Cryptage

- Prise en main (encodage base64)

a. openssl enc -base64 -e -in textin.txt -out textcod.txt
b. openssl enc -base64 -d -in textcod.txt -out textcout.txt
c. diff textin.txt textout.txt => retourne rien : fichiers identiques
d. Le codage en base64 sert a :
Ce n'est pas du chiffrement, c'est de l'encodage !

- Cryptage à clé secrète

a.

openssl enc -aes128 -P –nosalt enter aes-128-cbc encryption password: Verifying - enter aes-128-cbc encryption password: key=584F1DFF657074732F099F37039DD418 iv =BEED463C997AF521E671CC6017FE1964	Avec AES

openssl enc -bf -P -nosalt enter bf-cbc encryption password: Verifying - enter bf-cbc encryption password: key=584F1DFF657074732F099F37039DD418 iv =BEED463C997AF521	Avec Blowfich

openssl enc -des -P -nosalt enter des-cbc encryption password: Verifying - enter des-cbc encryption password: key=584F1DFF65707473 iv =2F099F37039DD418	Avec DES

openssl enc -des3 -P -nosalt enter des-ede3-cbc encryption password: Verifying - enter des-ede3-cbc encryption password: key=584F1DFF657074732F099F37039DD418BEED463C997AF521 iv =E671CC6017FE1964	Avec DES3

b. Pour un même algorythme, le vecteur d'initialisation est le même pour un même mot de passe.

c.

openssl enc -des –P enter des-cbc encryption password: Verifying - enter des-cbc encryption password: salt=33365ABB9DD16B2D key=641BD5A09B776340 iv =91AAD0563D048B09	Avec DES

openssl enc -des -P enter des-cbc encryption password: Verifying - enter des-cbc encryption password: salt=C2BADD034D29FD58 key=8B6D69F8B41E3D64 iv =7A05B69CD6EB3D87	Avec DES

d. Pour un même algorythme, quand le « salt » change, l'IV change lui aussi, pour un même mot de passe.
e. openssl enc -des -K 641BD5A09B776340 -iv 91AAD0563D048B09 -in toto.txt -out toto.a -e
f. openssl enc -des -K 641BD5A09B776340 -iv 91AAD0563D048B09 -in toto.a -out totod.txt -d

- Clés asymétriques

a. openssl genrsa -out fich.txt 2048
Generating RSA private key, 2048 bit long modulus . . .

Contenu de « fich.txt » :

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAuQdpgR36upf9I1i4NKxst3Eu3gmOnYaKqatqd9OAc85tgbay
6b5/osS+xnNuGq4xrRrSLR084MnNE4ZwPwR+P5ChbSW9X3i8d1Wk/jzLDQRdywST
MxkcOEewzIh/JpF6HJfhkLxIh5qBrOGynQrIgFioELnQv3kMCjAE0izhU379VzAW
am8VXqySinnj/TTYeU/GH0lQ/eQIrofFmqg4IBH4rxIsB3iY0xJvI3HsRcQAY49K
b6xgfaqHLuo+M4qECBH3/flanm7l9GGLrzkCWyxQI6B7VU49GLG4tPCdwvX4khjR
FDMD/vIvbHNZLujSaAh0PcajkQEAU62j3dsg7wIDAQABAoIBAFNocvgAcrFAqJ0R
dmBQReXfwLfY6RA7wTBBFIqVrjcGHDk4Cajy9h4mELXW/RBL7BrTl2E859+ROMAP
f3P464xt/0b7l0V9YMAOvITbFNF2YW2OT2jebek08A8TjPXu6HQRR15+cdenH8O2
LlU6si2hSYnYqbBWucWx5cp07tI7DWoawfoirg22MwbYvyc4Jnl1QQpgQQX6Bqpv
PmMj0HMC9uGrpaNiHLTJ8FvTy7JfXwl2vfxKQOzdt1++aJy2y0N5Rq8EREO04SJT
9kYh1bwbzCAz8njnsHboX3RxE8Gly/J4wTP8wMeVJQBkeDn8QawILT2T8Bj+06Jc
4oGrPtkCgYEA3a0eB7ec1FPDRGHdMhChK8dFI5GiEIjg1GsG/xtgI3AYhQFoel14
lY2yp2YSXKnOIWPqb1+t4s/vjT3Ri1+oFfm/egEf+1deISdsrUbzcTtFMddiAVbe
SR+OxI+QtMT+XD4yGRUKjtqBSf3Zwn9YGV7a4SFYdP8J+Q46JBwNILMCgYEA1a2o
D+4PduCAQfmLQG89IvRnLSrQX77gGp80hi4ELJRI+7XAcBWknCvz/+A042kELsOy
97ftHXUswj7lT12rIMALKGFb1/xnWqpxEFYOZ464G1w7IDjo23QrGslNBJop7NON
ibVvCexZ12O4i2QT0KEKEgaTKxrIwjwLdtOzZNUCgYEAl+4Pt/BTL38dRN/iD28w
V2Xi8AbfUX/OwCd+ixfDI2avl3Eonz0y6SVNvceKbDIBUgc95Qlpjxs+rsogtOph
tHYQktjoh30QzJ5NsNEBBqk9unRI+mwEO4/CdNuErTCauLPz+BbgvpnppMG0HsbS
pcjKMSR+kOk/d5AVryv+n1sCgYEAhD4ldTZwe7IVrr8yX35459k6wcltjNQk/lTp
vOFd0/kx8hZaMwQyDDVnnUS1dsjXvdmAOa+rIEAU02MpqCTgdDRms2cN4G5lyMcT
kniwEYdSihxau2Z9NtR+mOVctSx0Jg4H2uJfBlUwhQ1CeYJGgSgpg15uVo8NEKj4
r2H19MECgYAZsn2M1DYLQYQ6OhxWqS009+hpqr4IAnxNvGPAWDzB2V28jZEu6Vx4
+GxUe6SQ5nQuiWF29PXEGPJ35c3K0Mhk4q5/4uUOoQb7aUS2/IovLJCdgGS9kw0x
HT3tn3jimqwbF5Kf9XD+Rw/dWEOMpVTr4KDDqH3GUaV88iJzzBDg4A==
-----END RSA PRIVATE KEY-----
```

b. openssl genrsa -out fichdes.txt -des 2048
Generating RSA private key, 2048 bit long modulus
Enter pass phrase for fichdes.txt:
Verifying - Enter pass phrase for fichdes.txt:

Contenu du fichier « fichdes.txt » :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,6535D0D26E5E390C

SGp3nwYh4TuELLMw0CvFLqb8KEFsh+KiLdoARqqx9IGzfbg4MAgPbm+Qbd4xFNHP
w7Vq0MyRkITotpwiTdXV6IZhgGZsTPLX3YnKDGMptaW1I4xihPO7aiFNvt4iuXEF
E1iupGYPGM4bH90IFillsC6iTUdWrQlOvm8Psd/x4FNDq5uZWWOThVOFFkHWaqXl
grg3rIH4fqD491lHvFNe+5Zr6FBqXg5Mh5D4GllpSx3J62HG2bc5i+2fAOZ7pkX2
w1rlYSrY95x4nZTG3xBcoy4cOYxdYg/g1NzZW/YBLxxIPhRW+z4gtzRBHetdCvjV
```

```
yBSlNC1uBqhXELxW3b9RhYtC7ZvxrakbgO9dbCHLm6SNr2e9YLjYXK1jjJZ9gISF
DlmgW9o/Zsqq24M7hdoX7DBHDbyiSOVuN3wtiqHGhS0VZIk5PtDAFOxs0E8SnwMI
YX4gPfskko63nQAyxODD45CwmbJ+DUbjRS8KbgNsSNdtc12IPUix12UyLoHbevBo
mgqDM8PzfRFN6cX9Fr+pOvcmsxd8CxbiLD8dD5Lb5WkzPCf/aAoPXFnzeYhnnETB
Vbu1KFYke4GcRBIy5Alp2c5rHKL0uXyy3V7xfSFgEtTTXmYOxy2hvYWGHsZ48slb
JaMGDrGldvzq1FMp0cbCSYQKbJvq71VCyQyrvttNzUJSD2UFnnIod/Cp1Z+A93fl
1ZU4euAZXUoJarS4n2LGQoKS25KyDxeIot3cbEGRZPhjRHk77qc4OWafni8mo/Jg
frDM1OT0ZuD7mzyLPbVzzQ1yK9I32+QgwKguWgbqAHFwah42RXrJ2xp/lCBnYVsR
zUtXIVaA8TRs21qthVPnhk7KnfKZfHoCjXGbSFtjllv7+3fSYAdIfY60bfOMpDAo
Xr1jPDWYouTNLZEev1j5m74moDrztNBcfrLUMgH1FZ4EqL/b7i7i1lcOJFk/PYdo
FL4sA+42o8fP3eWetmO+6QgWVXV+vUt2TkVCtWPG5vVsFogxyq9wI5uZXcYBw+se
px1KfzpoMbAXmQY1epOyfauJwX0VBKLiOMxrPGvDS7gwjO9vEo/azHYtnSRcLuGU
9EfGHUBfvn5NIqHZ0Z7ZQgZMeYtn1mTS26ZDOp1quUX3IW/z7evHyUHIKCgp+zGC
H0JYbNdisXXT9TNM95cpXubqgHuGg3qrfxlLLY8dXd8mQP7F4jeArG21Jcm/dROh
TfakdIhvANA++f1tywXgZaHU7yKqTiK2lHK2Pwb4kpxvJYIyNaPOjct02PXC683x
FPVyNQHEzsLvXLNFEON17MTdSrDzGIoHHew7sAh5jLILPM3ZWUXlkUIGKTxYHZN1
svIYg7JUTEL7uxtYpUOtov0sMA6yp3+/oY6yYppAMf2Wfwu6xtH68b5X1h8PDdk8
SLczvvniufbpLIlAGuhx7Gq5jWED0IhmYunRPxfMHJ55ih8QFuAJbbLXboFcAQSD
UwQ3dIfJUS0zC7JlPKSbftqgWDpPPV3YfceZvWMoW8tAhsXrPuq6yOWlV+rBDszC
ciehCY2+uIla9Oop8OB8xiEKg9q0V+qyJGjP/dshDy8cicZ5Y/CN3g==
-----END RSA PRIVATE KEY-----
```

c. Le format ASN1 est un format de fichier texte, ou des blocs sont bornés par des "BEGIN" et des "END". Ces blocs contiennent une en-tête (type,info) ainsi que la clé. Ce type de fichier peut contenir plusieurs clés.

d. openssl rsa -in fichdes.txt -pubout -out clepub
Enter pass phrase for fichdes.txt:
writing RSA key

Contenu du fichier « clepub » :

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqYPEddlWd9YMrJT87y98
KdV5aGbCbr1F5yulA0VPB1GrVgEpkvH8ycEBtr9k+9q5ZtMnHTNjRZfqgXhksr8i
geRkONaM5JIla791qtcJptB49nizJjUeZ14qn2rn5dGeZ8C5HRgd/GeKSJmorg2j
A+htJ7XS4cWSJYFjOOoQ0zmSqSYKebXNqWg4yjDJmEAUw0/GKEO74DyQUid/ozm4
UHNHu00TbC44YWuSJewg9RF1mbG8maFn1MKUCG774DomlP9RWwJ1dDuFGDdGwg4c
TQiao65H7g1+kvsxTpZgFfXCzeCbN4zvqZ1P2XZb+TNEidjvjSrPV48TaAJLxzEY7wIDAQAB
-----END PUBLIC KEY-----
```

e. **Cryptage :**
openssl rsautl -in mess.txt -out chab.txt -pubin -inkey clepub –encrypt
Décryptage :
Essai avec clé publique : openssl rsautl -in chab.txt -out decchab.txt -inkey clepub –decrypt
unable to load Private Key
Essai avec clé privée : openssl rsautl -in chab.txt -out decchab.txt -inkey fichdes.txt -decrypt
Enter pass phrase for fichdes.txt:

- Message digest

a. "arbre"
$ openssl dgst emp.txt
MD5(emp.txt)= 8e6c32949d486c9770b16130011e2ad9

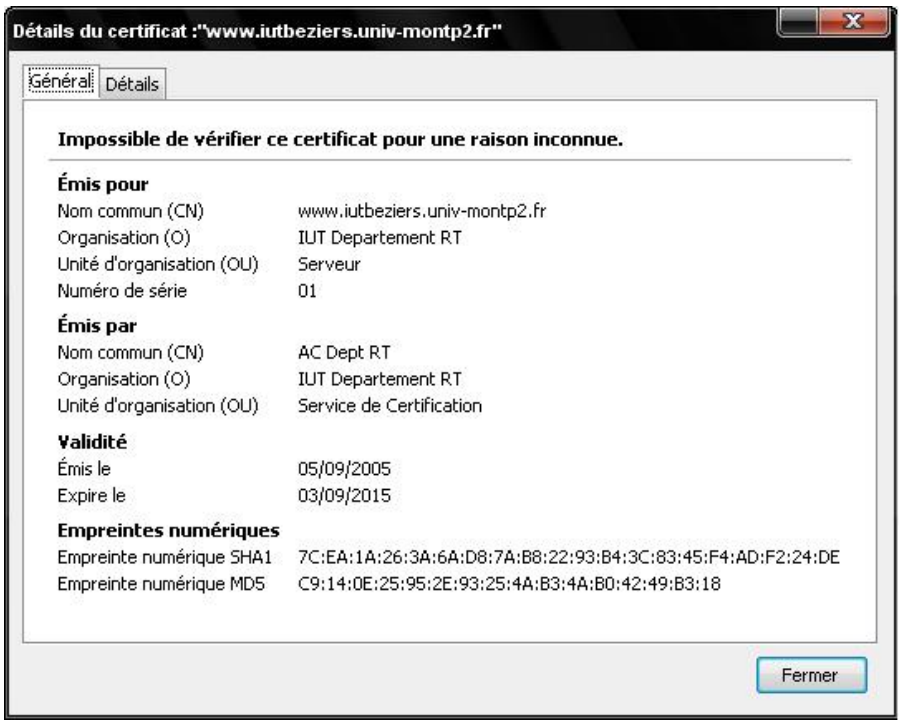
b. "brbre"
$ openssl dgst emp.txt

MD5(emp.txt)= d167b81468bda9b7e26837f57502390f
Conclusion : Pour un seul caractère de changé, l'empreinte est totalement modifiée

c. Les empreintes peuvent servir a vérifier si les fichiers système ont été modifiés.
On peut les stocker dans une partie du système d'exploitation
d. openssl dgst -md5 -out empreinte.txt -sign priv.txt fich.txt
e. openssl dgst -md5 -verify pub.txt -signature empreinte.txt fich.txt
f. Les empreintes signées permettent de savoir si les empreintes n'ont pas étés modifiées.
On peut les stocker sur une clé USB par exemple.

SSL : Exemple HTTPS

a. Certificat :



b. Champs : Les informations sur le propriétaire (nom, organisation, numéro), des informations sur l'autorité de certification (nom, organisation, unité), la validité, et les empreintes (SHA1 et MD5) C'est l'autorité de certification qui « authentifie » les données. Cette AC a pour charge de vérifier que les informations contenues dans le certificat sont vraies.

c. Certificat du AC :