Nilda BALDA ***SIO 1***	Bloc 1	TP 2 **Les empreintes cryptographiques MD5/SHA1** 2023 - 2024 Semestre 2

Compte-rendu

Sommaire

I. Introducti:on :

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en s'aidant souvent de secrets ou clés. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message supposément inintelligible à autre que qui de droit.

II. Empreinte MD5

a. Manipulations basiques

Q1 - Passez la commande suivante :

La commande permet d'afficher le texte.

Q2 - Calculez le résumé MD5 de "fichier1" par la commande "md5sum".

```
administrateur@Debian-12-Bookworm:~$ su
Mot de passe :
root@Debian-12-Bookworm:/home/administrateur# echo bonjour > fichier1
root@Debian-12-Bookworm:/home/administrateur# md5sum
md5sum fichier1
^C
root@Debian-12-Bookworm:/home/administrateur# md5sum fichier1
94baaad4d1347ec6e15ae35c88ee8bc8  fichier1
```

Q3 - Passez la commande suivante :

Q4 - Calculez le résumé MD5 de "fichier2"

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour > fichier2
root@Debian-12-Bookworm:/home/administrateur# md5sum fichier2
94baaad4d1347ec6e15ae35c88ee8bc8  fichier2
```

Q5 - Comparez le résumé de fichier1 et le résumé de fichier2. Qu'en concluez-vous ?

Les fichiers 1 et 2 ont le même message crypté, les mêmes caractères.

Q6 - Passez les commandes suivantes :

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour1 > fichier3
root@Debian-12-Bookworm:/home/administrateur# md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
```

Le résultat de la commande md5sum est-il conforme à vos attentes ? Le message crypté du fichier 3 est différent du fichier 1 et 2.

b. Quelques subtilités…

Q7 - Passez la commande :

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour | md5sum
94baaad4d1347ec6e15ae35c88ee8bc8  -
```

Q8 - Vérifiez le calcul en utilisant le calculateur MD5 on line infra :
Sur internet je trouve : d138d6809fc793d4376da08b20f8e97c
Le calcul trouvé dans la commande du VM (Linux) est différent du calcul trouvé sur internet.

Q9 - Passez la commande :

```
root@Debian-12-Bookworm:/home/administrateur# echo -n bonjour | md5sum
f02368945726d5fc2a14eb576f7276c0  -
```

Q10 - Vérifiez le calcul en utilisant le calculateur MD5 on line infra :
Le calcul trouvé sur internet est : ccf435bf06f991858d29486b40fe6748
Le début commence par des lettres.

III. Empreinte SHA1

Q11 - Passez la commande suivante :

Q12 - Calculez le résumé SHA1 de “fichier4” par la commande “sha1sum”.

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour > fichier4
root@Debian-12-Bookworm:/home/administrateur# sha1sum fichier4
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier4
```

Q13 - Passez la commande suivante :
Q14 - Calculez le résumé SHA1 de “fichier 5”

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour > fichier5
root@Debian-12-Bookworm:/home/administrateur# sha1sum fichier5
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier5
```

Q15 - Comparez le résumé de fichier1 et le résumé de fichier2. Qu'en concluez-vous ?

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.
Le fichier1 a été créé avant le fichier2.
Le nom du fichier 1 est différent de celui du fichier 2.

Q16 - Passez les commandes suivantes :

```
root@Debian-12-Bookworm:/home/administrateur# echo bonjour1 > fichier6
root@Debian-12-Bookworm:/home/administrateur# sha1sum fichier6
c83904636c6d95cd84e2e298e1d7298e966aed98  fichier6
```

Le résultat de la commande sha1sum est-il conforme à vos attentes ? Oui le résultat est conforme.

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

17 - Passez successivement mes commandes infra :
Les commande permets d'afficher les messages cryptés du fichier3.

```
root@Debian-12-Bookworm:/home/administrateur# sum fichier3
55386     1 fichier3
root@Debian-12-Bookworm:/home/administrateur# md5sum fichier3
f5acb92e2ac2c8403f8503c552a1d659  fichier3
root@Debian-12-Bookworm:/home/administrateur# sha1sum fichier3
c83904636c6d95cd84e2e298e1d7298e966aed98  fichier3
root@Debian-12-Bookworm:/home/administrateur# sha512sum fichier3
b137e593a9bc3632f2d963dd1105e5ccf072b119aaab2b7e7e04e6cd2e806031d8f820d20
7bb7420916a106f1b427508b5d2be605bc723706ea367e9d8c7e780  fichier3
```

Qu'en concluez-vous ? Après avoir passé les différentes commandes, les caractères des messages cryptés sont tous différents et à la fin du message il y a le "fichier 3".

V. Vérifier l'intégrité d'un logiciel téléchargé

Q18 - Télécharger maintenant l'empreinte "sha1" correspondant au fichier téléchargé précédemment.

Q19 - Vérifiez que le logiciel téléchargé est bien conforme à l'original !