td1

1

1.1

```
md5 : `md5sum Downloads/annexe.txt` -> bc7ffb91df2177eabd4c781143af470b
sha1 : `sha1sum Downloads/annexe.txt` -> fd92ded1a403fec3cf94beb534a32f30c3d535ba
sha256 : `sha256sum Downloads/annexe.txt` ->
7b95e677872a1f8ba2c6b2ecb1e260ebfdcf16cb0b5bc76ecf9904d65a357f9
```

1.2

- MD5: 128 bits
- SHA-1: 160 bits
- SHA-256: 256 bits

1.3

`md5sum Downloads/annexe.txt > Cours/3A/protoCrypto/td1/digest`

1.4

```
~> md5sum -c Cours/3A/protoCrypto/td1/digest
Downloads/annexe.txt: OK
```

1.5

```
~> nvim Downloads/annexe.txt && md5sum Downloads/annexe.txt
#added a space at the end of the file
b0ab088403adb2191286242c001f10bd  Downloads/annexe.txt
```

1.6

On voit qu'une legere difference entraine un hash tres different.

2

2.1

```
~> gpg --gen-key
~> gpg --list-keys
pub   rsa3072 2023-11-15 [SC] [expires: 2025-11-14]
      962AC8C9FABC31FA07B72970B44B92170F4DC6E7
uid           [ultimate] maxime <max.soulie01@laposte.net>
sub   rsa3072 2023-11-15 [E] [expires: 2025-11-14]
```

2.2

```
~> gpg --export -a 962AC8C9FABC31FA07B72970B44B92170F4DC6E7 > public_key_A.asc

~> gpg --export-secret-keys -a 962AC8C9FABC31FA07B72970B44B92170F4DC6E7 >
private_key_A.asc
```

2.4

```
gpg --import Downloads/publickey.asc
```

2.5

```
~> gpg --encrypt --recipient 2C77BD2799AD3CBAE70D19124B904863C38F0D08 --output
annexe.txt Downloads/annexe.txt
```

2.6

```
~> gpg --decrypt Downloads/annexe\(1\).txt > annexe\(1\)_decrypt.txt
gpg: encrypted with 3072-bit RSA key, ID 9EF57D69D3288486, created 2023-11-15
      "maxime <max.soulie01@laposte.net>"
```

annexe(1).txt :

```
Ergo ego senator inimicus, si ita vultis, homini, amicus esse, sicut semper fui,
rei publicae debeo. Quid? si ipsas inimicitias, depono rei publicae causa, quis
me tandem iure reprehendet, praesertim cum ego omnium meorum consiliorum atque
factorum exempla semper ex summorum hominum consiliis atque factis mihi censuerim
petenda.

Utque proeliorum periti rectores primo catervas densas opponunt et fortes, deinde
leves armaturas, post iaculatores ultimasque subsidiales acies, si fors adegerit,
iuvaturas, ita praepositis urbanae familiae suspensae digerentibus sollicite,
quos insignes faciunt virgae dexteris aptatae velut tessera data castrensi iuxta
vehiculi frontem omne textrinum incedit: huic atratum coquinae iungitur
```

ministerium, dein totum promiscue servitium cum otiosis plebeiis de vicinitate coniunctis: postrema multitudo spadonum a senibus in pueros desinens, obluridi distortaque lineamentorum conpage deformes, ut quaqua incesserit quisquam cernens mutilorum hominum agmina detestetur memoriam Samiramidis reginae illius veteris, quae teneros mares castravit omnium prima velut vim iniectans naturae, eandemque ab instituto cursu retorquens, quae inter ipsa oriundi crepundia per primigenios seminis fontes tacita quodam modo lege vias propagandae posteritatis ostendit.

Ex his quidam aeternitati se commendari posse per statuas aestimantes eas ardenter adfectant quasi plus praemii de figmentis aereis sensu carentibus adepturi, quam ex conscientia honeste recteque factorum, easque auro curant inbracteari, quod Acilio Glabrioni delatum est primo, cum consiliis armisque regem superasset Antiochum. quam autem sit pulchrum exigua haec spernentem et minima ad ascensus verae gloriae tendere longos et arduos, ut memorat vates Ascraeus, Censorius Cato monstravit. qui interrogatus quam ob rem inter multos... statuam non haberet malo inquit ambigere bonos quam ob rem id non meruerim, quam quod est gravius cur inpetraverim mussitare.

Inter has ruinarum varietates a Nisibi quam tuebatur accitus Vrsicinus, cui nos obsecuturos iunxerat imperiale praeceptum, dispicere litis exitialis certamina cogebatur abnuens et reclamans, adulatorum oblatrantibus turmis, bellicosus sane milesque semper et militum ductor sed forensibus iurgiis longe discretus, qui metu sui discriminis anxius cum accusatores quaesitoresque subditivos sibi consociatos ex isdem foveis cerneret emergentes, quae clam palamve agitabantur, occultis Constantium litteris edocebat inplorans subsidia, quorum metu tumor notissimus Caesaris exhalaret.

2.7

```
~> gpg --sign --output annexe.txt Downloads/annexe.txt
```

2.8

```
~> gpg --verify Downloads/annxeu.txt
gpg: Signature made Wed 15 Nov 2023 11:43:23 AM CET
gpg:                using RSA key 2C77BD2799AD3CBAE70D19124B904863C38F0D08
gpg: Good signature from "Cerzen <alan191100@gmail.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 2C77 BD27 99AD 3CBA E70D  1912 4B90 4863 C38F 0D08
```

2.9

```
~> gpg --clearsign --output annexe_signed.txt Downloads/annexe.txt
gpg --verify annexe_signed.txt
gpg: Signature made Wed 15 Nov 2023 11:47:07 AM CET
gpg:                using RSA key 962AC8C9FABC31FA07B72970B44B92170F4DC6E7
gpg: Good signature from "maxime <max.soulie01@laposte.net>" [ultimate]
```

3

3.1

```
~> openssl genpkey -algorithm RSA -out
Cours/3A/protoCrypto/td1/keys/private_key.pem -aes256
```

3.2

```
 ~> openssl rsa -pubout -in Cours/3A/protoCrypto/td1/keys/private_key.pem -out
Cours/3A/protoCrypto/td1/keys/public_key.pem
```

Maxime Soulié