Compte Rendu TP1

ELHIMDI Yasmine

PARMENTIER Laurent

Exercice 0 : Introduction

```
laubosslink@po-lbl:~$ hexdump hextest.txt
0000000 3141 3261 000a
0000005
```

Remarque: le code ASCII de A est 65, celui de 1 est 49 celui de a est 97 et le saut de ligne est 10

On a les lettres qui sont regroupés par paire, et inversé. Dans la sortie, 0x31 ⇔ dec(49) ⇔ 1, et 0x41 ⇔ dec(65) ⇔ A.

Si on le lit tel quel, on a donc:

```
1A2a
```

Exercice 1 : chiffreme symétrique

1. Algorithmes

```
        base64              Base 64

        bf-cbc              Blowfish in CBC mode
        bf                  Alias for bf-cbc
        bf-cfb              Blowfish in CFB mode
        bf-ecb              Blowfish in ECB mode
        bf-ofb              Blowfish in OFB mode

        cast-cbc            CAST in CBC mode
        cast                Alias for cast-cbc
        cast5-cbc           CAST5 in CBC mode
        cast5-cfb           CAST5 in CFB mode
        cast5-ecb           CAST5 in ECB mode
        cast5-ofb           CAST5 in OFB mode
```

```
        des-cbc             DES in CBC mode
        des                 Alias for des-cbc
        des-cfb             DES in CBC mode
        des-ofb             DES in OFB mode
        des-ecb             DES in ECB mode

        des-ede-cbc         Two key triple DES EDE in CBC mode
        des-ede             Two key triple DES EDE in ECB mode
        des-ede-cfb         Two key triple DES EDE in CFB mode
        des-ede-ofb         Two key triple DES EDE in OFB mode

        des-ede3-cbc        Three key triple DES EDE in CBC mode
        des-ede3            Three key triple DES EDE in ECB mode
        des3                Alias for des-ede3-cbc
        des-ede3-cfb        Three key triple DES EDE CFB mode
        des-ede3-ofb        Three key triple DES EDE in OFB mode

        desx                DESX algorithm.

        gost89              GOST 28147-89 in CFB mode (provided by ccgost
engine)
        gost89-cnt          `GOST 28147-89 in CNT mode (provided by ccgost
engine)

        idea-cbc            IDEA algorithm in CBC mode
        idea                same as idea-cbc
        idea-cfb            IDEA in CFB mode
        idea-ecb            IDEA in ECB mode
        idea-ofb            IDEA in OFB mode
        rc2-cbc             128 bit RC2 in CBC mode
        rc2                 Alias for rc2-cbc
        rc2-cfb             128 bit RC2 in CFB mode
        rc2-ecb             128 bit RC2 in ECB mode
        rc2-ofb             128 bit RC2 in OFB mode
        rc2-64-cbc          64 bit RC2 in CBC mode
        rc2-40-cbc          40 bit RC2 in CBC mode

        rc4                 128 bit RC4
        rc4-64              64 bit RC4
        rc4-40              40 bit RC4

        rc5-cbc             RC5 cipher in CBC mode
        rc5                 Alias for rc5-cbc
        rc5-cfb             RC5 cipher in CFB mode
        rc5-ecb             RC5 cipher in ECB mode
        rc5-ofb             RC5 cipher in OFB mode

        aes-[128|192|256]-cbc  128/192/256 bit AES in CBC mode
        aes-[128|192|256]      Alias for aes-[128|192|256]-cbc
        aes-[128|192|256]-cfb  128/192/256 bit AES in 128 bit CFB mode
        aes-[128|192|256]-cfb1 128/192/256 bit AES in 1 bit CFB mode
```

```
        aes-[128|192|256]-cfb8 128/192/256 bit AES in 8 bit CFB mode
        aes-[128|192|256]-ecb  128/192/256 bit AES in ECB mode
        aes-[128|192|256]-ofb  128/192/256 bit AES in OFB mode
```

On retrouve les modes opératoires suivant:

- ecb
- cfb
- ofb
- cbc
- cnt

En RC4 il n'y a pas de mode opératoire car le chiffrement symétrique peut prendre une chaine de taille quelconque. TODO compléter

2. Chiffrement/déchiffrement AES

```
laubosslink@po-lbl:~$ echo "helloworld" >source.txt
laubosslink@po-lbl:~$ openssl enc -a -e -aes-128-cbc -in source.txt -out
sortie.enc
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
laubosslink@po-lbl:~$ cat source.txt
helloworld
laubosslink@po-lbl:~$ cat sortie.enc
U2FsdGVkX19Zo3eXCILPGJ74Iq/5c9BmcZdl5IYBkQQ=
laubosslink@po-lbl:~$ openssl enc -a -d -aes-128-cbc -in sortie.enc -out
source2.txt -p
enter aes-128-cbc decryption password:
salt=59A377970882CF18
key=70EE8746D739C3A871EF2572D419F14A
iv =EB2C804AE4D600619D9181F87AFC3FE8
laubosslink@po-lbl:~$ cat source2.txt
helloworld
```

Note: mot de passe utilisé : '1234'. On peut le spécifier via l'option -k.

3. Partie du fichier qui correspond au fichier chiffre

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ hexdump
sortie.enc
0000000 6153 746c 6465 5f5f 28d3 7101 4aa0 7743 # salted__ suivis du chiffré
0000010 20f6 ec83 3e85 9685 c9d1 726e 32a1 2409 # les 8 derniers octets
représente le bourrage
```

Note: Le texte chiffré fait 192bits. Soit 24 octets.

Sans bourrage:

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ hexdump
source2-sansbourage.txt
0000000 6568 6c6c 776f 726f 646c 050a 0505 0505
0000010
```

Note: Sans bourrage on retrouve bien un chiffré de 128bits. Soit 16 octets. Il y avait donc 64 bits de bourrage. Ce bourrage est ajouté à la fin.

4. CLI avec la cle de chiffrement

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
enc -e -aes-128-cbc -in source.txt -out sortie.enc -K 1234 -iv 1234
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
enc -d -aes-128-cbc -in sortie.enc -out source2.txt -p -K 1234 -iv 1234
salt=0100000000000000
key=12340000000000000000000000000000
iv =12340000000000000000000000000000
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ cat
source2.txt
helloworld
```

Avec le même IV mais un bit modifié:

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
enc -d -aes-128-cbc -in sortie.enc -out source2.txt -p -K 1234 -iv 0234
salt=0100000000000000
key=12340000000000000000000000000000
iv =02340000000000000000000000000000
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ cat
source2.txt
xelloworld
```

Note: Comme on a modifié le premier bit de l'IV, selon le mode utilisé [1)], dans ce cas le mode CBC, on retrouve le 1er caractère modifié.

Exercice 2 : Fonction de hachage et MAC

---

1. Fonctions de hachage disponibles

```
-md5|-md4|-md2|-sha1|-sha|-mdc2|-ripemd160|-dss1
```

2. Hachage avec SHA-1

Le hachage du fichier source.txt nous donne le haché suivant :

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
dgst -sha1 source.txt
SHA1(source.txt)= e7509a8c032f3bc2a8df1df476f8ef03436185fa
```

Après modification du premier caractère du fichier source.txt, on obtient un haché complétement différent :

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl dgst -sha1 source.txt >
empreinte2.txt
SHA1(source.txt)= 3847ad417c997b33384f1db214abb636141176ad
```

3. Hachage avec SHA-1 et MD5

Hachage du sujet de tp en **SHA-1** :

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl dgst -sha1
tp_crypto_apl_2A.pdf > tp_empreinte_sha1.txt
SHA1(tp_crypto_apl_2A.pdf)= 1c3ef8969fcf235fc75266f78df7006919803616
```

Taille de l'empreinte SHA1 : 160 bits

Hachage du sujet de tp en **MD5** :

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl dgst -md5
tp_crypto_apl_2A.pdf > tp_empreinte_md5.txt
MD5(tp_crypto_apl_2A.pdf)= 4758e7521496e8d786a33b4908f98824
```

Taille de l'empreinte MD5 : 128 bits

4. Calcul du MAC

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl dgst -sha1 -hmac 1234
source.txt > mac_source.txt
MAC-SHA1(source.txt)= 2cea329bc89cf6e45e847b6c51db25057840cbb0
```

Taille de l'empreinte : 160 bits

Exercice 3 : Crypto Systeme RSA

1.Generation de clé

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
genrsa -out ma_cle_rsa.pem 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....................+++
.....................................................................
.....................+++
e is 65537 (0x10001)
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ cat
ma_cle_rsa.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAqDWo53rs663C3yIqGj9n7TGycKctZup1RiHLzjjLH1jhNBj6
9F0fcE2K53Q94xZAB33N+QngM/PnPW6x+ejbCUCopl0F02B2KvGEheCgjQmOfTgD
P5eiSMOaPihmE7oMYTYqNXtTpn93H9Sks1AoDGiaLxuz+ska/ynKvNSoioksMa41
wJxKpA1v/bDO4fHea6GVC2V3+HWuBXt8iazoT7O4m8OjmYd/soQx3CLVMdjFL3iH
AocgDKXaP1l0t/Ap1a8If/BzE+M29gDYiS04Z40UmA44l6IaY/0vy8JB6vOqS38u
dywBhiBK1FqmOq/h6mM5kmN821GpGj21vw5dyQIDAQABAoIBAA9bLrtLNpvhdhvm
w4834KX/1nmAWZ2+o8wuQ6vk9W48L/sQmMB8S+V1vsuYihnUKy5D5uzoYOZ9SswJ
8geNoYl7tKnTbje447DR8bZDJoUZrT9zQKCqmC8qZEduars8TesGBd5yDtXxZw+p
2wtfsvhHCGRqlAi+GU/YIeERTP2wmEhpHF3Y0y6K1DcmiJja5LHEsuwauOYGZwky
/iZkvz9j0rd7OT1XBoc/lxsSSHW1As3dIKkOAV/KeZnV8twccOg5V8r/NhuKIuC8
XoCbblawdcU5zD3ZeNBQyFlUfCPrOUKPYpxt+SS2tvIF9miaopUTrpJJp91PWkWB
OYkoGm0CgYEA1PNbvZQILQkPgNNB430da8+SweDDE7zq+ae8dYDqTHrjL77PfkRa
DInI2onHTRoth1tRT0b6lfPsHnRDeF4KjA48qbV1xPb3UUhOo45jCk+vvElJQf8S
D+LNmCs/tbDl2DN/OzD1U9JyhR1VtZGAnK+ipfV8qS0zksy/zPcrKQ8CgYEAyjbc
NpUEATiqNWyjC8SGgeY8PG7lcKbiPvkmjys1d3+e8Fqf0qRzwYjp9vpTge5xq3/d
LBYlMDU6jRkxbQJXC9gJquVkgvNdLoJMcneE85jWAjBokG78LjLmvSWsSeNklj4j
ldVbXbOvU8guYhE+Mgex6lhjdiWzTnJPnG5OG6cCgYEAiSTdnX9bsJ1YNbBYi8jF
DOzW6DP3jpupfPVw4wAOZQjzjYlGmlws3kxSZaQ8DcThM341JGhi8/XuyEI6Pafb
BQ4aNXXfDeW7q8Z0ltMZp8dgN1O/cVhzanW30NtxoXL248FunFFQfhZXmLEmxNOb
T82xY05xZYbt4wooMDmyuzMCgYAFpLROnagH9LHjXc3LFUf/thI2SY4Dr9Sel0t5
MWaDmD8yTAUr1sUYQJ7u8puEA8iOVboxccjF6KZiq7JSbX9KaFQUveQpN2uBUcea
ZjWCquBGHV29sis9itQfsT52rW7wNnm9w7+SBOK+vtZ0jDClKsvPU3orIPA5Hz2T
iwyI/wKBgCZhdchoR8Es7Zw2vw5cYEVWiujiJfDoTrI4vjZ2PLfum6MPNYEKKQYs
vZqqy3vNwvzkVJ8w2GdiFsTUvbIaaJr/2McSxKttXORFOZ75RSd0WpGteBQ+cQg9
sBpAM5NoknCAuQ9j46VfcAgr8LmLVCa36rb9QtXd2bSVG9JQhlee
-----END RSA PRIVATE KEY-----
```

2.Composants de la cle

Clé privé:

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsa -in ma_cle_rsa.pem
Private-Key: (2048 bit)
modulus:
    00:a8:35:a8:e7:7a:ec:eb:ad:c2:df:22:2a:1a:3f:
    67:ed:31:b2:70:a7:2d:66:ea:75:46:21:cb:ce:38:
    cb:1f:58:e1:34:18:fa:f4:5d:1f:70:4d:8a:e7:74:
    3d:e3:16:40:07:7d:cd:f9:09:e0:33:f3:e7:3d:6e:
    b1:f9:e8:db:09:40:a8:a6:5d:05:d3:60:76:2a:f1:
    84:85:e0:a0:8d:09:8e:7d:38:03:3f:97:a2:48:c3:
    9a:3e:28:66:13:ba:0c:61:36:2a:35:7b:53:a6:7f:
    77:1f:d4:a4:b3:50:28:0c:68:9a:2f:1b:b3:fa:c9:
    1a:ff:29:ca:bc:d4:a8:8a:89:2c:31:ae:35:c0:9c:
    4a:a4:0d:6f:fd:b0:ce:e1:f1:de:6b:a1:95:0b:65:
    77:f8:75:ae:05:7b:7c:89:ac:e8:4f:b3:b8:9b:c3:
    a3:99:87:7f:b2:84:31:dc:22:d5:31:d8:c5:2f:78:
    87:02:87:20:0c:a5:da:3f:59:74:b7:f0:29:d5:af:
    08:7f:f0:73:13:e3:36:f6:00:d8:89:2d:38:67:8d:
    14:98:0e:38:97:a2:1a:63:fd:2f:cb:c2:41:ea:f3:
    aa:4b:7f:2e:77:2c:01:86:20:4a:d4:5a:a6:3a:af:
    e1:ea:63:39:92:63:7c:db:51:a9:1a:3d:b5:bf:0e:
    5d:c9
publicExponent: 65537 (0x10001)
privateExponent:
    0f:5b:2e:bb:4b:36:9b:e1:76:1b:e6:c3:8f:37:e0:
    a5:ff:d6:79:80:59:9d:be:a3:cc:2e:43:ab:e4:f5:
    6e:3c:2f:fb:10:98:c0:7c:4b:e5:75:be:cb:98:8a:
    19:d4:2b:2e:43:e6:ec:e8:60:e6:7d:4a:cc:09:f2:
    07:8d:a1:89:7b:b4:a9:d3:6e:37:b8:e3:b0:d1:f1:
    b6:43:26:85:19:ad:3f:73:40:a0:aa:98:2f:2a:64:
    47:6e:6a:bb:3c:4d:eb:06:05:de:72:0e:d5:f1:67:
    0f:a9:db:0b:5f:b2:f8:47:08:64:6a:94:08:be:19:
    4f:d8:21:e1:11:4c:fd:b0:98:48:69:1c:5d:d8:d3:
    2e:8a:d4:37:26:88:98:da:e4:b1:c4:b2:ec:1a:b8:
    e6:06:67:09:32:fe:26:64:bf:3f:63:d2:b7:7b:39:
    3d:57:06:87:3f:97:1b:12:48:75:b5:02:cd:dd:20:
    a9:0e:01:5f:ca:79:99:d5:f2:dc:1c:70:e8:39:57:
    ca:ff:36:1b:8a:22:e0:bc:5e:80:9b:6e:56:b0:75:
    c5:39:cc:3d:d9:78:d0:50:c8:59:54:7c:23:eb:39:
    42:8f:62:9c:6d:f9:24:b6:b6:f2:05:f6:68:9a:a2:
    95:13:ae:92:49:a7:dd:4f:5a:45:81:39:89:28:1a:
    6d
prime1:
    00:d4:f3:5b:bd:94:08:2d:09:0f:80:d3:41:e3:7d:
    1d:6b:cf:92:c1:e0:c3:13:bc:ea:f9:a7:bc:75:80:
    ea:4c:7a:e3:2f:be:cf:7e:44:5a:0c:89:c8:da:89:
    c7:4d:1a:2d:87:5b:51:4f:46:fa:95:f3:ec:1e:74:
    43:78:5e:0a:8c:0e:3c:a9:b5:75:c4:f6:f7:51:48:
    4e:a3:8e:63:0a:4f:af:bc:49:49:41:ff:12:0f:e2:
```

```
    cd:98:2b:3f:b5:b0:e5:d8:33:7f:3b:30:f5:53:d2:
    72:85:1d:55:b5:91:80:9c:af:a2:a5:f5:7c:a9:2d:
    33:92:cc:bf:cc:f7:2b:29:0f
prime2:
    00:ca:36:dc:36:95:04:01:38:aa:35:6c:a3:0b:c4:
    86:81:e6:3c:3c:6e:e5:70:a6:e2:3e:f9:26:8f:2b:
    35:77:7f:9e:f0:5a:9f:d2:a4:73:c1:88:e9:f6:fa:
    53:81:ee:71:ab:7f:dd:2c:16:25:30:35:3a:8d:19:
    31:6d:02:57:0b:d8:09:aa:e5:64:82:f3:5d:2e:82:
    4c:72:77:84:f3:98:d6:02:30:68:90:6e:fc:2e:32:
    e6:bd:25:ac:49:e3:64:96:3e:23:95:d5:5b:5d:b3:
    af:53:c8:2e:62:11:3e:32:07:b1:ea:58:63:76:25:
    b3:4e:72:4f:9c:6e:4e:1b:a7
exponent1:
    00:89:24:dd:9d:7f:5b:b0:9d:58:35:b0:58:8b:c8:
    c5:0c:ec:d6:e8:33:f7:8e:9b:a9:7c:f5:70:e3:00:
    0e:65:08:f3:8d:89:46:9a:5c:2c:de:4c:52:65:a4:
    3c:0d:c4:e1:33:7e:35:24:68:62:f3:f5:ee:c8:42:
    3a:3d:a7:db:05:0e:1a:35:75:df:0d:e5:bb:ab:c6:
    74:96:d3:19:a7:c7:60:37:53:bf:71:58:73:6a:75:
    b7:d0:db:71:a1:72:f6:e3:c1:6e:9c:51:50:7e:16:
    57:98:b1:26:c4:d3:9b:4f:cd:b1:63:4e:71:65:86:
    ed:e3:0a:28:30:39:b2:bb:33
exponent2:
    05:a4:b4:4e:9d:a8:07:f4:b1:e3:5d:cd:cb:15:47:
    ff:b6:12:36:49:8e:03:af:d4:9e:97:4b:79:31:66:
    83:98:3f:32:4c:05:2b:d6:c5:18:40:9e:ee:f2:9b:
    84:03:c8:8e:55:ba:31:71:c8:c5:e8:a6:62:ab:b2:
    52:6d:7f:4a:68:54:14:bd:e4:29:37:6b:81:51:c7:
    9a:66:35:82:aa:e0:46:1d:5d:bd:b2:2b:3d:8a:d4:
    1f:b1:3e:76:ad:6e:f0:36:79:bd:c3:bf:92:04:e2:
    be:be:d6:74:8c:30:a5:2a:cb:cf:53:7a:2b:20:f0:
    39:1f:3d:93:8b:0c:88:ff
coefficient:
    26:61:75:c8:68:47:c1:2c:ed:9c:36:bf:0e:5c:60:
    45:56:8a:e8:e2:25:f0:e8:4e:b2:38:be:36:76:3c:
    b7:ee:9b:a3:0f:35:81:0a:29:06:2c:bd:9a:aa:cb:
    7b:cd:c2:fc:e4:54:9f:30:d8:67:62:16:c4:d4:bd:
    b2:1a:68:9a:ff:d8:c7:12:c4:ab:6d:5c:e4:45:39:
    9e:f9:45:27:74:5a:91:ad:78:14:3e:71:08:3d:b0:
    1a:40:33:93:68:92:70:80:b9:0f:63:e3:a5:5f:70:
    08:2b:f0:b9:8b:54:26:b7:ea:b6:fd:42:d5:dd:d9:
    b4:95:1b:d2:50:86:57:9e
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAqDWo53rs663C3yIqGj9n7TGycKctZup1RiHLzjjLH1jhNBj6
9F0fcE2K53Q94xZAB33N+QngM/PnPW6x+ejbCUCopl0F02B2KvGEheCgjQmOfTgD
P5eiSMOaPihmE7oMYTYqNXtTpn93H9Sks1AoDGiaLxuz+ska/ynKvNSoioksMa41
wJxKpA1v/bDO4fHea6GVC2V3+HWuBXt8iazoT7O4m8OjmYd/soQx3CLVMdjFL3iH
AocgDKXaP1l0t/Ap1a8If/BzE+M29gDYiS04Z40UmA44l6IaY/0vy8JB6vOqS38u
dywBhiBK1FqmOq/h6mM5kmN821GpGj21vw5dyQIDAQABAoIBAA9bLrtLNpvhdhvm
```

```
w4834KX/1nmAWZ2+o8wuQ6vk9W48L/sQmMB8S+V1vsuYihnUKy5D5uzoYOZ9SswJ
8geNoYl7tKnTbje447DR8bZDJoUZrT9zQKCqmC8qZEduars8TesGBd5yDtXxZw+p
2wtfsvhHCGRqlAi+GU/YIeERTP2wmEhpHF3Y0y6K1DcmiJja5LHEsuwauOYGZwky
/iZkvz9j0rd7OT1XBoc/lxsSSHW1As3dIKkOAV/KeZnV8twccOg5V8r/NhuKIuC8
XoCbblawdcU5zD3ZeNBQyFlUfCPrOUKPYpxt+SS2tvIF9miaopUTrpJJp91PWkWB
OYkoGm0CgYEA1PNbvZQILQkPgNNB430da8+SweDDE7zq+ae8dYDqTHrjL77PfkRa
DInI2onHTRoth1tRT0b6lfPsHnRDeF4KjA48qbV1xPb3UUhOo45jCk+vvElJQf8S
D+LNmCs/tbDl2DN/OzD1U9JyhR1VtZGAnK+ipfV8qS0zksy/zPcrKQ8CgYEAyjbc
NpUEATiqNWyjC8SGgeY8PG7lcKbiPvkmjys1d3+e8Fqf0qRzwYjp9vpTge5xq3/d
LBYlMDU6jRkxbQJXC9gJquVkgvNdLoJMcneE85jWAjBokG78LjLmvSWsSeNklj4j
ldVbXbOvU8guYhE+Mgex6lhjdiWzTnJPnG5OG6cCgYEAiSTdnX9bsJ1YNbBYi8jF
DOzW6DP3jpupfPVw4wAOZQjzjYlGmlws3kxSZaQ8DcThM341JGhi8/XuyEI6Pafb
BQ4aNXXfDeW7q8Z0ltMZp8dgN1O/cVhzanW30NtxoXL248FunFFQfhZXmLEmxNOb
T82xY05xZYbt4wooMDmyuzMCgYAFpLROnagH9LHjXc3LFUf/thI2SY4Dr9Sel0t5
MWaDmD8yTAUr1sUYQJ7u8puEA8iOVboxccjF6KZiq7JSbX9KaFQUveQpN2uBUcea
ZjWCquBGHV29sis9itQfsT52rW7wNnm9w7+SBOK+vtZ0jDClKsvPU3orIPA5Hz2T
iwyI/wKBgCZhdchoR8Es7Zw2vw5cYEVWiujiJfDoTrI4vjZ2PLfum6MPNYEKKQYs
vZqqy3vNwvzkVJ8w2GdiFsTUvbIaaJr/2McSxKttXORFOZ75RSd0WpGteBQ+cQg9
sBpAM5NoknCAuQ9j46VfcAgr8LmLVCa36rb9QtXd2bSVG9JQhlee
-----END RSA PRIVATE KEY-----
```

Note:

- Equivalent à faire un cat ma_cle_rsa.pem.
- On a bien l'exposant privé pour faire le déchiffrement. Ainsi que le modulo commun. M = C^D MOD N
- On retrouve P et Q dans exponent1, et exponent2.

Clé publique:

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsa -in ma_cle_rsa.pem -pubout
writing RSA key
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsa -in ma_cle_publique_rsa.pem -text -pubin
Public-Key: (2048 bit)
Modulus:
    00:a8:35:a8:e7:7a:ec:eb:ad:c2:df:22:2a:1a:3f:
    67:ed:31:b2:70:a7:2d:66:ea:75:46:21:cb:ce:38:
    cb:1f:58:e1:34:18:fa:f4:5d:1f:70:4d:8a:e7:74:
    3d:e3:16:40:07:7d:cd:f9:09:e0:33:f3:e7:3d:6e:
    b1:f9:e8:db:09:40:a8:a6:5d:05:d3:60:76:2a:f1:
    84:85:e0:a0:8d:09:8e:7d:38:03:3f:97:a2:48:c3:
    9a:3e:28:66:13:ba:0c:61:36:2a:35:7b:53:a6:7f:
    77:1f:d4:a4:b3:50:28:0c:68:9a:2f:1b:b3:fa:c9:
    1a:ff:29:ca:bc:d4:a8:8a:89:2c:31:ae:35:c0:9c:
    4a:a4:0d:6f:fd:b0:ce:e1:f1:de:6b:a1:95:0b:65:
    77:f8:75:ae:05:7b:7c:89:ac:e8:4f:b3:b8:9b:c3:
    a3:99:87:7f:b2:84:31:dc:22:d5:31:d8:c5:2f:78:
    87:02:87:20:0c:a5:da:3f:59:74:b7:f0:29:d5:af:
    08:7f:f0:73:13:e3:36:f6:00:d8:89:2d:38:67:8d:
```

```
    14:98:0e:38:97:a2:1a:63:fd:2f:cb:c2:41:ea:f3:
    aa:4b:7f:2e:77:2c:01:86:20:4a:d4:5a:a6:3a:af:
    e1:ea:63:39:92:63:7c:db:51:a9:1a:3d:b5:bf:0e:
    5d:c9
Exponent: 65537 (0x10001)
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqDWo53rs663C3yIqGj9n
7TGycKctZup1RiHLzjjLH1jhNBj69F0fcE2K53Q94xZAB33N+QngM/PnPW6x+ejb
CUCopl0F02B2KvGEheCgjQmOfTgDP5eiSMOaPihmE7oMYTYqNXtTpn93H9Sks1Ao
DGiaLxuz+ska/ynKvNSoioksMa41wJxKpA1v/bDO4fHea6GVC2V3+HWuBXt8iazo
T7O4m8OjmYd/soQx3CLVMdjFL3iHAocgDKXaP1l0t/Ap1a8If/BzE+M29gDYiS04
Z40UmA44l6IaY/0vy8JB6vOqS38udywBhiBK1FqmOq/h6mM5kmN821GpGj21vw5d
yQIDAQAB
-----END PUBLIC KEY-----
```

Note: On retrouve bien le modulo, et l'exposant publique pour chiffrer. C = M^E MOD N.

3. Stockage de la cle RSA - en chiffré AES 128

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsa -aes128 -in ma_cle_rsa.pem -out ma_cle_rsa_chiffre.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ cat
ma_cle_rsa_chiffre.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6DB61C91EA3EE8A7E12BDF00260C05DF

ynm9hyPTn8pflFLWYLLtFTP9F3pcJnpfRsHZRu3x45Uz93UjQT2J3TYnwiFUXxk6
GbNc2xtZfa/fCggfr9uLYVnuPVr55xUCfIR1RZrYva6/g+5kWc8VPVFSjUalHdv2
kRhRV2p85UBXYwvyxjOcglvqNcubDYvEDcq08Cun8Y+GMdmusHbFGVhLDimHgVBr
uyFrH23WOJul3gjjrObdsoLKYUYctA26+fAH9eozUnPhvICEgmmHJ2/qn7PK8gzJ
Ra+Wn8a7ndg59qijsEzk+v2JJSWFkJiNZK7CEqkJ9HrrlUa8P56axjO9FebXNsfQ
RcEsOk9tAkdDRQPiwMKjVEbKhpT8ywtf44AS3G8nXG//wOb4kSNzlDWrOH6BzS/g
DX6SXWcJSjlyQfgBFT30ttVqU1zP5F6+m4oVHfknitPlOsydLrEP17hlgVe4ur2K
cTUDir1iyxThJqmguPYo6En5XXrB2DpKSYzRpkkuT29DEDrjZqOGDmYqKlkVUFkX
r2QoZPQP8548P6jaZimqOMk/KHovOiZBET8yn1cujbTwnzC0QcvsrPG3+1un+ga9
WvqtoUSrq3nd6Ysx8XaO7v2NSP6A1AiU4uCcHvn3xUSxVjvqvkldRNRbkKgkna6T
3Si9HgCqWXSMjP6jEHSrw4EHRbKeeRdY2LBzUePMAdhPRPloDQUoFDJ+zYSKS4MA
K66ME7fH7W9A54FDyKa79RqUmhSyej3eY4Uf6fUFiyNVXJ7qmy4pVGXjsx4gs0J8
i2SWr+qz6/YcwDWLYzXwEeGH+G3Y27dhrxlDr8jcRAKhFkQtgf50FTBPFeXCLcbe
cb7x1oovA7Qp7WHaED4CPLhu/fUOvHzNyd6bjDgzojPPFU7qxcBEQsu9d3e1z3M3
NQ0RJz0HA1ABe5VlYuB3y+3dOu/hdNZokae1s0ZqiTAD1riv7JdRhFtFUCmw0aWw
LYYiYHu8IqM3Jxmz5MJEbXkZ8wEULjkKJqGa/KwfZMHDspDxGdE0LbYZFxH9cbGp
lg4pdj720NQl+uFYaevvxFZNB//NVov5aAZA2i6BC6NK+ZQCFkIm8MiJsJiJ0IcS
LgqvZ3YAK7b6+NqxOGYJ/vY29crtPFdVmTw0oRJfOzzCCr65ObUeYvz2/Ewvr3lh
```

```
D+OUzT25kYdOVyWogfrb2eCdfSJnEyRDQ3ysMsnLQ9dkvF7v6s54ehfELVi2Zhw4
6/dzwxJNXeLIcI+hmcYhnOJSbPOxO2nMMjWCCpYNB2l+5k5X0Qy4s8Mi3ua+n/69
MtVG/ml0iS7roEmJi+WYRMLgIoQ0H0HbT7NFCimi6n0LIMGt8JaotctTFe8y/xTs
Ggpe8NZKzXSy0HJzr8HFh1eg78kTOHywX2mK1bKu4KaOUwwxPiZqe6Pe4D7Qlgpo
j1Cefp9BCNYHUywBZOeETSqepIrAZ+tOe0MujyTeV4R7n7qAh3JFA17sPKVZo9qn
x2pQAFHTFxeXPMzL363/kBTrXuA8dwwm3rZKQLLWL8OjcucE7Celrhs4y8Ki3m7+
wfxmCVwiMbgzg+18YruZ27TjZgQy3tl2rQEXPZS3bEA34oG8yTY6moIBhhYQ70l6
-----END RSA PRIVATE KEY-----
```

Note: On retrouve en entête les informations concernant l'algorithme AES-128-CBC utilisé pour chiffrer la clé RSA.

4. Stockage de la cle RSA

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsa -in ma_cle_rsa.pem -pubout -out ma_cle_publique_rsa.pem
writing RSA key
```

5. Chiffrer source.txt avec la clé RSA

Chiffré avec la clé ma_cle_rsa.pem.

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsautl -in source.txt -encrypt -inkey ma_cle_rsa.pem  -hexdump
0000 - 75 47 41 64 3c a0 8d ec-d6 c3 3d 0a a7 0b 8e 59   uGAd<.....=....Y
0010 - 61 12 76 78 40 fe 8d 31-a4 af 61 5b 13 a1 09 32   a.vx@..1..a[...2
0020 - 59 9a 9f f5 d7 05 8d 0e-56 34 3c a5 84 1e 68 33   Y.......V4<...h3
0030 - a8 b5 a9 63 1a c8 83 44-ab 97 45 5c f8 f1 5e 49   ...c...D..E\..^I
0040 - ac 2a 1c 03 64 e3 31 cc-17 f4 65 58 59 b5 4b 81   .*..d.1...eXY.K.
0050 - b5 2e 52 91 16 f8 b0 94-c0 ad 73 96 ac 66 04 11   ..R.......s..f..
0060 - b8 a7 db 0c ed 7e d8 1d-94 54 61 8b 0e 1a 5e ad   .....~...Ta...^.
0070 - d1 6c 3f f4 b5 19 a9 f9-33 dc dc 37 8e da 7f 99   .l?.....3..7....
0080 - 24 3b d4 c7 8b c6 79 d6-c1 52 62 c9 c2 6d 20 85   $;....y..Rb..m .
0090 - 30 0a b9 9f 5e e7 6d 7c-c9 e9 75 02 0a bd 81 9a   0...^.m|..u.....
00a0 - fd 7d ca 40 43 59 f5 70-e0 2d c3 75 43 89 0c 01   .}.@CY.p.-.uC...
00b0 - 87 5d 5b 90 a0 fe 48 6c-cc b6 78 ce a0 8d 60 5b   .][...Hl..x...`[
00c0 - 31 88 13 91 a4 c8 9f 65-57 47 ad 63 f4 b4 ce fc   1......eWG.c....
00d0 - c2 f3 03 03 7c 80 35 36-0f 20 6a cc fd 35 44 e8   ....|.56. j..5D.
00e0 - a1 ba 88 b5 72 4e f2 df-b0 4c 77 39 f3 6c c8 22   ....rN...Lw9.l."
00f0 - 82 2e 26 d9 f6 29 31 be-02 63 60 2b 7e 91 50 ab   ..&..)1..c`+~.P.
```

Chiffré avec la clé ma_cle_rsa_chiffre.pem.

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsautl -in source.txt -encrypt -inkey ma_cle_rsa_chiffre.pem  -hexdump
```

```
Enter pass phrase for ma_cle_rsa_chiffre.pem:
0000 - 9c ce da 19 d2 c6 5b 76-4d e1 73 a9 17 a9 ff 1b   ......[vM.s.....
0010 - f2 17 6b b8 29 e9 e7 f0-0b 40 7e e3 0f 4d e7 c9   ..k.)....@~..M..
0020 - eb 18 70 52 eb 03 bf 31-4c fc 82 c6 c3 57 7d b4   ..pR...1L....W}.
0030 - 4b 19 cd 67 bd ef 20 4e-dc 4a 15 96 44 33 20 07   K..g.. N.J..D3 .
0040 - 53 a7 a0 1c ac 29 9f 1c-0b 57 09 64 1d 90 66 ca   S....)...W.d..f.
0050 - e6 b2 b7 64 f2 af c4 e9-44 f7 bb 77 ed 91 a4 53   ...d....D..w...S
0060 - fc c0 72 71 f5 02 94 8e-9f c6 b5 f0 b7 5e 88 1a   ..rq.........^..
0070 - 13 8e 93 aa 91 2c 2c 61-53 9f a9 e9 b7 ff a9 48   .....,,aS......H
0080 - 12 fc 02 f9 af 57 f7 7a-e3 ef d7 18 0e c2 20 41   .....W.z...... A
0090 - 5f 2a 64 f3 5e 20 a9 b8-7e 60 f2 0c 11 70 53 a8   _*d.^ ..~`...pS.
00a0 - 37 3c 91 9f 78 21 cf 14-7d 31 b9 5c 9d fb 85 4b   7<..x!..}1.\...K
00b0 - 72 d6 5f b1 47 2e 93 54-1f b2 74 25 1a 85 f1 49   r._.G..T..t%...I
00c0 - 43 bd ff 53 24 9f 8a 03-49 7c 61 4b 6c d7 cd b7   C..S$...I|aKl...
00d0 - 37 68 96 13 95 ce b4 82-f3 3f 58 95 ae 0b 6b 31   7h.......?X...k1
00e0 - d4 09 a2 92 3b 75 5c 2f-0a 67 56 d5 20 ea f9 d7   ....;u\/.gV. ...
00f0 - 08 42 e8 29 5e 9d 66 f5-bd a4 35 97 1d 85 ca 47   .B.)^.f...5....G
```

Chiffrement avec la clé publique ma_cle_publique_rsa.pem.

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsautl -in source.txt -inkey ma_cle_publique_rsa.pem -pubin -encrypt -
hexdump
0000 - 2c e9 4f e0 d7 a5 6e cb-6c 01 1e 42 14 4d af 91   ,.O...n.l..B.M..
0010 - 9c 9d 91 69 48 aa 04 da-b8 3f 4b 33 f5 30 3d f5   ...iH....?K3.0=.
0020 - f4 32 9b d9 a7 0b 24 42-15 2a 26 f6 ad 77 10 6a   .2....$B.*&..w.j
0030 - 07 40 d7 dc 40 2c b7 18-d8 35 31 9e f7 aa 68 84   .@..@,...51...h.
0040 - c2 32 a9 89 36 3a f4 8f-9a a3 5f bf 2b 49 c3 6c   .2..6:...._.+I.l
0050 - e1 39 94 ca fc 39 1c e8-23 cb 1e 6c 63 32 79 32   .9...9..#..lc2y2
0060 - 6a 8f 7e 2f 53 9b 16 19-2a b2 d0 ae b4 03 c8 c1   j.~/S...*.......
0070 - d8 4e d5 29 1f 11 da 87-c7 9e 66 e0 0e 4d e1 ee   .N.).......f..M..
0080 - 97 59 3f fd 97 43 ba 0c-04 67 b9 8c 71 08 27 2c   .Y?..C...g..q.',
0090 - 94 85 fe d4 32 c0 10 15-cc a1 af 94 21 5b ad 52   ....2.......![.R
00a0 - 18 16 db 93 ca 3f 76 71-85 01 8c 18 fc 72 a8 0d   .....?vq.....r..
00b0 - 25 b2 44 96 ed cb 38 5c-1b f8 c8 76 3f 3a 29 75   %.D...8\...v?:)u
00c0 - f7 f5 cf 23 a7 7e 64 4a-07 39 5d 3f ae 67 cf 59   ...#.~dJ.9]?.g.Y
00d0 - 29 49 4a c9 dc ef a4 06-33 f5 c3 ba cd a2 9d f9   )IJ.....3.......
00e0 - 83 45 5a f2 d2 f2 51 a9-8c 67 6d 70 95 d8 c3 56   .EZ...Q..gmp...V
00f0 - 54 5f 6b 33 14 5f 17 49-cb b0 cc a1 49 00 05 18   T_k3._.I....I...
```

Note: On obtient des chiffrés car par défaut il y a un mode qui est utilisé. C'est le mode “PKCS#1 v1.5 (the default)” d'après le manuel.

6. Chiffrer le TP avec RSA mode OAEP

```
laubosslink@po-lbl:~/projects/courses/ensicaen/media/s4/ca/tps/tp1$ openssl
rsautl -in ../../tp_crypto_apl_2A.pdf -inkey ma_cle_publique_rsa.pem -pubin
-encrypt -oaep -hexdump
```

```
RSA operation error
140519185450656:error:0407906E:rsa routines:RSA_padding_add_PKCS1_OAEP:data
too large for key size:rsa_oaep.c:45:
```

Note: On constate que le fichier est trop volumineux pour être chiffré avec la taille de la clé OAEP. Dans ce genre de cas on passe en chiffrement symétrique. Cette limite est du au modulo, on peut aller jusqu'a 2048 bits dans le cas de notre clé généré.

Exercice 4 : certificats X509

---

1. Creation d'un certificat X509

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl req -new -key ma_cle_rsa.pem
-out certificat.csr
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]:ca
State or Province Name (full name) [Some-State]:normandie
Locality Name (eg, city) []:city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:company
Organizational Unit Name (eg, section) []:section
Common Name (e.g. server FQDN or YOUR name) []:Yasmine
Email Address []:yasmine.elhimdi@ecole.ensicaen.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:sp
```

Affichage du certificat :

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl req -in certificat.csr -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ca, ST=normandie, L=city, O=company, OU=section,
CN=Yasmine/emailAddress=yasmine.elhimdi@ecole.ensicaen.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

```
                    00:c9:9c:79:11:94:ed:ae:3e:11:d8:52:a8:f3:f6:
                    53:2b:8b:5c:78:84:34:28:37:48:d9:e6:41:2a:e8:
                    2a:83:ae:21:96:1d:79:32:8d:d6:64:a6:0d:61:57:
                    02:a2:65:f9:81:43:02:83:ec:3b:ff:6d:fa:ac:a1:
                    f5:7c:c0:c4:8c:af:e2:7b:6e:dd:d1:ca:34:53:e0:
                    40:02:4e:fd:d8:63:2c:09:e5:f5:37:b8:55:61:8e:
                    14:c9:02:b3:da:aa:4a:17:e3:0d:9d:27:f3:1a:b0:
                    a3:5c:b9:d4:2f:9a:b0:bc:d0:2f:22:b6:07:6c:28:
                    c2:3d:31:7b:00:27:49:e9:6b:cd:0e:38:af:ab:d5:
                    20:4d:db:11:d9:bf:b1:a3:14:ef:1d:ca:43:81:23:
                    c5:50:e2:33:24:00:42:fe:c4:4b:81:a1:4d:c9:ae:
                    e2:2e:42:0b:89:83:25:fb:12:64:65:0d:a2:92:ea:
                    8a:80:d6:27:d2:37:2f:bb:57:84:62:22:17:77:91:
                    ef:fe:56:eb:d9:2c:ef:a6:ae:fe:85:28:17:8b:fd:
                    f1:c4:6b:74:30:7d:9f:3d:cf:a4:8a:10:7a:8e:df:
                    a1:2e:98:cf:99:0d:7d:61:6c:01:aa:d9:c3:91:2e:
                    b9:d7:2b:06:f7:b6:05:bf:4f:4c:49:9a:8c:22:3e:
                    b2:3d
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :unable to print attribute
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
         9f:b6:95:19:e3:86:b5:a3:18:1b:06:27:81:2b:a4:63:51:03:
         cf:cf:dc:28:36:ef:ca:00:56:d6:04:56:c9:6d:dc:61:b7:66:
         0b:53:61:0e:cf:fe:70:95:22:fc:ac:12:d6:d0:da:65:6b:85:
         80:c5:a6:b8:7f:c8:14:b3:2a:70:d1:f7:19:48:86:e2:94:e6:
         a9:00:e9:2c:25:60:f7:81:4e:03:7c:bd:a2:8d:4c:bc:92:12:
         4e:9c:c0:66:1a:d4:ed:14:5e:d5:d1:cd:6c:33:0d:36:a7:78:
         f0:29:b9:9b:67:69:8a:12:7e:ac:25:f0:02:28:65:06:51:92:
         29:dd:8b:92:9e:57:d0:39:49:d0:a1:c9:f3:ec:1e:b0:f4:ed:
         27:ed:b9:ad:57:13:5c:51:a3:d3:b0:2d:03:3a:ca:3d:70:cb:
         18:d0:ba:83:9d:da:79:af:75:28:19:05:d7:b4:23:60:49:2a:
         e9:50:73:2c:61:2a:68:75:61:53:5f:24:c7:96:02:ac:cd:3d:
         7c:b2:58:bd:03:0d:46:87:4d:05:66:91:e8:5f:23:27:72:cb:
         85:72:4a:55:95:ae:51:19:96:e3:3d:4b:1a:73:8d:74:8a:2a:
         59:46:dc:fd:3f:7e:f9:8e:b3:ae:71:05:ea:62:11:3e:94:cb:
         a7:8c:65:e0
-----BEGIN CERTIFICATE REQUEST-----
MIIDCDCCAfACAQAwgZgxCzAJBgNVBAYTAmNhMRIwEAYDVQQIDAlub3JtYW5kaWUx
DTALBgNVBAcMBGNpdHkxEDAOBgNVBAoMB2NvbXBhbnkxEDAOBgNVBAsMB3NlY3Rp
b24xEDAOBgNVBAMMB1lhc21pbmUxMDAuBgkqhkiG9w0BCQEWIXlhc21pbmUuZWxo
aW1kaUBlY29sZS5lbnNpY2Flbi5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMmceRGU7a4+EdhSqPP2UyuLXHiENCg3SNnmQSroKoOuIZYdeTKN1mSm
DWFXAqJl+YFDAoPsO/9t+qyh9XzAxIyv4ntu3dHKNFPgQAJO/dhjLAnl9Te4VWGO
FMkCs9qqShfjDZ0n8xqwo1y51C+asLzQLyK2B2wowj0xewAnSelrzQ44r6vVIE3b
Edm/saMU7x3KQ4EjxVDiMyQAQv7ES4GhTcmu4i5CC4mDJfsSZGUNopLqioDWJ9I3
L7tXhGIiF3eR7/5W69ks76au/oUoF4v98cRrdDB9nz3PpIoQeo7foS6Yz5kNfWFs
AarZw5EuudcrBve2Bb9PTEmajCI+sj0CAwEAAaAqMBMGCSqGSIb3DQEJAjEGDARz
cHNzMBMGCSqGSIb3DQEJBzEGDAQxMjM0MA0GCSqGSIb3DQEBCwUAA4IBAQCftpUZ
44a1oxgbBieBK6RjUQPPz9woNu/KAFbWBFbJbdxht2YLU2EOz/5wlSL8rBLW0Npl
```

```
a4WAxaa4f8gUsypw0fcZSIbilOapAOksJWD3gU4DfL2ijUy8khJOnMBmGtTtFF7V
0c1sMw02p3jwKbmbZ2mKEn6sJfACKGUGUZIp3YuSnlfQOUnQocnz7B6w9O0n7bmt
VxNcUaPTsC0DOso9cMsY0LqDndp5r3UoGQXXtCNgSSrpUHMsYSpodWFTXyTHlgKs
zT18sli9Aw1Gh00FZpHoXyMncsuFckpVla5RGZbjPUsac410iipZRtz9P375jrOu
cQXqYhE+lMunjGXg
-----END CERTIFICATE REQUEST-----
```

Note: La clé privé n'y figure pas, on retrouve uniquement la clé publique (modulo, et l'exposant publique).

2. Envoi de requete de certificat a une autorite de certification

---

Generation d'une cle RSA 2048

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl genrsa 2048 > rsa_key.pem
Generating RSA private key, 2048 bit long modulus
.......+++
.....................................................................
......+++
e is 65537 (0x10001)
```

Chiffrement de la cle RSA :

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl rsa -aes128 -in rsa_key.pem
-out ca.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Creation du certificat X509

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl req -new -x509 -key ca.key
-out ca.crt
Enter pass phrase for ca.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]:fr
State or Province Name (full name) [Some-State]:normandie
Locality Name (eg, city) []:city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:company
Organizational Unit Name (eg, section) []:section
Common Name (e.g. server FQDN or YOUR name) []:yasmine
```

```
Email Address []:yasmine.elhimdi@ecole.ensicaen.fr
```

3. Signature du certificat et verification

```
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl x509 -CAcreateserial -
CAserial ca.srl -CAkey ca.key -in ca.crt
elhimdi@e204pc03:~/Documents/S3/Crypto$ openssl verify ca.crt
ca.crt: C = fr, ST = normandie, L = city, O = company, OU = section, CN =
yasmine, emailAddress = yasmine.elhimdi@ecole.ensicaen.fr
error 18 at 0 depth lookup:self signed certificate
OK
```

[1)] ici CBC, donc un XOR ente l'IV et le message clair