Mohamed
HAFAIDH

BTS SIO-1
TP - Cryptographiques

2 - Calculez le résumé MD5 de “fichier1” par la commande “md5sum”. Calculez le résumé MD5 de “fichier2”

```
root@yooceyy-GS60-6QC:~# md5sum fichier1
94baaad4d1347ec6e15ae35c88ee8bc8  fichier1

root@yooceyy-GS60-6QC:~# md5sum fichier2
94baaad4d1347ec6e15ae35c88ee8bc8  fichier2
```

Comparez le résumé de fichier1 et le résumé de fichier2. Qu'en concluez-vous ?

Je conclue que les deux valeurs du **fichier1** et **fichier2** sont identiques.

Le résultat de la commande md5sum est-il conforme à vos attentes ?

Non car nous avons changé la valeur du contenu le **bonjour1** c’est pour cela que la valeur **md5sum** est différente.

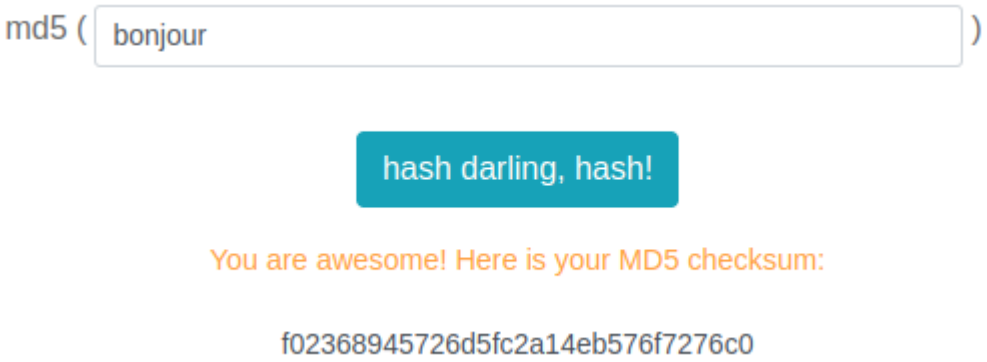
```
root@yooceyy-GS60-6QC:~# echo bonjour1 > fichier3
root@yooceyy-GS60-6QC:~# md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
```

Quelques subtilités…

7 - Passez la commande :

```
root@yooceyy-GS60-6QC:~# echo bonjour | md5sum
94baaad4d1347ec6e15ae35c88ee8bc8  -
root@yooceyy-GS60-6QC:~#
```

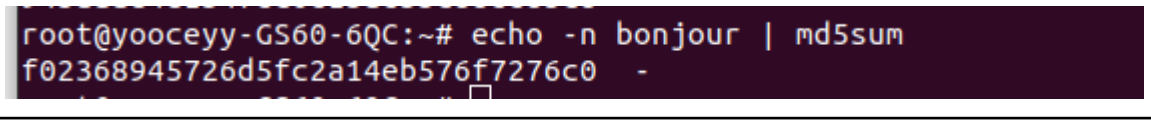
8 - Vérifiez le calcul en utilisant le calculateur MD5 on line infra :



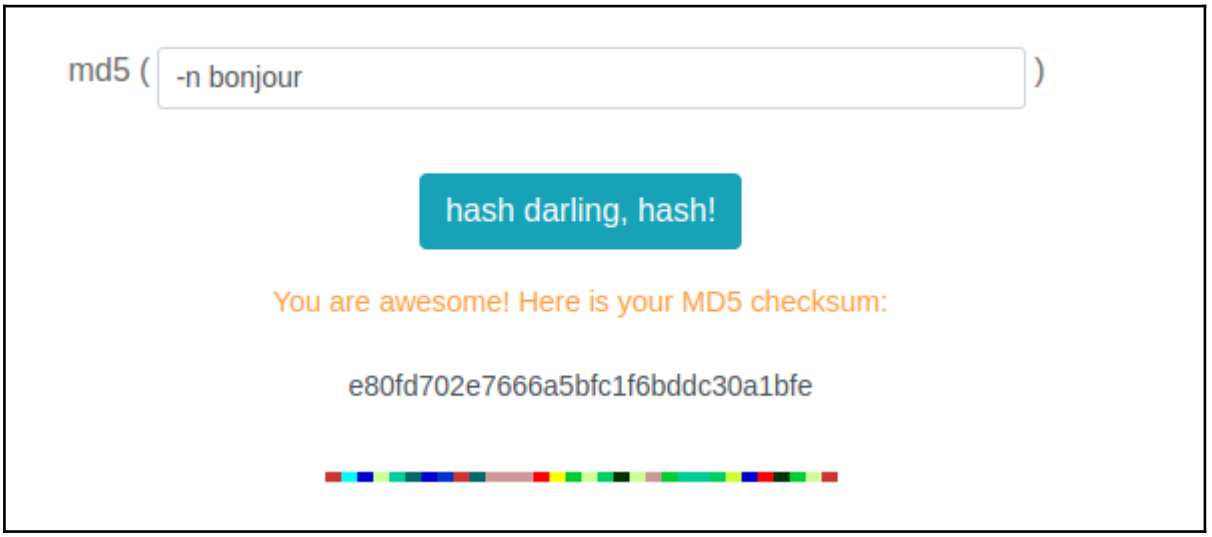
Que concluez-vous ?

La commande echo sur le terminal de linux nous affiche le bonjour sur le nano avec un espace puis un retour à la ligne, tandis que le calculateur MD5 nous affiche le bonjour sans espace ni retour à la ligne. c'est pour cela y'a une grosse différence.

9 - Passez la commande :



10 - Vérifiez le calcul en utilisant le calculateur MD5 on line infra :



Que concluez-vous ? A quoi sert le paramètre “-n” ?

-n affiche le premier nombre personnalisé de lignes. Par exemple, entrez head -n 5 nomfichier.txt pour afficher les cinq premières lignes de nomfichier.txt.

Empreinte SHA1 :

11 - Passez la commande suivante :

12 - Calculez le résumé SHA1 de “fichier4” par la commande “sha1sum”.

```
root@yooceyy-GS60-6QC:~# echo bonjour > fichier4
root@yooceyy-GS60-6QC:~# sha1sum fichier4
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier4
```

13 - Passez la commande suivante :

14 - Calculez le résumé SHA1 de “fichier5”

```
root@yooceyy-GS60-6QC:~# echo bonjour > fichier5
root@yooceyy-GS60-6QC:~# sha1sum fichier5
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier5
```

15 - Comparez le résumé de fichier1 et le résumé de fichier2. Qu'en concluez-vous ?

Points communs:

Les deux fichiers ont les mêmes droits d'accès : -rw-r--r--.
Ils appartiennent tous deux au même utilisateur et au même groupe : root.
Ils ont la même taille : 8 octets.
Ils ont été modifiés le même jour : 30 janvier.
Ils ont été modifiés à la même heure : 09:23.
Différences:

Le fichier1 a été créé avant le fichier2.

Le nom du fichier1 est différent de celui du fichier2.

Conclusion:

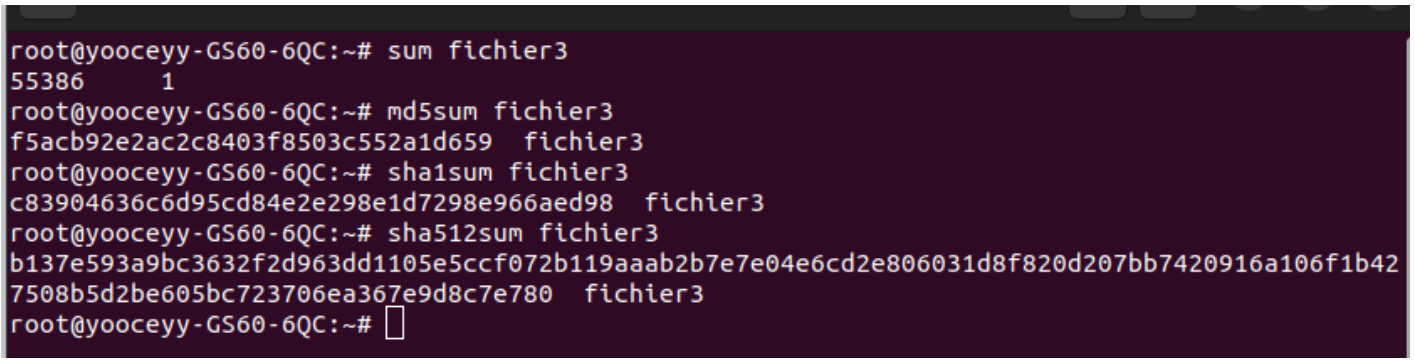
Les fichiers fichier1 et fichier2 sont très similaires. Ils ont la même taille, les mêmes droits d'accès, et ont été modifiés par le même utilisateur au même moment. La seule différence est leur nom et le fait que fichier1 a été créé avant fichier2.

16 - Passez les commandes suivantes :
Le résultat de la commande sha1sum est-il conforme à vos attentes ?

```
root@yooceyy-GS60-6QC:~# echo bonjour1 > fichier6
root@yooceyy-GS60-6QC:~# sha1sum fichier6
c83904636c6d95cd84e2e298e1d7298e966aed98  fichier6
```

Comparez les résumés de "sum", "md5sum", "sha1" et "sh512sum"

17 - Passez successivement les commandes infra :



Valeurs de hachage:

Les commandes md5sum, sha1sum et sha512sum fournissent différents hachages cryptographiques du contenu du fichier. Ces hachages représentent une "empreinte digitale" unique du fichier et peuvent être utilisés pour vérifier son intégrité ou le comparer à d'autres fichiers.
Considérations de sécurité:

MD5: Il est important de noter que MD5 est considéré comme une fonction de hachage cryptographiquement peu sûre en raison de la possibilité de collisions (deux fichiers différents générant le même hachage). Bien qu'il puisse encore être utilisé pour des applications non critiques, évitez de l'utiliser à des fins sensibles à la sécurité.

SHA-1: Bien que SHA-1 soit plus robuste que MD5, il a également montré qu'il était vulnérable à certaines attaques. Pour de meilleures pratiques de sécurité, il est recommandé d'utiliser des fonctions de hachage plus puissantes comme SHA-256 et SHA-512 pour les données sensibles.

Comparaison avec fichier1 et fichier2:

Sans connaître les hachages de fichier1 et fichier2, nous ne pouvons pas les comparer directement avec fichier3.

Vous allez télécharger l'utilitaire Linux “fdisk” (peu importe la version ici...).

```
root@yooceyy-GS60-6QC:~# sudo apt install fdisk
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  nvidia-firmware-535-535.86.05
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les paquets suivants seront mis à jour :
  fdisk
1 mis à jour, 0 nouvellement installés, 0 à enlever et 72 non mis à jour.
Il est nécessaire de prendre 122 ko dans les archives.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy-proposed/main amd64 fdisk amd64 2.
37.2-4ubuntu3.2 [122 kB]
122 ko réceptionnés en 1s (106 ko/s)
(Lecture de la base de données... 210833 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../fdisk_2.37.2-4ubuntu3.2_amd64.deb ...
Dépaquetage de fdisk (2.37.2-4ubuntu3.2) sur (2.37.2-4ubuntu3) ...
Paramétrage de fdisk (2.37.2-4ubuntu3.2) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
root@yooceyy-GS60-6QC:~#
```

18 - Télécharger maintenant l'empreinte “sha1” correspondant au fichier téléchargé précédemment.

19 - Vérifiez que le logiciel téléchargé est bien conforme à l'original !

```
root@yooceyy-GS60-6QC:/home/yooceyy/Bureau# sha1sum fdisk-0.9.1.tar.gz
26d626f4a4913a0ca7603c707539028b4a97f874  fdisk-0.9.1.tar.gz
root@yooceyy-GS60-6QC:/home/yooceyy/Bureau# cat fdisk-0.9.1.tar.gz.sha1
cat: fdisk-0.9.1.tar.gz.sha1: Aucun fichier ou dossier de ce type
root@yooceyy-GS60-6QC:/home/yooceyy/Bureau# cat fdisk-0.9.1.tar.gz.sha1
26d626f4a4913a0ca7603c707539028b4a97f874  fdisk-0.9.1.tar.gz
root@yooceyy-GS60-6QC:/home/yooceyy/Bureau#
```

Petit exercice sympa !

Le hachage de melchope avec SHA-512 correspond exactement au condensé donné. Cela confirme que le hachage utilisé est SHA-512.

Conclusion :
Le mot de passe melchope correspond au condensé effd456daab1ca177fdc0580a63eb4108cdf9335cfe70ddd2e73d399b46a70d3.
Le hachage utilisé est SHA-512.