Pierre-Yves
VASSARD
BTS SIO1

Compte rendue TP2

Pierre-Yves
VASSARD
BTS SIO1

Table des matières

Pierre-Yves
VASSARD
BTS SIO1

Empreinte MD5 :

```
administrateur@Debian-12-Bookworm:~/Documents/BLOC$ md5sum fichier1
94baaad4d1347ec6e15ae35c88ee8bc8  fichier1
administrateur@Debian-12-Bookworm:~/Documents/BLOC$ md5sum fichier2
94baaad4d1347ec6e15ae35c88ee8bc8  fichier2
```

4 :

5 : Les résumé des deux fichiers sont les mêmes car **bonjour** est écris dans les deux fichiers.

```
administrateur@Debian-12-Bookworm:~/Documents/BLOC$ md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
```

6 :

Oui cela correspond à mes attentes car en rajoutant un 1, à b**onjour**, cela modifie son résumé.

8 : Je peut conclure que la commande **echo**, par défaut, créer un saut de ligne par conséquent, son résumé est différent.

```
administrateur@Debian-12-Bookworm:~/Documents/BLOC1$ echo -n bonjour | md5sum
f02368945726d5fc2a14eb576f7276c0  -
```

9 :

Le paramètre -n sur la commande **echo** permet de ne pas afficher le saut de ligne, on peut le savoir en exécutant la commande **man echo** qui nous explique ce paramètre :

```
-n     Ne pas effectuer le saut de ligne final
```

Empreinte SHA1

15 :

```
administrateur@Debian-12-Bookworm:~/Documents/BLOC1$ sha1sum fichier4
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier4
administrateur@Debian-12-Bookworm:~/Documents/BLOC1$ sha1sum fichier5
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier5
```

Avec sha1sum, les résumé des deux fichiers sont les mêmes.

Pierre-Yves
VASSARD
BTS SIO1

16 :

```
administrateur@Debian-12-Bookworm:~/Documents/BLOC1$ sha1sum fichier6
c83904636c6d95cd84e2e298e1d7298e966aed98  fichier6
```

Les résumé sont différent suite à l'ajout d'un nouveau caractère à **bonjour**.

17 :

```
PY@Debian-12-Bookworm:~/Documents/tp2$ sum fichier3
55386     1 fichier3
PY@Debian-12-Bookworm:~/Documents/tp2$ md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
PY@Debian-12-Bookworm:~/Documents/tp2$ shalsum fichier3
bash: shalsum : commande introuvable
PY@Debian-12-Bookworm:~/Documents/tp2$ sha512sum fichier3
b137e593a9bc3632f2d963dd1105e5ccf072b119aaab2b7e7e04e6cd2e806031d8f820d207bb7420916a106f1b427508b5d2be605bc723706ea367e9d8c7e7
80  fichier3
PY@Debian-12-Bookworm:~/Documents/tp2$
```

J'en conclue que les protocole de chiffrage utilisé sont de plus en plus compliqué car plus de caractères dans leurs résumé.

20 :

```
PY@Debian-12-Bookworm:~/Documents/TP2$ sha1sum mdp1 mdp2 mdp3
af736132123d959e8755f478233a5ae65982f2b8  mdp1
c1ddc974efb085dde2b723ab6e8e120fb9fde195  mdp2
9be0cd43ebd63a50e0dddf165b7ad31423491f77  mdp3
PY@Debian-12-Bookworm:~/Documents/TP2$
```

L'algorithme de hachage utilisé est le sha1.