TP2 - Sécurité et Cryptographie

TP RSA

Charles RIO & Romain AUGER

16/02/2019

Table des matières

1 Génération d'une paire de clefs RSA

1.1 Question 1 : Générez une bi-clé RSA de 2048 bits dans un fichier .pem

Commande :

```
openssl genrsa -out cle.pem 2048
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ openssl genrsa -out cle.pem 2048
Generating RSA private key, 2048 bit long modulus
..................+++++
.....................................................+++++
e is 65537 (0x010001)
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAuGrVus6DVRWlZja/gYq+QH36QAfzR1G57zU9Vavephdf/jZ2
Trs+hw0SD3ojvACdKr4Zp2mhJB5GlDJiFo2QEcZfcRfX/ndBOoxDIp6O1MEOgUNT
V/llHarAYzxlLWBSX9/BGazKlXJew3NKitzfrtsLqp0dZhczrDB38AImK0VAvKqV
p2CcTaEwrlcoAcmAzbawFEblRIV1Pqj5VUag7cBSUcdlWt+5qPcFdsElAI6GZpgY
8/PgVs/JznTennGHI3eqF5fYs2Mz61Du6gi1LVU7QaR0AckR8ykM74huK+enpGdq
+ECmgajeeyKhKxCC1fAtbLBVEOwFdjylBE6qzQIDAQABAoIBAQCWXxaTUdyovhO1
uqKAwF7NO2uYVmM6HhucPy8Z8iCEEb9GC6aAIBGmETROxmro2x9MQOGuLmUkjENE
h6iPdzKoK7abArQuW5MmaEQ9sEgKlrh7EiidLVAT1q00vYRKcaX5YvuTMd+l6DH4
8MMxY1RIwXdL0Pytx/FsT8EcRMRWtqebxzgkepgdxqfInWG2PByws41ThoXOTBpr
TSMhb0gxDvN1buRW6NNFrEYK1NKMSlamY+vlvKI9POl+GUO8W8rWhgAnISw5lgrD
TszF343Gg7SNmyVKEN/hyGkkeW/mvnOVQTyBH3+PVdENeavONZe+LdwB4yKeI0QL
WaGFcAEBAoGBAOz5sWEvE3+2iL/rfTZwQcL9Uwf5XByQ+YyD+fcO7ABkDfa/2ikj
fp+LFNZ/PunduEOZSSzF/62WAvfQot04lj/HjNEyQ0nAnF2CqG7KLIxeGGF3M901
ySgY1+G/bVaKThnmfezaXqvKVdTKZsGQJwiqh36bw3ECkZ1q8sZIA7etAoGBAMc4
+LUFtOH9ZljoTujIy6Efv8oQuTRaDIr1/k0BYvbrmfsMFdTzfa6OStSmMF9KSb+J
PaCME7hzI5MTlc6+b94n73PbT8VYxGvg7GlgHpjcfbDwmmgcidXG7F69dsrKB+Et
IuKaRAyZp4XinqUJLOGUnMPvLWOYSNzE1HoguaOhAoGBALxtorSC6T9A1iW8yxhR
VIkGQ1Jw3eQ9BqDLhCQFsnRxGoVccc0KUzHrNkuEbHMrAMyHgx7d5XqScJO6SvYa
e6YFNxxUmhp31B2queE2Uwvd+gbt8Mhxbxy5/FadjwQj/wwrMW/3BxYUUgFcWy6I
P/FtH0X19wbSIxUHqDkvo/0VAoGAcNCaRihNHgxZAM/Mn5XVehB4kvyVZEf6Alb7
ArBeUmVodPmLA2Q/L7H0Pic+DTgMOyKEe33XTQQmiQr2MnU09CC5QGpY6fAyisR8
G9AKg5WYt7IIPhyrERvsjlnMA1oUzDa7IocpMdlxPCfwnpRrjfKSM4Iludhqqlnr
2JzfgwECgYA4ZGPOo3RMkbXSbCJvFWh8V3bNANzgYJaJaLPo2QVH1EQotvGcO0aU
ut+qF0ImoTQrA/xL6VqKJHdo9IxFYSwKwLvTdXuHoJDRIaj3yO14YoP6rptJYL3q
G6COgeZnVFlBBsTxD5Fztif/In9aQU6rQiUI8ORGazDeJmvK1gFgbQ==
-----END RSA PRIVATE KEY-----
```

2 Visualisation des clés RSA

2.1 Question 2 : Afficher le contenu du fichier .pem avec la commande cat sous Linux, puis avec la commande rsa de openssl. Comparer les différences ?

```
openssl rsa -in cle.epm -text -noout
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ cat cle.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA5Gmasm2LKco/CEaZkpMfLH9jo4EZIIJyrUtLrIg53Izqc6jA
fkjaPtDej0xzHukpYRs6uzlZ5cl9kmBwfgDqhEn/Zgxq/gCY7s1SHEwRHWyhW+EP
6goqOfzcCiB9GjZCdanfWQu8aqRdSjvFIHDo3y0GNcSZFS6OBCz0M3UBzwYHxnWg
mxcPvinU65dg2HzRtZ4VNH22nnEqVsD3s9IA5keGs6Rqi7EXEdItRL2pldfJjdkd
7RFQxjKLvcSHw815DU5gOEwsqXxQ6SpVI3VbZxcpbC+UGgx9HfFue57lsCIIha4h
nVPi5FL+Edv7UBa50/pypr/NH65IQapxHvazswIDAQABAoIBACPDGRJ4rkJDxSyx
iRf26vmXlG0kKF/7rKLPWDDSP2T1tzuWn1TmaS1OnJoJGTksvmrSzZZEu3uL2ZpS
eSpxUEaYI2HB7fqI82joQsPlcQSPXpA5I7m8D7J2kakQPyYcerlbeHnDqaN0ypp1
0z5qDzvqG7/NYT58xIWI2E86MadM+a/eni0pPC836mJZaWoR9+78uxIGW8a2Gd3r
5BfufGBgeILD0E1ufoGcamaItNF8FuOGxW0uUPm38mbXECwSZg1mDcyPAH4jLDYD
6Uxh4KZsR3B/J/gcrm9W9TVA3IeMO6PqG6iRAEV+G0iXyj7LWn0vJiGOys8f+5Na
JHalHTkCgYEA8n7JwEa3LQGx8rRGZzhOshzxA1fBsABwsBEWDb+lNcxO99Xh18OK
C2DE/BQx76CIYP9Haj0BlV7mIsplTwKWkiUkpRpEpxB0aXxFQDU4GMQJxD82+NiU
YuyEROxzROCytesMbRkekA/KWPBVdEDLdYiNEpHSKIxPgVSnpE6IoIUCgYEA8SIK
eyrmOf70Vp7oseLCUcUEvRE3U/TznVMfABzghF/7LjVlr+p8uLWLVUq2529pft7p
spdX9HxOrWQBHUhffZpYTjNKbvDVjG6pxUL8cUJAqyNGr0hwR5l0CNiX1jDKh+p/
yQ61MLzfcpeU4I/D/LP4znZ0iDX97uKwbHEvlNcCgYBid8GM5ioziGCt4S5Fc8Pg
54emh9gKk+MuW4HNC2kWs2PNl3ghmTFQ9XaHtduhJlq6qG5jYWpnMSXaMr14m+Bw
b8y1jjkabcAXpXKpY/Lne5NLsS+tVKTMlqYPJsSXz3ZCELP3CSAz93V/L/hDQJxd
mZlPVQ81j+Qo7Cs2uP0Z0QKBgCgYAegi5O8FvnjcqVJSov7XpIcPYsS5+PvSw1fQ
dWBtWSWAyWyrr5tCzG0dJDZtJvxqci84zO4g8TARbcIBs6b9z+sIyjqSHt/f0qiz
D6iBXKFYFzuz7r9o+4sxAGYj7LkWu7KhmG0HKpwyKhYAsZTGE/u4ZH31hEiBNtaB
J2k3AoGBAKqZJhydADRcx7ZhWiojEAJGaFovALYswU9gUn2U4mS3HqR9i22KZoXj
K9yYJExizPf+g79ecBFDW/uKVXj9qzoRpGMtRI0ZM2g9960wx4MTOztxoKMEbGzH
8UdYjqM94GaK+cM/5yid4xNk3QE2ruAVklK/8QFC98KoV7EzMLV7
-----END RSA PRIVATE KEY-----
```

```
Private-Key: (2048 bit)
modulus:
    00:e4:69:9a:b2:6d:8b:29:ca:3f:08:46:99:92:93:
    1f:2c:7f:63:a3:81:19:20:82:72:ad:4b:4b:ac:88:
    39:dc:8c:ea:73:a8:c0:7e:48:da:3e:d0:de:8f:4c:
    73:1e:e9:29:61:1b:3a:bb:39:59:e5:c9:7d:92:60:
    70:7e:00:ea:84:49:ff:66:0c:6a:fe:00:98:ee:cd:
    52:1c:4c:11:1d:6c:a1:5b:e1:0f:ea:0a:2a:39:fc:
    dc:0a:20:7d:1a:36:42:75:a9:df:59:0b:bc:6a:a4:
    5d:4a:3b:c5:20:70:e8:df:2d:06:35:c4:99:15:2e:
    8e:04:2c:f4:33:75:01:cf:06:07:c6:75:a0:9b:17:
    0f:be:29:d4:eb:97:60:d8:7c:d1:b5:9e:15:34:7d:
    b6:9e:71:2a:56:c0:f7:b3:d2:00:e6:47:86:b3:a4:
    6a:8b:b1:17:11:d2:2d:44:bd:a9:95:d7:c9:8d:d9:
    1d:ed:11:50:c6:32:8b:bd:c4:87:c3:cd:79:0d:4e:
    60:38:4c:2c:a9:7c:50:e9:2a:55:23:75:5b:67:17:
    29:6c:2f:94:1a:0c:7d:1d:f1:6e:7b:9e:e5:b0:22:
    08:85:ae:21:9d:53:e2:e4:52:fe:11:db:fb:50:16:
    b9:d3:fa:72:a6:bf:cd:1f:ae:48:41:aa:71:1e:f6:
    b3:b3
publicExponent: 65537 (0x10001)
privateExponent:
    23:c3:19:12:78:ae:42:43:c5:2c:b1:89:17:f6:ea:
    f9:97:94:6d:24:28:5f:fb:ac:a2:cf:58:30:d2:3f:
    64:f5:b7:3b:96:9f:54:e6:69:2d:4e:9c:9a:09:19:
    39:2c:be:6a:d2:cd:96:44:bb:7b:8b:d9:9a:52:79:
    2a:71:50:46:98:23:61:c1:ed:fa:88:f3:68:e8:42:
    c3:e5:71:04:8f:5e:90:39:23:b9:bc:0f:b2:76:91:
    a9:10:3f:26:1c:7a:b9:5b:78:79:c3:a9:a3:74:ca:
    9a:75:d3:3e:6a:0f:3b:ea:1b:bf:cd:61:3e:7c:c4:
    85:88:d8:4f:3a:31:a7:4c:f9:af:de:9e:2d:29:3c:
    2f:37:ea:62:59:69:6a:11:f7:ee:fc:bb:12:06:5b:
    c6:b6:19:dd:eb:e4:17:ee:7c:60:60:78:82:c3:d0:
    4d:6e:7e:81:9c:6a:66:88:b4:d1:7c:16:e3:86:c5:
    6d:2e:50:f9:b7:f2:66:d7:10:2c:12:66:0d:66:0d:
    cc:8f:00:7e:23:2c:36:03:e9:4c:61:e0:a6:6c:47:
    70:7f:27:f8:1c:ae:6f:56:f5:35:40:dc:87:8c:3b:
    a3:ea:1b:a8:91:00:45:7e:1b:48:97:ca:3e:cb:5a:
    7d:2f:26:21:8e:ca:cf:1f:fb:93:5a:24:76:a5:1d:
    39
prime1:
    00:f2:7e:c9:c0:46:b7:2d:01:b1:f2:b4:46:67:38:
    4e:b2:1c:f1:03:57:c1:b0:00:70:b0:11:16:0d:bf:
    a5:35:cc:4e:f7:d5:e1:d7:c3:8a:0b:60:c4:fc:14:
    31:ef:a0:88:60:ff:47:6a:3d:01:95:5e:e6:22:ca:
    65:4f:02:96:92:25:24:a5:1a:44:a7:10:74:69:7c:
    45:40:35:38:18:c4:09:c4:3f:36:f8:d8:94:62:ec:
    84:44:ec:73:44:e0:b2:b5:eb:0c:6d:19:1e:90:0f:
    ca:58:f0:55:74:40:cb:75:88:8d:12:91:d2:28:8c:
    4f:81:54:a7:a4:4e:88:a0:85
prime2:
    00:f1:22:0a:7b:2a:e6:39:fe:f4:56:9e:e8:b1:e2:
    c2:51:c5:04:bd:11:37:53:f4:f3:9d:53:1f:00:1c:
    e0:84:5f:fb:2e:35:65:af:ea:7c:b8:b5:8b:55:4a:
    b6:e7:6f:69:7e:de:e9:b2:97:57:f4:7c:4e:ad:64:
    01:1d:48:5f:7d:9a:58:4e:33:4a:6e:f0:d5:8c:6e:
    a9:c5:42:fc:71:42:40:ab:23:46:af:48:70:47:99:
    74:08:d8:97:d6:30:ca:87:ea:7f:c9:0e:b5:30:bc:
    df:72:97:94:e0:8f:c3:fc:b3:f8:ce:76:74:88:35:
    fd:ee:e2:b0:6c:71:2f:94:d7
exponent1:
    62:77:c1:8c:e6:2a:33:88:60:ad:e1:2e:45:73:c3:
    e0:e7:87:a6:87:d8:0a:93:e3:2e:5b:81:cd:0b:69:
    16:b3:63:cd:97:78:21:99:31:50:f5:76:87:b5:db:
    a1:26:5a:ba:a8:6e:63:61:6a:67:31:25:da:32:bd:
    78:9b:e0:70:6f:cc:b5:8e:39:1a:6d:c0:17:a5:72:
    a9:63:f2:e7:7b:93:4b:b1:2f:ad:54:a4:cc:96:a6:
    0f:26:c4:97:cf:76:42:10:b3:f7:09:20:33:f7:75:
    7f:2f:f8:43:40:9c:5d:99:99:4f:55:0f:35:8f:e4:
    28:ec:2b:36:b8:fd:19:d1
exponent2:
    28:18:01:e8:22:e4:ef:05:be:78:dc:a9:52:52:a2:
    fe:d7:a4:87:0f:62:c4:b9:f8:fb:d2:c3:57:d0:75:
    60:6d:59:25:80:c9:6c:ab:af:9b:42:cc:6d:1d:24:
    36:6d:26:fc:6a:72:2f:38:cc:ee:20:f1:30:11:6d:
    c2:01:b3:a6:fd:cf:eb:08:ca:3a:92:1e:df:df:d2:
    a8:b3:0f:a8:81:5c:a1:58:17:3b:b3:ee:bf:68:fb:
    8b:31:00:66:23:ec:b9:16:bb:b2:a1:98:6d:07:2a:
    9c:32:2a:16:00:b1:94:c6:13:fb:b8:64:7d:f5:84:
    48:81:36:d6:81:27:69:37
coefficient:
    00:aa:99:26:1c:9d:00:34:5c:c7:b6:61:5a:2a:23:
    10:02:46:68:5a:2f:00:b6:2c:c1:4f:60:52:7d:94:
    e2:64:b7:1e:a4:7d:8b:6d:8a:66:85:e3:2b:dc:98:
    24:4c:62:cc:f7:fe:83:bf:5e:70:11:43:5b:fb:8a:
    55:78:fd:ab:3a:11:a4:63:2d:44:8d:19:33:68:3d:
    f7:ad:30:c7:83:13:3b:3b:71:a0:a3:04:6c:6c:c7:
    f1:47:58:8e:a3:3d:e0:66:8a:f9:c3:3f:e7:28:9d:
    e3:13:64:dd:01:36:ae:e0:15:92:52:bf:f1:01:42:
    f7:c2:a8:57:b1:33:30:b5:7b
```

Avec la commande cat, le fichier est affiché tel quel. Par contre, avec rsa, la clé est affichés en hexadécimal. On peut distinguer les différents élements.

2.2 Question 3 : Que vaut votre exposant de chiffrement ? comparez avec ceux de vos voisins.

La valeur de l'exposant est : 65537. Cette valeur est identique pour tout le monde, c'est l'exposant public par défaut. Il permet une valeur assez élevée pour être assez sécurisé et permet une meilleure compatibilité.

2.3 Question 4 : Utilisez l'option -pubout pour exporter clé publique dans un fichier .pub.pem.

Commande :

```
1 openssl rsa -in cle.pem -pubout -out clepub.pub.pem
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ openssl rsa -in cle.pem -pubout -out clepub.pub.pem
writing RSA key
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ cat clepub.pub.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5Gmasm2LKco/CEaZkpMf
LH9jo4EZIIJyrUtLrIg53Izqc6jAfkjaPtDej0xzHukpYRs6uzlZ5cl9kmBwfgDq
hEn/Zgxq/gCY7s1SHEwRHWyhW+EP6goqOfzcCiB9GjZCdanfWQu8aqRdSjvFIHDo
3y0GNcSZFS6OBCz0M3UBzwYHxnWgmxcPvinU65dg2HzRtZ4VNH22nnEqVsD3s9IA
5keGs6Rqi7EXEdItRL2pldfJjdkd7RFQxjKLvcSHw815DU5gOEwsqXxQ6SpVI3Vb
ZxcpbC+UGgx9HfFue57lsCIIha4hnVPi5FL+Edv7UBa50/pypr/NH65IQapxHvaz
swIDAQAB
-----END PUBLIC KEY-----
```

3 Chiffrement d'un fichier de clés RSA

3.1 Question 5 : Chiffré votre clé RSA avec un algorithme symétrique ; Afficher le contenu du fichier .pem puis avec la commande rsa. Essayer différents algorithmes symétriques

3.1.1 DES3

Commande :

```
1 openssl rsa -in cle.pem -des3 -out cle.pem
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ openssl rsa -in cle.pem -des3 -out cle.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ cat cle.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D271BCA725C9FC1A

OBAi+QziDuzTZw9EsPTXCv4ZSAp1NJNAKfcHjiddtV4LcCmdDZSJxnBQK+BoRbch
eT4aB4fcE093XEFnVFYPvq3MgN5cr+kiH0BTcGhCQjcEUV/Gitjs4EUuQlAavI4D
oQRDcpbiGXuGVMn4p/0r7gAgjNAPia38xPLHRQkiL+3KDA8qgRFtS+rCWCA2vu3P
X9ze0RimLOc/pKojB4tqszeHLETiAu0JvYT3eeLrXfkM42fugf1gQ6UKlKzUEeVW
tSgMsj1RX6GCKAWsraSCZ/5gOHEkUe2YEyxnPkThR3RdH6y83LdjGizg8TeW9Mdn
x9bvJasLc9El82p4scSiJHPYj5A5wcOCf/I41H81+aQHNDDQBG5WK/NIV9cs3AVa
2ECTpzz9wJgIfI/k889CZ8cy560RS6H541dN2qaRoE7f5hJYpOXTxxHrUAEpfyUf
WVPCyM4YAZPVd6Q3/e+Z9Adr4r2YYzAzz6feXIMBfx11Lbib2JK1IQUa6SFnER/X
MpeF4QQ0G5vY74YdYGS8TpwKCt6s4/V1GreVHKTbVTg25E+OeNRPPtw8VBNHTQqI
W7YVKAlreal0270e8QyENQIvhWhzPeIOqTTDAl8a4ll+TwM7AmjSU6C5Q2+xy1Xr
yn49JZaVIJZ4+IkwI3ghWRIbQeYE3xD7T4NbOJ0CiPhGRm+r8QaHa43wl/snETq6
bJpwkgaRBhFBmmluFh9weTs9zUUxMVB0lu78ubmH+V/MSRLR90mdGLkGGmsdofFJ
uuVU/D6NwPfKYb3g7q4lgCsJIFsB52V+qxdKf5SVc3hkKGE1fgKvuRqOCfysirpA
SGvatujMaM2ObYxevP3ixWyyYlQubR2pV/Yc1cC8uxvyYPiO64c9pi8ipAgXZVGi
CBVh2E5lp5DfcQGxPaIHo5qD1ZwQq7EoZB9U8DUZ2/zO6AIZCpgPbP391BhnDSv2
BS0kYuOAa6Yd3aAj1kO1bg+GJfTWViJGOb/tdb7Lq9UvSgmHEndaVNtRsT42CKNK
7zr6Ff6AW9wMgM639ARcEkVKYWZq+vEafwuqoNXoeU1qRxD0+ntTPch8A1rWTN8E
wFcXoB4K+Plqnmh8KJ5wE3H+pxED0P1+Tr14Nl/WwDgUfNt8TqMaDc8BB9DbP+XO
Jpgjbez62LFEooVbFIZ2E14M58ElN2Vj/Lo1p4KI+ilty6QzYjFmCGuGx7NYrESN
R8kGDJPITWEgpcffZJb7Vj6plZK2XVghcHFzjCLo07d2Ks2PZLssUkjhX5m4AWCp
ZjT1L69y0/nqGQhHv9sKFQYYy7BqR9ISPy7z1bNOlUbXmOItbYF/BssnZ9X9LH4g
8xfoF0Zl6OTzopmKgEhAgYAlA/0VTJz53th72DItFInIeQ+jeYnjg+ro1A4Y2XIk
Sh6cEIgPdNsf/oOdZvrPf/y2oOPBr47j6jlQ/PsZZwIIM93/s6E5cOqjDCspaMra
fhkY29yxaeHJSLzPm7MOvlieJbDHYSRW2dtPINOEGyYuziOTE9bFuZJ54yRr3j9B
PYphsjsoQ3OUFJcDIkIZZdN7JXVjyxaKhOPKvn+Q2MlXFYLnjZcjzQ==
-----END RSA PRIVATE KEY-----
```

```
Enter pass phrase for enc.pem:
Private-Key: (2048 bit)
modulus:
    00:b8:6a:d5:ba:ce:83:55:15:a5:66:36:bf:81:8a:
    be:40:7d:fa:40:07:f3:47:51:b9:ef:35:3d:55:ab:
    de:a6:17:5f:fe:36:76:4e:bb:3e:87:0d:12:0f:7a:
    23:bc:00:9d:2a:be:19:a7:69:a1:24:1e:46:94:32:
    62:16:8d:90:11:c6:5f:71:17:d7:fe:77:41:3a:8c:
    43:22:9e:8e:d4:c1:0e:81:43:53:57:f9:65:1d:aa:
    c0:63:3c:65:2d:60:52:5f:df:c1:19:ac:ca:95:72:
    5e:c3:73:4a:8a:dc:df:ae:db:0b:aa:9d:1d:66:17:
    33:ac:30:77:f0:02:26:2b:45:40:bc:aa:95:a7:60:
    9c:4d:a1:30:ae:57:28:01:c9:80:cd:b6:b0:14:46:
    e5:44:85:75:3e:a8:f9:55:46:a0:ed:c0:52:51:c7:
    65:5a:df:b9:a8:f7:05:76:c1:25:00:8e:86:66:98:
    18:f3:f3:e0:56:cf:c9:ce:74:de:9e:71:87:23:77:
    aa:17:97:d8:b3:63:33:eb:50:ee:ea:08:b5:2d:55:
    3b:41:a4:74:01:c9:11:f3:29:0c:ef:88:6e:2b:e7:
    a7:a4:67:6a:f8:40:a6:81:a8:de:7b:22:a1:2b:10:
    82:d5:f0:2d:6c:b0:55:10:ec:05:76:3c:a5:04:4e:
    aa:cd
publicExponent: 65537 (0x10001)
privateExponent:
    00:96:5f:16:93:51:dc:a8:be:13:b5:ba:a2:80:c0:
```

3.1.2 AES256

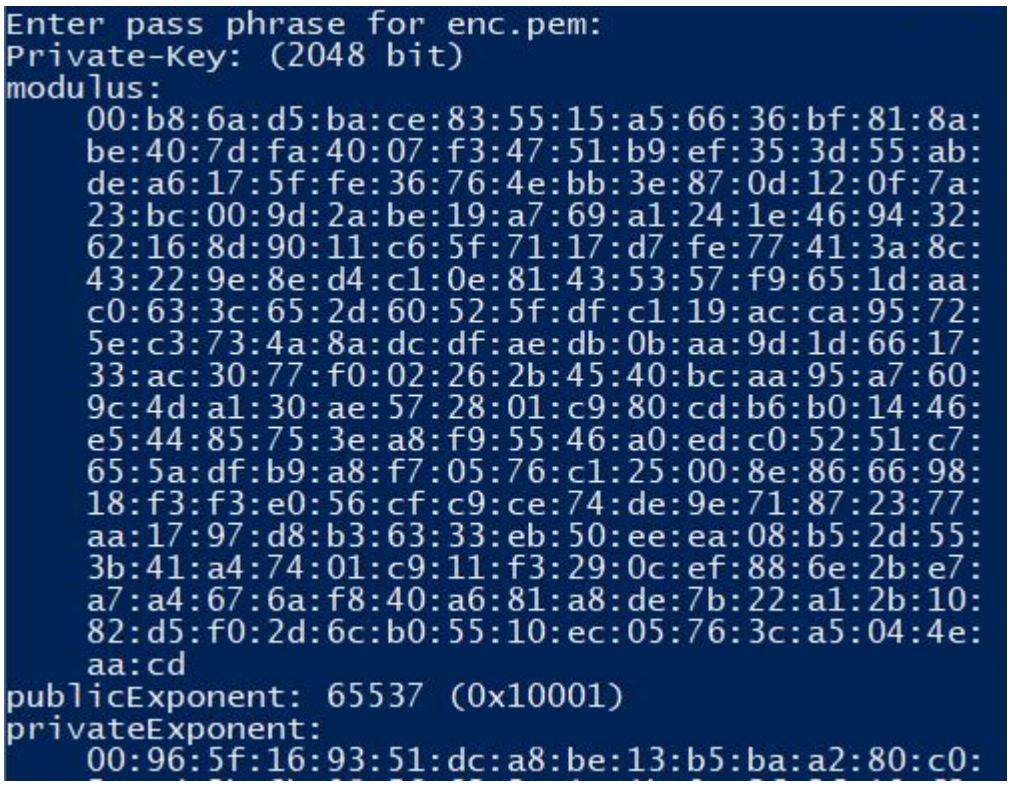
Commande :

```
1  openssl rsa -in cle.pem -aes256 -out cle_enc.pem
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ openssl rsa -in cle.pem -aes256 -out cle_enc.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
11404438@f206-15:~/Info/ING3/cryptographie/TP2(RSA)$ cat cle_enc.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,92081BDF7E47055435C20A4154863875

V4d217ODw1h1UzqBmyrOcGZqiybs7LQIHcFvIoMKGBfM+0h/UKI8I6KwDfZlWbIn
xeyqx13hGbhHFkc0iGABwWLojIBcK1sA4EMDyzzGSpJp/n1U2Dy01sijvbyiwyIR
CTcb3cXx7r3tzlcwGhK4LQJ+IvdNh1PsjbTqvchpwJkxOTl3c96ZyOw2EqxuK/hY
15QbhU2SxcP54aOZRBW+NNvVgPgttxk7ANsQYxf72FvUvUiegMUqSHNWwr2gdXOR
zyAATupcYgChH8wL9Pzl9yfM0oqtivYmFJ6k5I5TpzWw8w+ZVXyYwsRDZNGFw/k1
qkzENpI9n/w8yNOJTV/Qz3hHXwBEi4CynwawViO9tOEHU4GzbllloDKvMldcQxPmf
e9xD2lyQ8kiV4iqy2PJ8/kEwRoK5w24NlQe+YOxsGa6J6uNG0yuUasbHevMSfc3M
LyKaa0vnUQcXeBxGQKyUo2jlCtbxSGwovrY5VceDK1iDvPv7VN9etsg13GtDYnDR
/OpPK0CFAkd2rIMREsj+j7CHkVjCZSBQEUZsGdkRhxOwa+oPIOI0tflP9iGmqvqb
aSB0rwvaPpJvKJ0GDvOEQDcXCSIpnLxXlqnP3Zvw3jQD57bixYP0DwIob8R9bHjY
oEwjxSilPIJP3J7f7Qcng2Xo5jyHrx+/3JRBWfxIWHdqKAYGjVyj4Bftvd+Hnsrn
AKgfqMnTBJwLJj578zubflVFH5zYKVv4jdxA/gT+977SFGyEx/WPaE9tfFB0fmMB
TjYkyBa+A59FXj/01PhEirkF3I7NBObnDw1TSgKTsbmOtg49klW/JumjoReliLYD
3N+/mKlQSPoJGN2tuaYtyZ5vlcb+VDc8Q3jEEfkWcLpcn1YgUpXllBEfq46FyaSn
XE0TTjP3IL4rKTYkit8cGJP6kgib5VQmXphHGo6mQ/owwArKOLfmpvvA/Z5bq6mP
I+JHVXjslHVO3C0Z6hpUjT37cZ4ftTofdKb7PHk2ctYs447zOE1jqIBbuAseEoyg
5tzkjBdFCLlJb8PtbwG1sLn7rIFXQ1YVOnZjVA4YemaIMuqGR9bTqrjkdMMwdorl
jzPkf1Wep52Tjq03Rmf7q74ILqx3YWv9ZdRa5iGX2UcKpOALhzx+L4V4ufAU6Era
1IDUGDiEkU+YbA3ISXKl7yvaaL055kiIdABAiqnrk8l0iyGKfwDl5CxgPp0m50dn
5pGDsYd7wYmM4Qn/FEOx4qq9mz+Ak56MewlhCBdae7Wo4ANy3GXaJ5ae0vpL8RCd
a0tmqDyMdFDfYNNWzguvbowCDlstq1gkNam0Ixdd/5iV31aKFrk+fGSQEWHAAMbw
8Cet6GEOpQ33J67fspA8V4mmvzNGQJ/+YwlMLLu1asB8RH3QoM/sVh9wC2e1kgCF
RiWP5+K8g9K8Nh+Mzvh1VX65Dlf5Tukwkwv1ou/EdqtIvq60w2ngzef70F6nERBd
LDlsB8ejDMVvS/9hh07tAMG9PrVqqKo3th3VmXz85kLoersok27MnoB+tKs2UhKF
9Og2tfPh36PIdGxC3u6YGBIdc1gvezRN7hl8DGgnrxReV2/JOfAlos5ibEOYJUCp
-----END RSA PRIVATE KEY-----
```



4 Chiffrement, déchiffrement avec RSA

4.1 Question 6 : Echanger entre vous vos clés publiques et chiffrez de petit message. Envoyez-lez à vos collègues.

Fichier à chiffrer :

```
1 Texte à communiquer chiffré.
```

On utilise la commande suivante pour chiffer :

```
1 openssl rsautl -encrypt -in test.txt -inkey cle.pem -out test_enc.txt
```

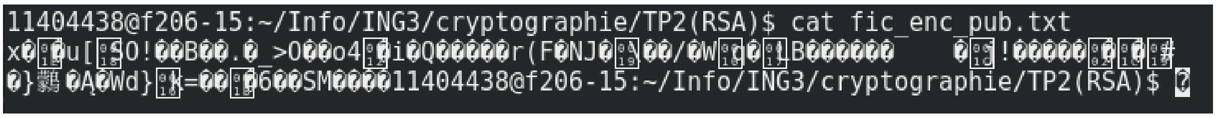
Résultat :

On utilise la commande suivante pour déchiffer :

```
1 openssl rsautl -decrypt -in test_enc.txt -inkey cle.pem -out test_dec.
    txt
```

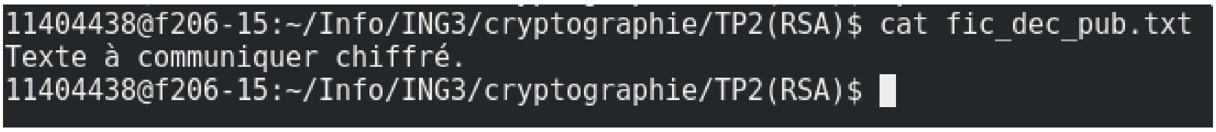
Chiffrement avec clé publique :

```
openssl rsautl -encrypt -in test.txt -inkey clepub.pub.pem -out
    fic_enc_pub.txt -pubin
```



Déchiffrement :

```
openssl rsautl -decrypt -in fic_enc_pub.txt -inkey cle.pem -out
    fic_dec_pub.txt
```

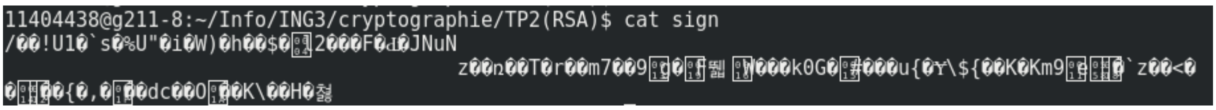


5 Signature avec RSA

5.1 Question 7 : Signez un petit fichier et échanger le avec vos collègues

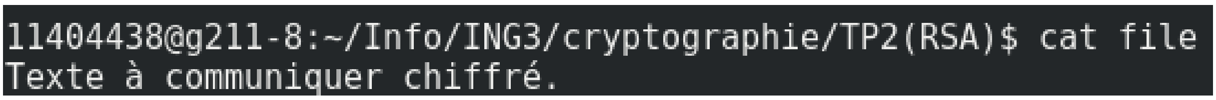
Commande pour signer le fichier test.txt :

```
openssl rsautl -sign -in test.txt -inkey cle.pem -out sign
```



On vérifie avec la commande suivante :

```
openssl rsautl -verify -in sign -pubin -inkey clepub.pub.pem -out file
```



6 Empreinte d'un document

6.1 Question 8 : Signez un gros fichier en utilisant son empreinte

Calcul de l'empreinte d'un document avec la fonction md5 :

```
1 openssl dgst -md5 -out empreinte test.txt
```

```
11404438@g211-8:~/Info/ING3/cryptographie/TP2(RSA)$ cat empreinte
MD5(test.txt)= f9c79c37f0481fdb40cda0c4ec777147
```

Calcul de l'empreinte d'un document avec la fonction sha256 :

```
1 openssl dgst -sha256 -out empreinte test.txt
```

```
11404438@g211-8:~/Info/ING3/cryptographie/TP2(RSA)$ cat empreinte
SHA256(test.txt)= e8786cee000e3ae71e1153ebee33dc0b9043ef6b4547655c9ae88e7c99874da4
```

On signe l'empreinte calculée :

```
1 openssl rsautl -sign -in empreinte -inkey cle.pem -out fic_sign
```

On vérifie avec la commande suivante :

```
1 openssl rsautl -verify -in fic_sign -pubin -inkey clepub.pub.pem -out
      fic_unsign
```

```
11404438@g211-8:~/Info/ING3/cryptographie/TP2(RSA)$ cat fic_unsign
SHA256(test.txt)= e8786cee000e3ae71e1153ebee33dc0b9043ef6b4547655c9ae88e7c99874da4
```