PROTOCOLE TLS/SSL

1. CHIFFREMENT ASYMÉTRIQUE

1. Quelle est la version du paquet OpenSSL de votre système ? Où se trouve les certificats des différents CA (Certification Authority) sur votre environnement ?

openssl version -a

```
stanne@stanne:~$ openssl version -a
OpenSSL 1.1.1n  15 Mar 2022
built on: Tue May 10 18:37:36 2022 UTC
platform: debian-amd64
options:  bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -ffile-prefix-map
=/build/openssl-iy042u/openssl-1.1.1n=. -fstack-protector-strong -Wformat -Werror=format-security -D
OPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_A
SM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK16
00_ASM -DRC4_ASM -DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOL
Y1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-1.1"
Seeding source: os-specific
```

openssl version -d

```
stanne@stanne:~$ openssl version -d
OPENSSLDIR: "/usr/lib/ssl"
```

2. Chiffrement asymétrique avec RSA :

a. Générer un couple de clés (publique, privée) pour Alice et sauvegarder-le dans un fichier cle.pem. Quel est le codage utilisé dans ce fichier ?

openssl genrsa -out cle.pem 1024

```
stanne@stanne:~$ openssl version -d
OPENSSLDIR: "/usr/lib/ssl"
stanne@stanne:~$ openssl genrsa -out cle.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....................................+++++
.............+++++
e is 65537 (0x010001)
```

Le fichier au format PEM (Privacy Enhanced Mail, format en base 64) :

cat cle.pem

```
stanne@stanne:~$ cat cle.pem
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDii2MLnBqZQ97SlzM+adVDMYxIkncU/uH+7vIsA8OhdplPSEyh
rnOpqEW2jad8T+Jj3iQluLzOtc+PRGOwAtQs29P2Yc45RzCIgUP7z+fBGjEWHNQP
BPAyyM9QQ563fn+krqmLTOi2tF2JVS6YlF4VM9xyct1iHvACXfxkFPNqcQIDAQAB
AoGABMfaPDl8GjXjcuA79Zo4JOXbxwBIQQor7LxQIfumjYk6LQEilNrgyOtAxVxx
516sMV1Tt/QRELzxd12DTFsS7SFAbU+bSvGcOefdyqyxS4ToiApu+6MGuLoFNy2q
1TPknnd6B4mJSPS2oXEmzdcjOXMZSTelyK3FUBOrquz7iiOCQQDxwhtkqRQvflOq
Bm3KxBvWt8VEKHmK3UcGIcsuVnjMbLcig7I7ZFdLMfVJcvtHzHx9+5RvTcir7Br8
8Eo1Rp+7AkEA7+PYZCMBwUu/W3YYwlJwGdDhPBExhL5frxFBK9zofMv3Vx2zYy5k
mBQKjaGEIrkZqzD1iNYQXnhbKkvxxU3NwwJAK43732uyrkfFDOmxmAkytsFO8dOU
6hapeApYj5WW18WyTK6LSrXuICbO+PGVIb9OYmgTuuW51Hep+Q3VYLnDhwJAB9zL
5txO3msBJppETXouOmpiN3nIybUDpdVG8YOYAZ8dyDks+/81RNbDUckNb6XpdXbx
VT7O4onHUyeSEQ1vyQJAegsNSdyYohLOMt+H1R/cXTyK6ERhde/FuOeXGIR4m7WG
nx4wSYfq+4DFHS39A2STL6ybAUXXaK3N/gtNbJD55g==
-----END RSA PRIVATE KEY-----
```

b. Comment extraire la clé publique sauvegardée dans cle.pem afin de de la stocker dans pub.pem ?

La partie publique de la paire de clés RSA est publique, donc n'importe qui peut communiquer avec elle. Avec l'option -pubout, vous pouvez exporter la partie publique de la clé.

openssl rsa -in cle.pem -pubout – out pub.pem
Pour verifier : cat pub.pem

```
stanne@stanne:~$ openssl rsa -in cle.pem -pubout -out pub.pem
writing RSA key
stanne@stanne:~$ cat pub.pem
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDii2MLnBqZQ97SlzM+adVDMYxI
kncU/uH+7vIsA8OhdplPSEyhrnOpqEW2jad8T+Jj3iQluLzOtc+PRGOwAtQs29P2
Yc45RzCIgUP7z+fBGjEWHNQPBPAyyM9QQ563fn+krqmLTOi2tF2JVS6YlF4VM9xy
ct1iHvACXfxkFPNqcQIDAQAB
-----END PUBLIC KEY-----
```

c. Bob, qui est en procession du fichier pub.pem, veut chiffrer un message secret et l'envoyer à Alice en utilisant la clé publique d'Alice. Il envoie le à Alice le message chiffré. Quelle est la commande à utiliser ?
openssl rsautl -encrypt -in messagesecret.txt -inkey -pub.pem –pubin -out messagechiffre.txt
cat messagechiffre.txt

```
cle.pem  messagechiffre.txt  messagesecret.txt  pub.pem
stanne@stanne:~$ openssl rsautl -encrypt -in messagesecret.txt -inkey pub.pem -pubin -out messagechi
ffre.txt
stanne@stanne:~$ cat messagechiffre.txt
|}♦o♦♦af♦♦♦♦bL♦♦1       ♦♦3uS♦♦''♦♦V♦v♦Js.♦)~♦(JQ♦♦O♦♦♦♦s♦♦zj♦♦♦♦H♦C♦♦xb♦t♦♦P#d♦♦ ♦Xx ♦A&-r''XK)♦♦♦♦^h
H♦$o♦♦v¦¶ /Gi¶V¥^´s├┼┼e@s├┼┼e:·$
```

d. Quelle est la commande qui permet à Alice de déchiffrer le secret en utilisant sa clé privée ?

openssl rsautl -decrypt -in messagechiffre.txt -inkey cle.pem -out messagedechiffre.txt
cat messagedechiffre.txt

```
cle.pem  messagechiffre.txt  messagedechiffre.txt  messagesecret.txt  pub.pem
stanne@stanne:~$ openssl rsautl -decrypt -in messagechiffre.txt -inkey cle.pem -out messagedechiffre
.txt
stanne@stanne:~$ cat messagedechiffre.txt
```