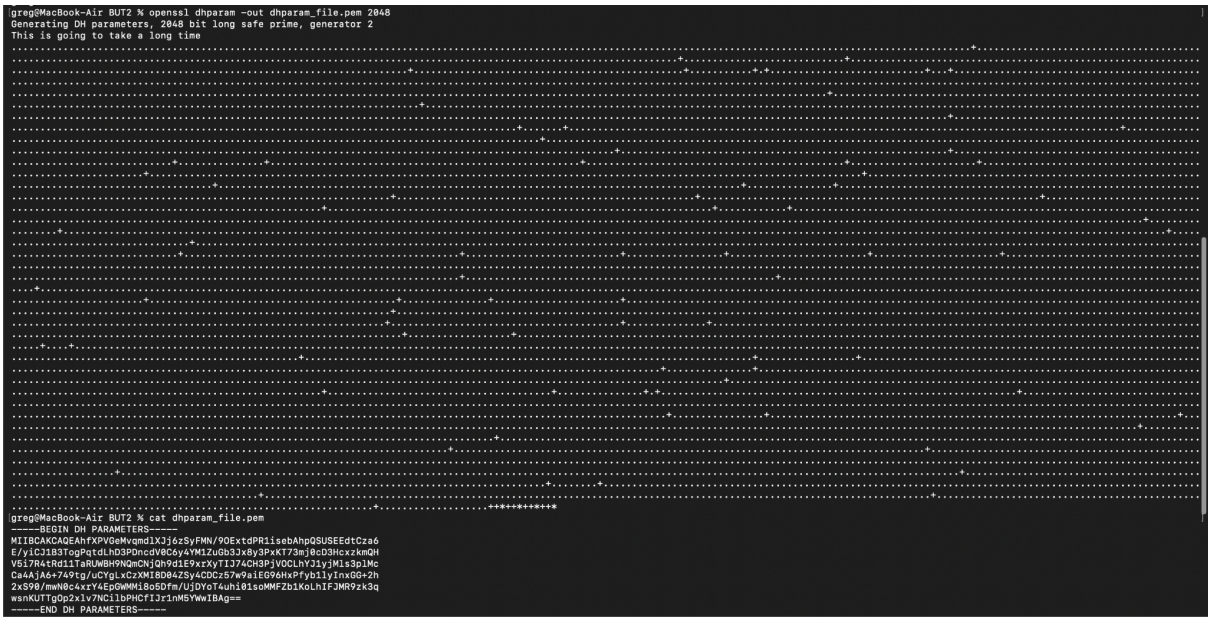
# TP2 : Protocole d’échange de clés Diffie-Hellman

## Q1)

Génération du fichier dhparams.pem contenant les paramètres Diffie-Hellman, transmi par message à Alice :



## Q2)

Génération des paires de clés d'Alice et Bob.

Pour BOB :

```
[greg@MacBook-Air BUT2 % openssl genpkey -paramfile dhparam_file.pem -out bob_privkey.pem
[greg@MacBook-Air BUT2 % openssl pkey -in bob_privkey.pem -pubout -out bob_pubkey.pem
[greg@MacBook-Air BUT2 % cat bob_privkey.pem
-----BEGIN PRIVATE KEY-----
MIICJgIBADCCARcGCSqGSIb3DQEDATCCAQgCggEBAIX1z1RnjL6pnZVyY+s0shTD
f/ThMbXT0dYrHmwIaUElEhBHbQs2uhP8ogidQd06ID6rXS4Q9zw53HVdAusuGDNW
bhm9ycfMtz8Sk+95o9HA9x3Mc5JkB1eYu0eLUXddU2kVFgR/TUJgjY0IfXdRPca1
8kyCe+Ah9z41Tgi4WCdcozJbN6ZTHAmuAIwOvu+PbYP7gmIC8Qs1zCPA9OGUsuAg
ws+e8PWohBveh8T38m9ZciJ8RhvtodsUvdP5sDdHOMa2OBKRljDIvKOQ35v1Iw2K
E+LoYtNbKDDBWW9SqC4SBSTEfc5N6sLJylE04DqdsZb+zQopWzxwnyCa9ZzOWFsC
AQIEggEEAoIBAE8MZC8SLhyiIbbl8w7+5mZ61k/8lPmc6FzyJHLkIyveGXcZgNeZ
OnrrbnOaHP55hGZaSWMf7SQyGyMwaSY+9eQKMYGVGu+UYKpSqhvbnh7I2mM0D6xb
S0CwxfD3aB+tfv2i2lExAfJ10x9kOcqP495jpNcngM1zJ4JLe46yl6MCEuYKk/CY
H5ANP/HaOTbMSqJWrOQQ2wqVc5sT0eN8mPUEV2q0J3Z0E5FidWOgTSk4VLanEkiE
K3GZ6onOfzy7Td+GIxrzuUDjgbTWPAkcTyvzicig9S3LF3vPnGoYejx4dNPAPuAL
okg57Rz674zAlE5wWuPTzWNIN8GszxLSpCU=
-----END PRIVATE KEY-----
[greg@MacBook-Air BUT2 % cat bob_pubkey.pem
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAIX1z1RnjL6pnZVyY+s0shTDf/Th
MbXT0dYrHmwIaUElEhBHbQs2uhP8ogidQd06ID6rXS4Q9zw53HVdAusuGDNWbhm9
ycfMtz8Sk+95o9HA9x3Mc5JkB1eYu0eLUXddU2kVFgR/TUJgjY0IfXdRPca18kyC
e+Ah9z41Tgi4WCdcozJbN6ZTHAmuAIwOvu+PbYP7gmIC8Qs1zCPA9OGUsuAgws+e
8PWohBveh8T38m9ZciJ8RhvtodsUvdP5sDdHOMa2OBKRljDIvKOQ35v1Iw2KE+Lo
YtNbKDDBWW9SqC4SBSTEfc5N6sLJylE04DqdsZb+zQopWzxwnyCa9ZzOWFsCAQID
ggEFAAKCAQBuHnJ0AUF1xVvGFG0QTxJF36v4+/nrp0LIwH65UOw4DrcRvsAvISll
rVYv9Jvf9LM/oAqUZemLbW3m7cHgeChclbq38BBraJzmU3a8FzZZqzoTxnngrySD
/6JDDQtwDdeFpCFBRsnZ0S+VNmuAS4w2cXy6KbqXPRSrwm7Ig1Vywv1IvC1HukHk
FUHw+PI7001m0TRvUHnmt70boadT6wJTz3CavABAQt3OEm/5Dgam1Ynr4JZxYjex
fkoHGP8J2w1GTCi5i0wFo7noPedklu82qlucWvKLuKs/JvNJgolunzqgOwXR8/qp
l3iOeju/BiZCs++RnvHNOhuJNL4EWNUV
-----END PUBLIC KEY-----
greg@MacBook-Air BUT2 %
```

Pour ALICE :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ openssl genpkey -paramfile dhparam_file.pem -out alice_privkey.pem
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ openssl pkey -in alice_privkey.pem -pubout -out alice_pubkey.pem
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat alice_pubkey.pem
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAIX1z1RnjL6pnZVyY+s0shTDf/Th
MbXT0dYrHmwIaUElEhBHbQs2uhP8ogidQd06ID6rXS4Q9zw53HVdAusuGDNWbhm9
ycfMtz8Sk+95o9HA9x3Mc5JkB1eYu0eLUXddU2kVFgR/TUJgjY0IfXdRPca18kyC
e+Ah9z41Tgi4WCdcozJbN6ZTHAmuAIwOvu+PbYP7gmIC8Qs1zCPA9OGUsuAgws+e
8PWohBveh8T38m9ZciJ8RhvtodsUvdP5sDdHOMa2OBKRljDIvKOQ35v1Iw2KE+Lo
YtNbKDDBWW9SqC4SBSTEfc5N6sLJylE04DqdsZb+zQopWzxwnyCa9ZzOWFsCAQID
ggEFAAKCAQA3Y0+uK920ZHiE5FHDKJ4K23u6oGxgmrowxxLwNI+a+BPy2t2xvgIh
McMYj5K94eeTNQ4W/PSN6sBpcsVk0tvtBq4kC1bGSt+6J8P87rkw2OPtGhimPHKG
8qc9OLaDzzYI3EsqoVW8E516LiWDnuE/OAQgw6xKvV/tf4bYzwTu9JqCXDHtXPDY
fzMZ9AwvLc5noKcKj1pOj9TPCYzvCoH0fVT5nlIfSFBNDpRyZp0p/VpkgoyVwe9M
DJkhxbh6XlIK5tpMZ950WYdup8No468oHvhUE0ZR4VZWreYdSF3+5xDnbWI0O+0u
kqNrx7uHnqrEL8aXSvzUiDl+4mY1jg6r
-----END PUBLIC KEY-----
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat alice_privkey.pem
-----BEGIN PRIVATE KEY-----
MIICJgIBADCCARcGCSqGSIb3DQEDATCCAQgCggEBAIX1z1RnjL6pnZVyY+s0shTD
f/ThMbXT0dYrHmwIaUElEhBHbQs2uhP8ogidQd06ID6rXS4Q9zw53HVdAusuGDNW
bhm9ycfMtz8Sk+95o9HA9x3Mc5JkB1eYu0eLUXddU2kVFgR/TUJgjY0IfXdRPca1
8kyCe+Ah9z41Tgi4WCdcozJbN6ZTHAmuAIwOvu+PbYP7gmIC8Qs1zCPA9OGUsuAg
ws+e8PWohBveh8T38m9ZciJ8RhvtodsUvdP5sDdHOMa2OBKRljDIvKOQ35v1Iw2K
E+LoYtNbKDDBWW9SqC4SBSTEfc5N6sLJylE04DqdsZb+zQopWzxwnyCa9ZzOWFsC
AQIEggEEAoIBAHkElkHiW11BFe1d1D/H+0O6a2JoPnX7hktplcshG2px9WwNdSWE
K46OXTdp+Cqyff8hyUsYJNOSeANmiwhTfbs/kF0gdXc5zaEx8ZTH3OjTXgdWZK4b
T74ZncmtFpPt+Zmo0B9piQe0ktpVBMt3oEjuoW/G58FAVUld3o84BMeub/NmDxqx
L1bVqTpYUKaZToa8bJCpt1TV7/j7ub7FUlj9IWWocBIaPsp0TOVypxLFGDJuFGPy
RMS2QkEV7e+SlQLfpsTUrtZWeDwgAIUeo4L39NLti1Fca7uQaDQWhC7IXkGHLla2
sN9q1+CbzE9DvRGKYjKivNK2YtOahRRYGyY=
-----END PRIVATE KEY-----
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```

## Q3)

Chez Bob :

```
[greg@MacBook-Air BUT2 % openssl pkeyutl -derive -inkey bob_privkey.pem -peerkey alice_pubkey.pem -out sharedkey.bin
[greg@MacBook-Air BUT2 % cat sharedkey.bin
e??E/&0?[x?]???cM?e??ZS?S?\k
                            D?0?
K?1??i????Wf???5$??     ??!?2Ec?ld?oo?C??rf6J{?????u?p6?=W????'Mt?G?Bw????go?
?'v4Y o??t?????{?v?Y??j?v^
[??O????????3xAi?hT??^?i=c????:R?ŷ?ą Ekw=???19%
greg@MacBook-Air BUT2 % xxd sharedkey.bin
00000000: 65c1 cd45 142f 2630 cd11 5b78 ee92 b6ab  e..E./&0..[x....
00000010: 8997 c20f 634d a3cf b5ca fb5a 1753 9d53  ....cM.....Z.S.S
00000020: a45c 6b0c 44e1 9730 970b f8b8 c8e5 b5dc  .\k.D..0........
00000030: 0384 cad8 692b f888 83a9 6bb2 0206 be5d  ....i+....k....]
00000040: 46d9 633d 305c ec4d 27d5 47e4 ce19 f904  F.c=0\.M'.G.....
00000050: f4cf 610d 4b3f 31a0 bf69 bdd8 e1af d704  ..a.K?1..i......
00000060: c69c 6695 b4b6 3524 028a c509 a6f6 2197  ..f...5$......!.
00000070: 3245 1363 d26c 6400 c66f 111b 2d87 6fd0  2E.c.ld..o..-.o.
00000080: 43c6 d872 6636 d492 7bdf 9fc7 fa3f 75ad  C..rf6..{....?u.
00000090: 7036 d63d 57c1 82ae 8f27 4dc5 a5d3 47d4  p6.=W....'M...G.
000000a0: 4277 bc9b fbe0 676f 8f05 0af0 2776 1134  Bw....go....'v.4
000000b0: 5920 6f94 a074 c2f9 99f9 e07b ef76 b2f3  Y o..t.....{.v..
000000c0: a7bc a656 f3f2 6ad2 765e 0a85 db4f b098  ...V..j.v^...O..
000000d0: fdbc ac06 3fb2 3378 4169 11e3 6854 f9e7  ....?.3xAi..hT..
000000e0: 5eef b369 1e3d 6305 f2cb c0f7 3a52 9edf  ^..i.=c.....:R..
000000f0: a6e6 81c4 8520 456b 773d 1493 f2ec 3139  ..... Ekw=....19
greg@MacBook-Air BUT2 %
```

Chez Alice :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ openssl pkeyutl -derive -inkey alice_privkey.pem -peerkey bob_pubkey.pem -out sharedkey.bin
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ xxd sharedkey.bin
00000000: 65c1 cd45 142f 2630 cd11 5b78 ee92 b6ab  e..E./&0..[x....
00000010: 8997 c20f 634d a3cf b5ca fb5a 1753 9d53  ....cM.....Z.S.S
00000020: a45c 6b0c 44e1 9730 970b f8b8 c8e5 b5dc  .\k.D..0........
00000030: 0384 cad8 692b f888 83a9 6bb2 0206 be5d  ....i+....k....]
00000040: 46d9 633d 305c ec4d 27d5 47e4 ce19 f904  F.c=0\.M'.G.....
00000050: f4cf 610d 4b3f 31a0 bf69 bdd8 e1af d704  ..a.K?1..i......
00000060: c69c 6695 b4b6 3524 028a c509 a6f6 2197  ..f...5$......!.
00000070: 3245 1363 d26c 6400 c66f 111b 2d87 6fd0  2E.c.ld..o..-.o.
00000080: 43c6 d872 6636 d492 7bdf 9fc7 fa3f 75ad  C..rf6..{....?u.
00000090: 7036 d63d 57c1 82ae 8f27 4dc5 a5d3 47d4  p6.=W....'M...G.
000000a0: 4277 bc9b fbe0 676f 8f05 0af0 2776 1134  Bw....go....'v.4
000000b0: 5920 6f94 a074 c2f9 99f9 e07b ef76 b2f3  Y o..t.....{.v..
000000c0: a7bc a656 f3f2 6ad2 765e 0a85 db4f b098  ...V..j.v^...O..
000000d0: fdbc ac06 3fb2 3378 4169 11e3 6854 f9e7  ....?.3xAi..hT..
000000e0: 5eef b369 1e3d 6305 f2cb c0f7 3a52 9edf  ^..i.=c.....:R..
000000f0: a6e6 81c4 8520 456b 773d 1493 f2ec 3139  ..... Ekw=....19
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```

## Q4)

Pour Bob :

Création du message à envoyer :

```
[greg@MacBook-Air BUT2 % nano plaintext_message.txt
[greg@MacBook-Air BUT2 % cat plaintext_message.txt
 Salut Florian
```

Conversion de la clé en Hexa :

```
[greg@MacBook-Air BUT2 % xxd sharedkey.bin hex_sharedkey
[greg@MacBook-Air BUT2 % cat hex_sharedkey
 00000000: 65c1 cd45 142f 2630 cd11 5b78 ee92 b6ab  e..E./&0..[x....
 00000010: 8997 c20f 634d a3cf b5ca fb5a 1753 9d53  ....cM.....Z.S.S
 00000020: a45c 6b0c 44e1 9730 970b f8b8 c8e5 b5dc  .\k.D..0........
 00000030: 0384 cad8 692b f888 83a9 6bb2 0206 be5d  ....i+....k....]
 00000040: 46d9 633d 305c ec4d 27d5 47e4 ce19 f904  F.c=0\.M'.G.....
 00000050: f4cf 610d 4b3f 31a0 bf69 bdd8 e1af d704  ..a.K?1..i......
 00000060: c69c 6695 b4b6 3524 028a c509 a6f6 2197  ..f...5$......!.
 00000070: 3245 1363 d26c 6400 c66f 111b 2d87 6fd0  2E.c.ld..o..-.o.
 00000080: 43c6 d872 6636 d492 7bdf 9fc7 fa3f 75ad  C..rf6..{....?u.
 00000090: 7036 d63d 57c1 82ae 8f27 4dc5 a5d3 47d4  p6.=W....'M...G.
 000000a0: 4277 bc9b fbe0 676f 8f05 0af0 2776 1134  Bw....go....'v.4
 000000b0: 5920 6f94 a074 c2f9 99f9 e07b ef76 b2f3  Y o..t.....{.v..
 000000c0: a7bc a656 f3f2 6ad2 765e 0a85 db4f b098  ...V..j.v^...O..
 000000d0: fdbc ac06 3fb2 3378 4169 11e3 6854 f9e7  ....?.3xAi..hT..
 000000e0: 5eef b369 1e3d 6305 f2cb c0f7 3a52 9edf  ^..i.=c.....:R..
 000000f0: a6e6 81c4 8520 456b 773d 1493 f2ec 3139  ..... Ekw=....19
```

Pour Alice :

Création du message à envoyer :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ nano plaintext_message.txt
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat plaintext_message.txt
Comment ca va le Greg ??
```

Conversion de la clé en Hexa :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ xxd sharedkey.bin sharedkeyHexa
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat sharedkeyHexa
00000000: 65c1 cd45 142f 2630 cd11 5b78 ee92 b6ab  e..E./&0..[x....
00000010: 8997 c20f 634d a3cf b5ca fb5a 1753 9d53  ....cM.....Z.S.S
00000020: a45c 6b0c 44e1 9730 970b f8b8 c8e5 b5dc  .\k.D..0........
00000030: 0384 cad8 692b f888 83a9 6bb2 0206 be5d  ....i+....k....]
00000040: 46d9 633d 305c ec4d 27d5 47e4 ce19 f904  F.c=0\.M'.G.....
00000050: f4cf 610d 4b3f 31a0 bf69 bdd8 e1af d704  ..a.K?1..i......
00000060: c69c 6695 b4b6 3524 028a c509 a6f6 2197  ..f...5$......!.
00000070: 3245 1363 d26c 6400 c66f 111b 2d87 6fd0  2E.c.ld..o..-.o.
00000080: 43c6 d872 6636 d492 7bdf 9fc7 fa3f 75ad  C..rf6..{....?u.
00000090: 7036 d63d 57c1 82ae 8f27 4dc5 a5d3 47d4  p6.=W....'M...G.
000000a0: 4277 bc9b fbe0 676f 8f05 0af0 2776 1134  Bw....go....'v.4
000000b0: 5920 6f94 a074 c2f9 99f9 e07b ef76 b2f3  Y o..t.....{.v..
000000c0: a7bc a656 f3f2 6ad2 765e 0a85 db4f b098  ...V..j.v^...O..
000000d0: fdbc ac06 3fb2 3378 4169 11e3 6854 f9e7  ....?.3xAi..hT..
000000e0: 5eef b369 1e3d 6305 f2cb c0f7 3a52 9edf  ^..i.=c.....:R..
000000f0: a6e6 81c4 8520 456b 773d 1493 f2ec 3139  ..... Ekw=....19
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```

Génération de l'IV Partagé :

```
[greg@MacBook-Air BUT2 % openssl rand -hex 16 > hex_IV
[greg@MacBook-Air BUT2 % cat hex_IV
 54e87e96bad060e0675c9979c6537a25
```

Conversion de la clef 2048 en 256

```
[greg@MacBook-Air BUT2 % MY_KEY=$(openssl dgst -sha256 sharedkey.bin | awk '{print $2}')
[greg@MacBook-Air BUT2 % echo $MY_KEY
 8f4f8852cfce1e194293bea9395a1d5a5b3ef9f6f63e63f79b0ffeef71fd6e3f
```

Chiffrage du message avec AES-256-CBC :

Bob :

```
[greg@MacBook-Air BUT2 % openssl enc -aes-256-cbc -in plaintext_message.txt -out encrypted_message.enc -K $MY_KEY -iv 54e87e96bad060e0675c9979c6537a25
[greg@MacBook-Air BUT2 % cat encrypted_message.enc
 ???B-????-
 G2%
```

Alice :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ openssl enc -aes-256-cbc -in plaintext_message.txt -out encrypted_message.enc -K $MY_KEY -iv 54
e87e96bad060e0675c9979c6537a25
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat encrypted_message.enc
◆◆z◆L~7\◆◆J◆J◆(◆|◆◆'◆◆◆sdF◆C)florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```

## Q5)

Déchiffrement du message fourni par Alice à Bob :

```
greg@MacBook-Air BUT2 % openssl enc -d -aes-256-cbc -in encrypted_message_alice.enc -out decrypted_message.txt -K $MY_KEY -iv 54e87e96bad060e0675c9979c6537a25
[greg@MacBook-Air BUT2 % cat decrypted_message.txt
 Comment ca va le Greg ??
 greg@MacBook-Air BUT2 %
```

Déchiffrement du message fourni par Bob à Alice :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ openssl enc -d -aes-256-cbc -in encrypted_message_bob.enc -out decrypted_message_bob.txt -K $MY
_KEY -iv 54e87e96bad060e0675c9979c6537a25
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat decrypted_message_bob.txt
Salut Florian
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```

## Q6)

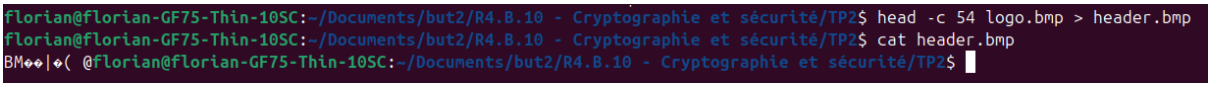
Un attaquant en MITM intercepte les clés publiques échangées entre Alice et Bob, crée ses propres clés et fait croire à chacun qu'il communique avec l'autre. Il peut ainsi lire, modifier et transmettre tous les messages sans être détecté.

Remède : authentifier les clés publiques via signatures numériques, certificats ou TLS.

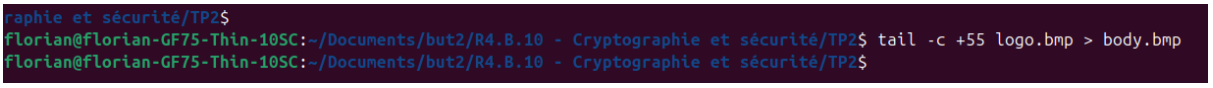
## Q7 :

Dans un fichier BMP, les premiers octets constituent l'en-tête (header) qui décrit l'image : taille, largeur, hauteur, profondeur de couleur, etc.
Si on chiffre tout le fichier, le logiciel d'affichage ne peut plus reconnaître le format BMP.
De plus, Un BMP classique possède **54 octets d'en-tête** puis les données de pixels

Pour ce faire :
On extrait l'entête dans un fichier header.bpm :

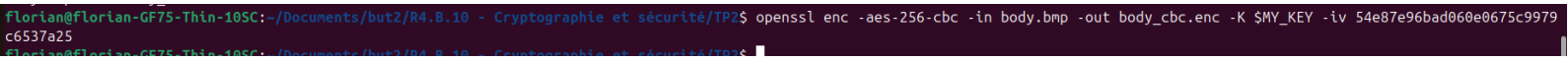



Puis le corps dans un autre fichier body.bpm :




On chiffre ensuite le corps avec le modèle voulu :
AES-256-ECB :

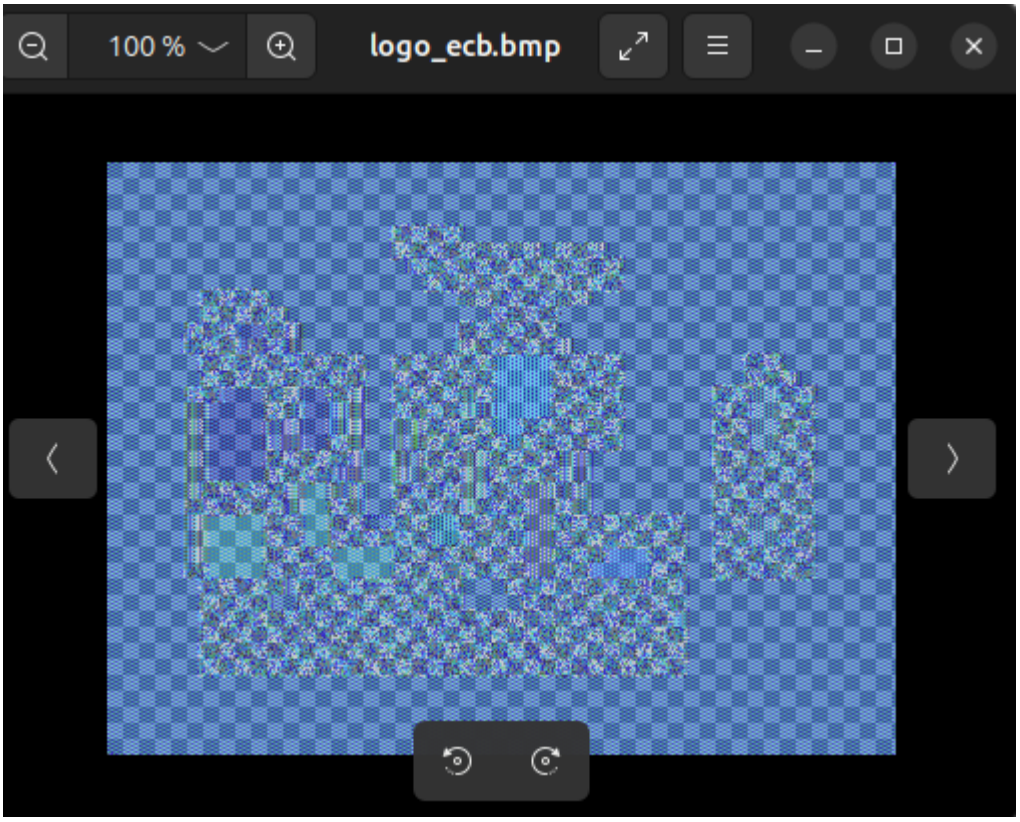

AES-256-CBC :



Nous pouvons ensuite recréer l'image en fusionnant le header avec le corp voulu :

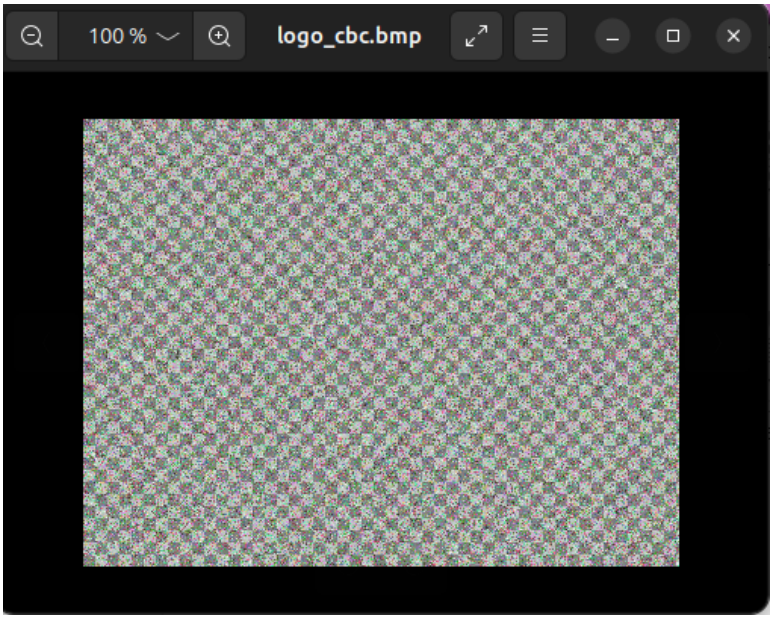
ECB :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat header.bmp body_ecb.enc > logo_ecb.bmp
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```




CBC :

```
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$ cat header.bmp body_cbc.enc > logo_cbc.bmp
florian@florian-GF75-Thin-10SC:~/Documents/but2/R4.B.10 - Cryptographie et sécurité/TP2$
```



Chiffrement RSA :

Lors de l'essai de chiffrement de l'image avec RSA, on constate que cela ne fonctionne pas pour l'ensemble du fichier. En effet, RSA ne permet de chiffrer que de petites quantités de données, limitées par la taille de la clé. Une image étant trop volumineuse, le chiffrement échoue. RSA n'est donc pas adapté au chiffrement direct de fichiers volumineux et est généralement utilisé pour chiffrer des clés symétriques (comme AES), qui servent ensuite à chiffrer les données.