:38:c1:62:ba:50:0d:23:1e:27:b2:54:97:45:b7:
e0:e2:c4:07:c1
exponent1:
00:a4:20:7f:da:63:09:75:a0:d9:c2:fa:95:66:de:
18:11:af:ac:80:1e:25:44:28:ba:cb:74:29:03:e3:
c5:e7:ce:ca:12:2d:21:f8:4c:cd:df:72:88:18:3c:
4f:4a:4f:d4:80:f8:74:28:65:c8:01:70:4b:bb:bf:
a2:0f:07:d5:c3
exponent2:
00:98:15:8e:37:74:3f:ac:5f:fe:58:cf:76:6e:97:
99:20:5e:0c:18:32:b0:4a:4c:dd:f0:dd:2f:a4:ac:
57:14:06:2c:e2:41:e3:bc:cd:c2:6c:52:16:44:d0:
9b:7b:2b:97:26:e0:08:c2:14:1a:76:e3:0f:83:cf:
eb:41:d8:05:2b
coefficient:
```




```
00:8b:a8:aa:25:80:be:48:0d:e4:18:0d:ae:6f:b8:
21:11:0d:11:4f:b5:1f:3b:0f:42:66:e9:70:81:6e:
09:40:cf:bc:03:11:e1:fa:86:31:e9:98:86:60:96:
65:94:d7:aa:47:83:1d:19:cb:d3:62:76:c4:7a:33:
de:d8:7e:ba:b3
writing RSA key
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwgGJdAgEAAoGBANTigvPnVUMPk3
ER1bPjAmbSfWWc3SniFTWHQO4yI/Mud3ldl9xbQnCZ3ghmYp2J4rgmbJx5sjXT
b9AXWuP1FGku51AcEQavI0uJBtB2PhAV/VPW00ETeJe0vmwibCTdT0w7+a5atd
vfdj0Yo4hdgRQMw6hffaaQPGapgdL59L9lAgEDAoGBAJJBrKKaONdft6C2jnfs
rESMU5kTPhvsDi0vgJ7MF/d0T6Y+ZT2SLEsRPrBEQb5b7HrESGhRiXk3n+APke
10DZo4ZCdWNBcoFq+U5Sn0s67cmyn25qspMCG8LZoZDVDtCPveN26HXqzz34pe
CsV42qG1/0iqhIySf5PcHFSrGKSrAkEA9jC/x5S0MHFGpHfgGk0kGoeCwC035j
0YMS49hdWo27YvG00y9HM0zyvMJFp273e+wXSuPJisAihxmZ9zFovApQJBA0Qg
VVMuX4KP/YU3MaXjZbCNEiRMCG9zT0lLx3cCgp4JQ1Ni1Zs0o6J7IWc46TjBYr
pQDSMeJ7JUL0W340LEB8ECQQckIH/aYw11oNnC+pVm3hgRr6yAHiVEKLrLdCkD
48XnzsoSLSH4TM3fcogYPE9KT9SA+HQoZcgBcEu7v6IPB9XDAKEAmBWON3Q/rF
/+WM92bpeZIF4MGDKwSkzd8N0vpKxXFAYs4kHjvM3CbFIWRNCbeyuXJuAIwhQa
duMPg8/rQdgFKwJBAluoqiWAvkgN5BgNrm+4IRENEU+1HzsPQmbpcIFuCuDPvA
MR4fqGMemYhmCWZZTXqkeDHRnL02J2xHoz3th+urM=
-----END PRIVATE KEY-----
```

2.4. Obtén la clave pública asociada a una de las claves privadas que generaste en el ejercicio anterior y almacénala en el fichero pubkey.mem

Unset

```
$ openssl pkey -pubout -in clave_privada.pem -out pubkey.mem
```

```
~/mnt/d:/t/a/s/Practicas-SSI/Practica_03_Cifrado_asimetrico_OpenSSL on main !7 ?2
$ openssl pkey -pubout -in clave_privada_rsa_2048.pem -out pubkey.mem

~/mnt/d:/t/a/s/Practicas-SSI/Practica_03_Cifrado_asimetrico_OpenSSL on main !7 ?3
$ cat pubkey.mem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAR78BRdd638G+u57lTHB4
dUbahECbJL001gAS7q5/VHDNto/eBGJr43wBhl8ojq7c+enEu1GoruTHiTKjHLhV
xTuBDJdhKnOnK2K6Zk0FbuCB64V+e06nqbU1bPNxLQm1hgralMjH2tqjM5+dCImN
b2gHgCVF1SVEk3xrCVHK59129Ty4ZfZF/vOj66X4DA8XgwmvHICsLOXRGiWw7Uy9
i9F11LXjQh9VqBHn30mgEftdizwkF17W5Of6j2VTebjxCyrwDVoVNNRqHZktaUHQ
Xq3K3C6nQpx/BLD/eZR90K10U5SLVQwk10fkHdJhLE/wQJ50Q0y+AHfJqjMcFVFt
lQIDAQAB
-----END PUBLIC KEY-----
```



3. Cifrando

3.1. Usando la clave pública RSA que obtuviste en el ejercicio anterior (almacenada en pubkey.pem), cifra el fichero DancingMan.txt almacenando el resultado en el fichero cipher.txt en formato hexadecimal. Genera 1 también el fichero resultante en binario porque para descifrarlo posteriormente lo necesitarás con esa codificación.

- Cifrado en binario:

Unset

```
$ openssl pkeyutl -encrypt -in DancingMan.txt -out cifrado.txt  
-inkey pubkey.pem -pubin
```

```
/mnt/d/vscode/Practicas-SSI/Practica_03_Cifrado_asimetrico_OpenSSL on main !8 ?7  
openssl pkeyutl -encrypt -in DancingMan_short.txt -out cifrado.txt -inkey pubkey_8192.pem -pubin  
  
/mnt/d/vscode/Practicas-SSI/Practica_03_Cifrado_asimetrico_OpenSSL on main !9 ?7  
cat cifrado.txt  
00c0%0n'00,30  
r00Q009.=(0yv000u00:4P*zp0JE0000gfr0000050$  
000h00ux000u.|le~0000 0w~A0rBzn0000'"d0000/00%=000H00q P0a0b;0_00  
o~G060*0ew3000s$0P0]0g7Tj0@09D00]000#50000aV0H|0  
J00E00H04000$ 061a0~0E[|00000/  
0  
0J00'o00u00000:A03'{00F:00E00:00$E0)^0000h00000E}0p.  
L0#60UY0[+600_0/Ipe0000]}Z00N;y0+000^00+000 I00j00]00E 00;000A0009]I00J400%xx00E000h00IcG*006j00AR00)p'Y0u`Z0000"0  
0k o#0E0j05000VF0p0B00000YG0~00bx0b0\00M000F-c0?b7.0000nz00*f~!P0;0Y7i0Q*0A0(00G0000P[0ch  
00&0/  
.:0,00500{00}+T2]=0*0~00  
vu0.}Y2D0a00P0000I0=0Bc0Z"Fz0jp3D0:~0000L0kñs0n_0K00+00I;000\}01100j00J-3d=00 0  
00p000q0u@g00H1((000WZ>z0?00$VBY0Aec0200000,0"000)<4S00s010I00v0,00?B000p0Z00WR000v0-0G,000K0,00010A0 0  
00'0@0000]2~-0000000F0000Yt0t-s00M0k0wJQw0k0-I00J 0@-  
00D010x0 0000v0;t0_rQ0"00
```



- Cifrado en hexadecimal:

Unset

```
$ openssl pkeyutl -encrypt -in DancingMan.txt -out cifrado.txt  
-inkey pubkey.mem -pubin -hexdump
```

```
on main !9 ?7  
openssl pkeyutl -encrypt -in DancingMan_short.txt -out cifrado_hex.txt -inkey pubkey_8192.mem -pubin -hexdump  
on main !9 ?8  
cat cifrado_hex.txt  
0000 - 07 65 7e cb 75 9d a6 09-f5 b9 77 de c0 e5 3d 31 .e~.u....w...=1  
0010 - 40 9e ac 0d a1 81 83 d5-05 aa 72 fb 0a 58 13 8f @.....r..X..  
0020 - 16 62 c3 61 98 f8 a2 72-d2 6f 23 29 3f 34 4a 27 .b.a...r.o#)?4J'  
0030 - 1f 57 03 a9 e8 5f a4 41-6a 98 70 a6 64 a7 62 51 .W..._Aj.p.d.bQ  
0040 - 55 2a b3 f4 69 95 f4 d3-c9 d1 a0 0a ce 87 40 b8 U*.i.....@.  
0050 - df b8 16 50 b7 e3 c4 1f-ae ec 56 48 97 9e 37 87 ...P.....VH..7.  
0060 - 7b 18 8f e2 4f 40 a4 77-2b 0a a1 7a 09 eb c6 58 {...Q@.w+..z...X  
0070 - 14 3b 95 c0 7a 48 4b 86-bf ab 85 7f 15 f6 80 37 .;..zHK.....7  
0080 - 4c 80 7e 39 52 0e ed 0d-52 5e 93 b4 ae d1 4e dd L~9R...R^....N.  
0090 - 65 5c a7 d1 f8 e3 a5 7b-89 81 54 14 1c 53 ca ad e\.....{...T...S..  
00a0 - 1e db 56 be 08 1b 00 39-8c a0 27 a6 e5 23 65 87 ..V.....9...'.#e.  
00b0 - ef 0d fb 1b 07 44 c4 69-4c a5 03 69 10 a2 26 af ....D.i.l..i..&.  
00c0 - 08 63 c5 ca 52 72 e2 33-04 4d 35 1a b2 ea 66 74 .c...Rr.3.M5...ft  
00d0 - 23 e6 9d 92 1b 22 7d e4-a0 c5 c1 36 44 ad 45 1e #...."}.....6D.E.  
00e0 - 0e bd 8e 90 67 fe 3f c3-bd a0 48 13 7f 09 40 9a ...g.?...H...@.  
00f0 - d1 62 64 7c a2 8f 6d 4e-33 54 1a af 77 65 0a ff .bd|..mN3T..we..  
0100 - 4b 3d 8d 12 6a 28 9d e7-82 e0 69 d0 95 56 9d 11 K=...j(....i...V..  
0110 - 8e 5d 3f f4 98 1e 2e f8-d5 94 01 0e bc 88 e9 5e .]?.....^  
0120 - 54 53 42 41 13 b1 9d 9d-6b c2 e1 76 2d ff f7 e6 TSBA....k..v....  
0130 - 06 80 93 2b 3d af da 39-97 13 b2 63 11 a7 15 4a ...+=...9...c...J  
0140 - 8e f2 89 a7 2d 70 a2 40-14 d4 58 75 e2 24 2c 4e ....-p.@..Xu.$,N  
0150 - 7c 1d d6 1b 5c 6a 2e 81-ec c0 b2 eb 62 e8 eb ae [...\]......b...  
0160 - db df af 1b e7 18 a8 9e-bf 00 39 da c8 8a 05 9a .....9.....  
0170 - f5 e6 50 75 3c ab 2c db-d6 fb 7c 20 77 fb bb d7 ..Pu<.,...| w...  
0180 - cb 94 07 b2 50 9a e9 44-5e de 25 30 8a cb 15 92 ....P..D^.%0...  
0190 - a6 62 df 22 e2 eb e3 9a-ba 85 d8 e7 12 2c 7d 1a .b.".....,}.  
01a0 - 77 25 de 80 41 c8 b5 53-fb 7d 93 b3 95 dd 6f a1 w%..A..S.}....o.  
01b0 - a6 c6 45 cc c9 c9 c7 ed-d8 c9 16 52 93 62 c4 53 .E.....R.b.S  
01c0 - 5e 28 ab d2 53 c5 6a 42-03 2a 20 97 98 88 30 f5 ^(..S.jB.* ...0.  
01d0 - 27 14 f4 16 d9 0d cf dd-18 eb 25 83 fe b7 d7 41 '.....%.A  
01e0 - 62 2c 4b b8 4a 40 25 4f-b0 11 da da 3e bf 22 22 b,K.J%0.....>.""  
01f0 - e4 d0 8c 9f 55 2a 54 78-3d 35 b8 58 f4 78 97 5c ....U*Tx=5.X.X.\  
0200 - 2a c2 70 38 6c 12 a8 fd-9b 9a 70 cf f7 ee a4 21 *.p8l.....p....!  
0210 - 38 dc f9 f5 b3 83 5e 90-fb eb d3 52 46 ae 7c 57 8.....^.....RF.[W  
0220 - f4 fb 9d 84 57 60 e6 54-24 48 ee 37 25 b4 5c 98 ....W'.T$H.7%.\.  
0230 - c6 79 26 52 c7 25 0a c8-30 08 c6 a8 43 37 a1 59 .y&R%.0...C7.Y  
0240 - 5d 89 c9 cf 1b 4f e7 3a-61 d1 7c 1f 9a a9 68 01 ]....O.:a.|...h.  
0250 - 66 fd 5d c2 98 bb 0c fe-d8 83 d2 8d 7f b4 b5 1a f.].  
0260 - fe a9 81 c9 2f 2c 92 f6-f9 46 6b 63 2d cd 75 47 ....,....Fkc-UG  
0270 - b4 08 68 83 43 6f ff 17-64 21 34 89 cb 14 f8 cd .h.Co..d!4.....  
0280 - 29 44 d3 41 0c a8 a4 eb-36 2b 3a b3 d2 4a d0 c4 )D.A....6+!..J..  
0290 - 5d ae 97 99 a7 18 24 dc-f7 53 e4 ba 63 d5 ee 42 W.....Q.S..c..B  
02a0 - 6a 6e b4 22 6e 92 51 fd-61 3c 0a 42 ba e9 e2 9a jn."n.Q.a<.B....  
02b0 - aa 1e 30 fe 07 0f 64 1d-fd ec 4c ca 6c fd 80 ed ..0....d...L.l...  
02c0 - 13 09 c7 98 a9 f7 77 40-53 c6 bc a1 be 5d ac 9c .....w@S....].  
02d0 - 4c a1 ad 3f a6 56 72 a0-26 c3 c5 25 0a b3 fe 50 L..?Vr.&..%...P  
02e0 - 6f 4c 7b 5f d3 c8 a7 4e-cf 77 f7 76 75 1e ce 12 oL{...N.w.vu...  
02f0 - ac d1 68 8d 83 8b 94 61-2e 8b eb 40 90 b1 ce 76 ..h....a...@...v  
0300 - a3 cc bf 68 b8 1d e4 50-7a 61 00 35 b8 6d 28 3e ...h...Pza.5.m(>  
0310 - ab d1 b0 58 b7 bd d0 2c-d2 35 1c d0 20 68 75 ca ...X...,5... hu.  
0320 - 18 7e 84 45 c8 02 d2 1f-9b 03 c2 38 f9 d4 a8 fb .~.E.....8....  
0330 - 23 b3 c8 01 1c 7c 2d 04-13 57 64 e2 6b 41 1f 6e #....|...Wd.kA.n  
0340 - 7a 1c d9 b1 b5 87 df 99-79 ca b6 50 7d ef 28 46 z.....y..P}.(F  
0350 - da ac fa 94 ec 34 25 2b-c7 3f 19 fd f7 a3 69 19 ....4%+..?....i.  
0360 - 0d ac e8 24 42 42 bb 51-53 8b e8 9f 4a 22 e9 c6 ...$BB.QS...J"..  
0370 - 79 90 74 d8 b2 29 9f f9-74 1d 46 9d c8 87 b3 4e y.t..).t.F...N  
0380 - 4a 7a 06 ed e5 80 17 0c-8f 8a c4 60 c1 85 39 86 Jz.....^...9.  
0390 - c4 80 b9 94 55 57 ec 5d-65 cc 69 39 2b 7f ff 6d ....UW. ]e.i9+..m  
03a0 - 4d a6 19 c4 52 96 05 24-92 90 ce 02 a0 a3 71 f7 M...R..$......q.  
03b0 - 17 9f 66 d0 ab 15 5d 52-be 1e fb 6a fb 67 a7 d7 ..f... ]R...j.g..  
03c0 - c9 72 ba 41 e6 1f d3 8a-9d f9 11 fc 0b 13 cf 58 .r.A.....X  
03d0 - 9e 6e 01 3c e7 18 9c 3b-c5 a7 74 62 c7 f8 37 5d .n.<...;..tb..7]  
03e0 - 03 58 5a c5 08 ad d7 fa-d4 ec 83 cd 15 39 5c 71 .XZ.....9]q  
03f0 - 96 a8 de ac 8f e6 8f 57-17 67 6f e0 6c 46 e1 49 .....W.go.lf.I
```



3.2. Usando la clave privada correspondiente a la pública generada anteriormente descifra el contenido del fichero cipher.txt y almacena el resultado en el fichero plain.txt. Para poder hacerlo el fichero con el texto cifrado debe estar codificado en binario, no en hexadecimal.

- Descifrado del binario:

Unset

```
$ openssl pkeyutl -decrypt -inkey clave_privada_rsa_8192.pem  
-in cifrado.txt -out descifrado.txt
```

```
on main !9 ?8  
$ openssl pkeyutl -decrypt -inkey clave_privada_rsa_8192.pem -in cifrado.txt -out descifrado.txt  
on main !9 ?8  
$ cat descifrado.txt  
Holmes had been seated for some hours in silence with his long, thin back curved over a chemical vessel in which he  
was brewing a particularly malodorous product. His head was sunk upon his breast, and he looked from my point of v  
iew like a strange, lank bird, with dull gray plumage and a black top-knot. "So, Watson," said he, suddenly, "you d  
o not propose to invest in South African securities?"
```