Tamda Zohir
BTS Services Informatiques aux Organisations
Bloc 1 - Mise à disposition des services informatiques

Le 30 janvier 2024

# Empreintes cryptographiques

# Sommaire

# Manipulations de la MD5

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour > fichier1
administrateur@debian:~/Bureau/TP TZ$ md5sum fichier1
94baaad4d1347ec6e15ae35c88ee8bc8 fichier1
```

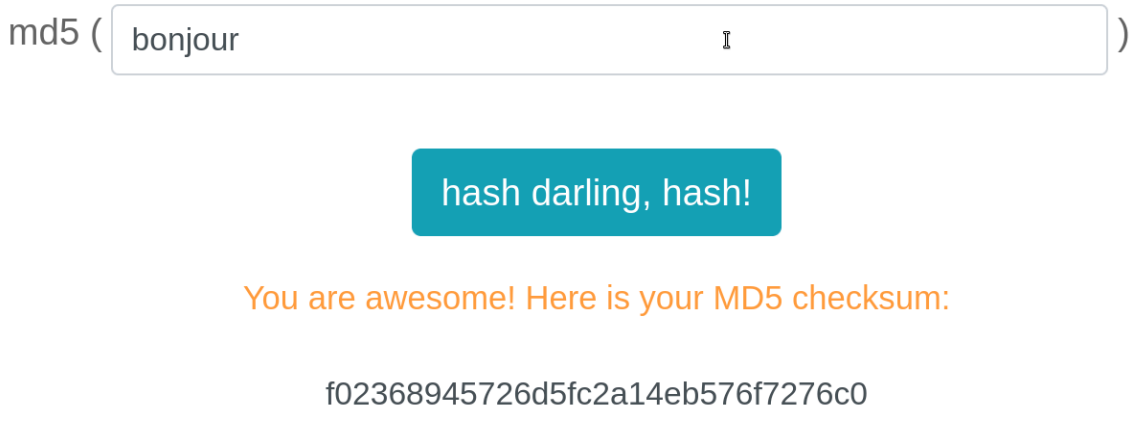
```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour > fichier2
administrateur@debian:~/Bureau/TP TZ$ md5sum fichier2
94baaad4d1347ec6e15ae35c88ee8bc8 fichier2
```

On constate que les résultats des empreintes MD5 sont identiques car on a écrit “bonjour” à la fois dans le fichier1 et dans le fichier2.

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour1 > fichier3
administrateur@debian:~/Bureau/TP TZ$ md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
```

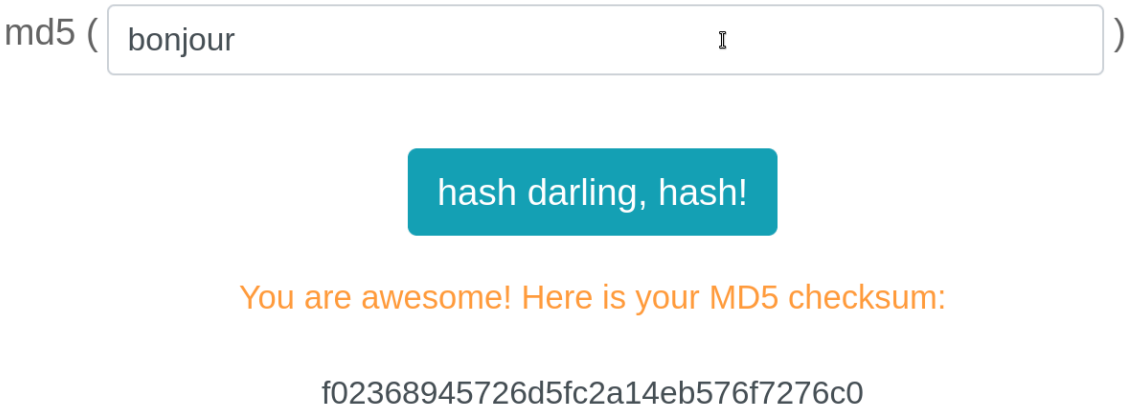
En revanche, si on met “bonjour1” au lieu de “bonjour”, les résultats des empreintes MD5 pour “fichier2” et “fichier3” ne sont plus les mêmes.

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour | md5sum
94baaad4d1347ec6e15ae35c88ee8bc8  -
```




On peut en conclure que les résultats des empreintes MD5 dans le terminal et sur le site http://www.md5.cz/ ne sont pas identiques.

```
administrateur@debian:~/Bureau/TP TZ$ echo -n bonjour | md5sum
f02368945726d5fc2a14eb576f7276c0 -
```




La commande echo a un paramètre appelé -n: elle permet de supprimer un caractère spécial servant d'aller à la ligne.
En revanche, on constate que ces résultats sont identiques. On se rend compte que la commande echo met par défaut un caractère spécial permettant d'aller à la ligne. Or, le fait de l'ajouter change le résultat de l'empreinte MD5.

# Manipulations de la SHA1

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour > fichier4
administrateur@debian:~/Bureau/TP TZ$ sha1sum fichier4
e7bc546316d2d0ec13a2d3117b13468f5e939f95 fichier
```

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour > fichier5
administrateur@debian:~/Bureau/TP TZ$ sha1sum fichier5
e7bc546316d2d0ec13a2d3117b13468f5e939f95 fichier5
```

Après avoir écrit “bonjour” à la fois dans le fichier4 et dans le fichier5. On constate que les résultats des empreintes SHA1 sont identiques.

```
administrateur@debian:~/Bureau/TP TZ$ echo bonjour1 > fichier6
administrateur@debian:~/Bureau/TP TZ$ sha1sum fichier6
c83904636c6d95cd84e2e298e1d7298e966aed98 fichier6
```

En revanche, en comparant les résultats des empreintes SHA1 à la fois dans le fichier5 et dans le fichier6, on remarque qu’ils ne sont plus identiques.

```
administrateur@debian:~/Bureau/TP TZ$ sum fichier3
55386 1 fichier3

administrateur@debian:~/Bureau/TP TZ$ md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659 fichier3

administrateur@debian:~/Bureau/TP TZ$ sha1sum fichier3
c83904636c6d95cd84e2e298e1d7298e966aed98 fichier3

administrateur@debian:~/Bureau/TP TZ$ sha512sum fichier3
b137e593a9bc3632f2d963dd1105e5ccf072b119aaab2b7e7e04e6cd2e806031d
8f820d207bb7420916a106f1b427508b5d2be605bc723706ea367e9d8c7e780
fichier3
```

On constate que les résultats de différentes empreintes cryptographiques n’ont pas la même longueur.

# Vérifier l’intégrité d’un logiciel

```
# Convertir le nom du dossier compressé en SHA1
administrateur@debian:~/Bureau$ sha1sum gnufdisk-2.0.0a1.tar.gz
8921ee9e88c2954376ff1e221fb1d48583ad847a gnufdisk-2.0.0a1.tar.gz

# Lire le fichier contenant l’empreinte SHA1
administrateur@debian:~/Bureau$ cat gnufdisk-2.0.0a1.tar.gz.sha1
8921ee9e88c2954376ff1e221fb1d48583ad847a gnufdisk-2.0.0a1.tar.gz
```

Le logiciel qui est téléchargé est bien conforme à l’original car les empreintes SHA 1 sont identiques.

# Trouver le mot de passe

La méthode adéquate pour trouver le mot de passe est de déterminer le nombre de caractères contenus dans chaque empreinte cryptographique.

| *Types d'empreintes* | *Taille de caractères* |
|---|---|
| SUM | 5 |
| MD5 | 32 |
| SHA1 | 40 |
| SHA256 | 64 |
| SHA512 | 128 |

```
administrateur@debian:~/Bureau/TP TZ/petit_exercice$ echo -n
effd456daab1ca177fdc0580a63eb4108cdf9335cfe70ddd2e73d399b46a70d3 > mot_de_passe
administrateur@debian:~/Bureau/TP TZ/petit_exercice$ wc -m mot_de_passe
64 mot_de_passe
```

Le terminal indique qu'il y a 64 caractères pour ce mot de passe hashé, ce qui signifie qu'il s'agit d'une empreinte de type SHA256.

Après cela, on peut la comparer avec les différents mots de passe.

```
administrateur@debian:~/Bureau/TP TZ/petit_exercice$ echo -n charlyshop | sha256sum
2ab7a80ba7a04910055a7c58113d2d9c3f7fa76b2197ab29a7e2b084b10a550e -

administrateur@debian:~/Bureau/TP TZ/petit_exercice$ echo -n sandydeluz | sha256sum
effd456daab1ca177fdc0580a63eb4108cdf9335cfe70ddd2e73d399b46a70d3 -

administrateur@debian:~/Bureau/TP TZ/petit_exercice$ echo -n melchope | sha256sum
2586fedb229fc65d3dd6d3b523134e74cbbf88e992d466495c0cfd75f1a43c21 -
```

On voit que le mot de passe qui a été haché est identique par rapport à ce qu'on a eu, donc le mot de passe est "sandydeluz".

# Webographie


- https://www.cyberciti.biz/faq/check-sha1-hash-cheksum-on-linux-freebsd-and-unix/

# Conclusion

Pour en conclure, l’empreinte cryptographique est souvent utilisée pour vérifier l’intégrité du fichier, ce qui permet de vérifier si ce dernier est vulnérable ou pas.