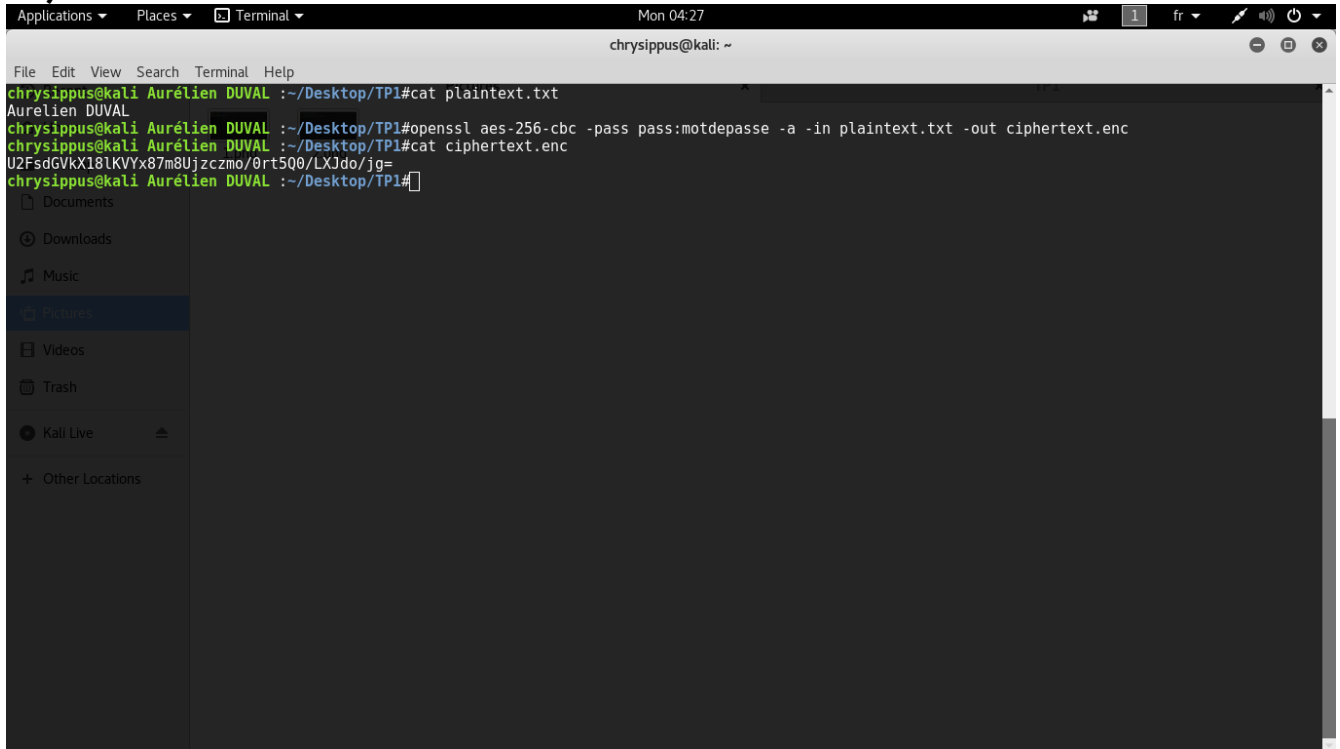


## TP1 : Cryptographie et sécurité informatique

### Exercice 3 : OpenSSL

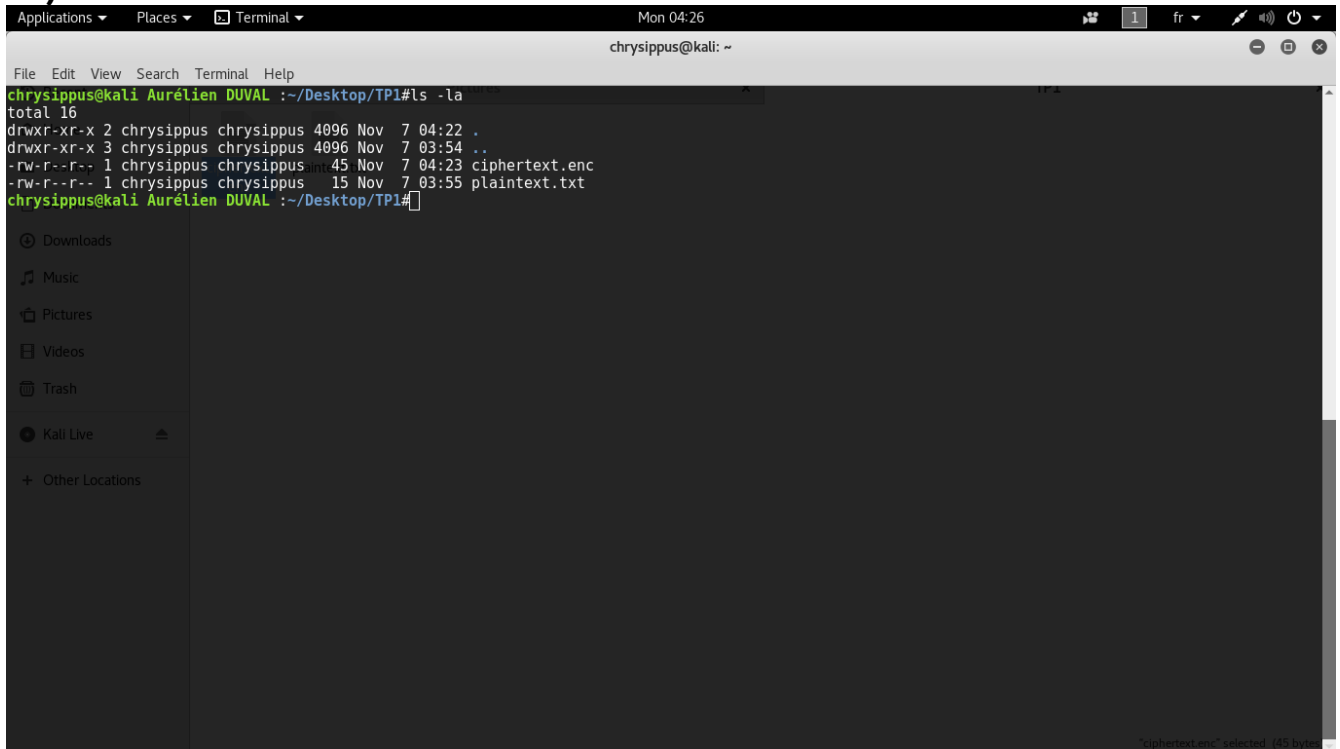
1)



A terminal window titled 'chrysippus@kali: ~' showing the following commands and output:

```
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cat plaintext.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#openssl aes-256-cbc -pass pass:motdepasse -a -in plaintext.txt -out ciphertext.enc
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cat ciphertext.enc
U2FsdGVkX18lKVYx87m8Ujzczo/0rt5Q0/LXJdo/jg=
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#
```

2)



A terminal window titled 'chrysippus@kali: ~' showing the following command and output:

```
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#ls -la
total 16
drwxr-xr-x 2 chrysippus chrysippus 4096 Nov  7 04:22 .
drwxr-xr-x 3 chrysippus chrysippus 4096 Nov  7 03:54 ..
-rw-r--r-- 1 chrysippus chrysippus   45 Nov  7 04:23 ciphertext.enc
-rw-r--r-- 1 chrysippus chrysippus   15 Nov  7 03:55 plaintext.txt
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#
```

On remarque que le fichier chiffré pèse 45 octets alors que le fichier d'origine ne pèse que 15 octets. Ceci s'explique par la présence du bloc c0 généré par le système pour le

mode cbc, mais aussi par le fait qu'openssl utilise des blocs de taille 16 octets pour effectuer le chiffrement, ainsi il complète avec un padding le fichier d'origine qui est de 15 octets.

3)

```
Applications ▾ Places ▾ Terminal ▾ Mon 04:43
chrysippus@kali: ~

File Edit View Search Terminal Help
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cat plaintext.txt
Aurelien DUVAL
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#openssl des-ede3-ofb -pass pass:motdepasse -in plaintext.txt -out ciphertextDES.enc
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cat ciphertextDES.enc
Salted 00G000!00000
00MD0m700chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#^C
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#openssl des-ede3-ofb -pass pass:motdepasse -in ciphertextDES.enc -out plaintextDES.txt -d
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cat plaintextDES.txt
Aurelien DUVAL
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#
```

4)

```
Applications ▾ Places ▾ Terminal ▾ Mon 04:49
chrysippus@kali: ~

File Edit View Search Terminal Help
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#mkdir Aurelien\ DUVAL
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cp plaintext.txt Aurelien\ DUVAL/
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#cd Aurelien\ DUVAL/
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#ls
plaintext.txt
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#tar cvf plaintext.tar plaintext.txt
plaintext.txt
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#ls
plaintext.tar plaintext.txt
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#openssl desx-cbc -pass pass:motdepasse -in plaintext.tar -out plaintextTar.enc -p
salt=AFD28B614E63C323
key=7D189ACCCF9736C91808CB8B89479618E6168AA597383CD8
iv =770918A4C319AA05
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#ls -la
total 36
drwxr-xr-x 2 chrysippus chrysippus 4096 Nov  7 04:48 .
drwxr-xr-x 3 chrysippus chrysippus 4096 Nov  7 04:44 ..
-rw-r--r-- 1 chrysippus chrysippus 10240 Nov  7 04:46 plaintext.tar
-rw-r--r-- 1 chrysippus chrysippus 10264 Nov  7 04:48 plaintextTar.enc
-rw-r--r-- 1 chrysippus chrysippus 15 Nov  7 04:44 plaintext.txt
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1/Aurelien DUVAL#
```

5)

```

Applications Places Terminal Mon 04:58
chrysippus@kali: ~

File Edit View Search Terminal Help

chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#openssl rand 16 -hex > initialVector.txt
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#openssl rand 16 -hex > key.txt
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#cat initialVector.txt && cat key.txt && cat plaintext.txt
b9b7823e2db812abc2272c36f6d82d32 2.png 3.png 4.png
20f7acc5d3c57f23ba260212be65269
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#openssl camellia-128-cbc -in plaintext.txt -out ciphertextCamellia.enc -K 20f7acc5d3c57f23ba260212be65269 -iv b9b7823e2db812abc2272c36f6d82d32
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#cat ciphertextCamellia.enc
00000000: 4175 7265 6c69 656e 2044 5556 414c 0a01 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#cat ciphertextCamellia.enc
c5d3c57f23ba260212be65269 -iv b9b7823e2db812abc2272c36f6d82d32 -d
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#cat plaintextCamellia.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1/Aurélien DUVAL#

```

6)

```

Applications Places Terminal Mon 05:09
chrysippus@kali: ~

File Edit View Search Terminal Help

chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in plaintext.txt -out ciphertextBf3.enc
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in ciphertextBf3.enc -out plaintextBf3.txt -d -nopad
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#xxd plaintextBf3.txt
00000000: 4175 7265 6c69 656e 2044 5556 414c 0a01 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#nano plaintext2.txt
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#cat plaintext2.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#cat plaintext.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in plaintext2.txt -out ciphertextBf2.enc
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in ciphertextBf2.enc -out plaintextBf2.txt -d -nopad
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#xxd plaintextBf2.txt
00000000: 4175 7265 6c69 656e 2044 5556 410a 0202 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#nano plaintext3.txt
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#cat plaintext3.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in plaintext3.txt -out ciphertextBf3.enc
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in ciphertextBf3.enc -out plaintextBf3.txt -d -nopad
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#xxd plaintextBf3.txt
00000000: 4175 7265 6c69 656e 2044 5556 0a03 0303 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#nano plaintext4.txt
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#cat plaintext4.txt
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in plaintext4.txt -out ciphertextBf4.enc
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#openssl bf-cbc -pass pass:motdepasse -in ciphertextBf4.enc -out plaintextBf4.txt -d -nopad
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#xxd plaintextBf4.txt
00000000: 4175 7265 6c69 656e 2044 550a 0404 0404 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#cat plaintextBf3.txt && cat plaintextBf2.txt && cat plaintextBf3.txt && cat plaintextBf4.txt
Aurélien DUVAL
Aurélien DUVAL
Aurélien DUVAL
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#xxd plaintextBf3.txt && xxd plaintextBf2.txt && xxd plaintextBf3.txt && xxd plaintextBf4.txt
00000000: 4175 7265 6c69 656e 2044 5556 414c 0a01 Aurelien DUVAL...
00000000: 4175 7265 6c69 656e 2044 5556 410a 0202 Aurelien DUVAL...
00000000: 4175 7265 6c69 656e 2044 5556 0a03 0303 Aurelien DUVAL...
00000000: 4175 7265 6c69 656e 2044 550a 0404 0404 Aurelien DUVAL...
chrysippus@kali Aurélien DUVAL ~/Desktop/TP1#

```

On constate que le bourrage est de taille 2 puis 3,4 et enfin 5. En effet lorsque l'on enlève un caractère au fichier d'origine le programme remplit le vide par du padding/bourrage car la taille du fichier n'est pas un multiple de la taille d'un bloc traité.

The screenshot shows a Kali Linux terminal window with the following content:

```
Applications | Places | Terminal | Mon 05:21
chrysippus@kali: ~

File Edit View Search Terminal Help

chrysippus@kali Aurelien DUVAl :~/Desktop/TP1$ openssl speed aes
Doing aes-128 cbc for 3s on 16 size blocks: 11401378 aes-128 cbc's in 2.99s
Doing aes-128 cbc for 3s on 64 size blocks: 3153096 aes-128 cbc's in 2.99s
Doing aes-128 cbc for 3s on 256 size blocks: 798491 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 1024 size blocks: 441547 aes-128 cbc's in 2.98s
Doing aes-128 cbc for 3s on 8192 size blocks: 55428 aes-128 cbc's in 2.98s
Doing aes-192 cbc for 3s on 16 size blocks: 9591736 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 64 size blocks: 2576845 aes-192 cbc's in 2.99s
Doing aes-192 cbc for 3s on 256 size blocks: 658939 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 1024 size blocks: 370964 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 8192 size blocks: 47929 aes-192 cbc's in 3.00s
Doing aes-256 cbc for 3s on 16 size blocks: 8409649 aes-256 cbc's in 2.99s
Doing aes-256 cbc for 3s on 64 size blocks: 2206365 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 256 size blocks: 572442 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 1024 size blocks: 323874 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 8192 size blocks: ^C
chrysippus@kali Aurelien DUVAl :~/Desktop/TP1$ openssl speed des
Doing des cbc for 3s on 16 size blocks: 6519671 des cbc's in 3.00s
Doing des cbc for 3s on 64 size blocks: 1675503 des cbc's in 2.99s
Doing des cbc for 3s on 256 size blocks: 419695 des cbc's in 3.00s
Doing des cbc for 3s on 1024 size blocks: 105637 des cbc's in 3.00s
Doing des cbc for 3s on 8192 size blocks: 13305 des cbc's in 3.00s
Doing des ede3 for 3s on 16 size blocks: 581385 des ede3's in 2.93s
Doing des ede3 for 3s on 64 size blocks: 47716 des ede3's in 2.74s
Doing des ede3 for 3s on 256 size blocks: 9291 des ede3's in 2.39s
Doing des ede3 for 3s on 1024 size blocks: 2841 des ede3's in 2.54s
Doing des ede3 for 3s on 8192 size blocks: 394 des ede3's in 2.60s
OpenSSL 1.0.2h  3 May 2016
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(idx,cisc,16,int) aes(partial) blowfish(idx)
compiler: gcc -I . -I. -I./include -fPIC -DOPENSSL_PIC -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -m64 -DL_ENDIAN -g -O2 -fstack-prot
ector-strong -Wformat -Werror=format-security -Wdate-time -D_FORTIFY_SOURCE=2 -Wl,-z,relro -Wa,--noexecstack -Wall -DMD32_REG_T=int -DOPENSSL_IA32_SSE
2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSA256_ASM -DSA512_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM
-DWHIRLPOOL_ASM -DGHASH_ASM -DECP_NISTZ256_ASM
The 'numbers' are in 1000s of bytes per second processed.
type          16 bytes      64 bytes      256 bytes    1024 bytes    8192 bytes
des cbc       34771.58k     35863.61k     35813.97k     36057.43k     36331.52k
des ede3      3174.80k        1114.53k         995.19k         1145.35k         1241.40k
```

```
Applications ▾ Places ▾ Terminal ▾ Mon 05:23
chrysippus@kali: ~

File Edit View Search Terminal Help

chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#openssl speed des
Doing des cbc for 3s on 16 size blocks: 6412308 des cbc's in 2.97s
Doing des cbc for 3s on 64 size blocks: 1659259 des cbc's in 2.98s
Doing des cbc for 3s on 256 size blocks: 419776 des cbc's in 2.98s
Doing des cbc for 3s on 1024 size blocks: 105952 des cbc's in 2.99s
Doing des cbc for 3s on 8192 size blocks: 13220 des cbc's in 2.99s
Doing des ede3 for 3s on 16 size blocks: 2504278 des ede3's in 2.99s
Doing des ede3 for 3s on 64 size blocks: 625937 des ede3's in 3.00s
Doing des ede3 for 3s on 256 size blocks: 157274 des ede3's in 2.99s
Doing des ede3 for 3s on 1024 size blocks: 39104 des ede3's in 3.00s
Doing des ede3 for 3s on 8192 size blocks: ^C
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#openssl speed rsa
Doing 512 bit private rsa's for 10s: 95563 512 bit private RSA's in 9.99s
Doing 512 bit public rsa's for 10s: 1258876 512 bit public RSA's in 9.99s
Doing 1024 bit private rsa's for 10s: 34080 1024 bit private RSA's in 10.00s
Doing 1024 bit public rsa's for 10s: 517064 1024 bit public RSA's in 9.98s
Doing 2048 bit private rsa's for 10s: 7313 2048 bit private RSA's in 9.97s
Doing 2048 bit public rsa's for 10s: 165269 2048 bit public RSA's in 10.00s
Doing 4096 bit private rsa's for 10s: 688 4096 bit private RSA's in 10.00s
Doing 4096 bit public rsa's for 10s: 45137 4096 bit public RSA's in 10.00s
OpenSSL 1.0.2h  3 May 2016
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(idx,cisc,16,int) aes(partial) blowfish(idx)
compiler: gcc -I. -I. -I../include -fPIC -DOPENSSL_PIC -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -m64 -DL_ENDIAN -g -O2 -fstack-protector-strong -Wformat -Werror=format-security -Wdate-time -D_FORTIFY_SOURCE=2 -Wl,-z,relro -Wl,-z,relro -Wa,--noexecstack -Wall -DMD32_REG_T=int -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DWHIRLPOOL_ASM -DGHASH_ASM -DECP_NISTZ256_ASM
      sign    verify      sign/s verify/s
rsa 512 bits 0.000105s 0.000008s 956.9 126013.6
rsa 1024 bits 0.000293s 0.000019s 3408.0 51810.0
rsa 2048 bits 0.001363s 0.000061s 733.5 16526.9
rsa 4096 bits 0.014535s 0.000222s 68.8 4513.7
chrysippus@kali Aurélien DUVAL :~/Desktop/TP1#
```

On constate que RSA s'applique 172354 fois en 3 secondes pour des blocs de taille 1024b alors que DES ne s'applique que 105952 fois en 3 secondes pour des blocs de même taille. Encore une fois DES est plus lent !!