

TP Cyber sécurité : Hachage

SIO 1 – BLOC 3 – Cybersécurité – Thème 2 – Préserver l'identité numérique de l'organisation

Outils nécessaires au TP : Notepad++, 7-zip, Frhed.

Lien à faire obligatoires :

Hachage : Faire tous les chapitres

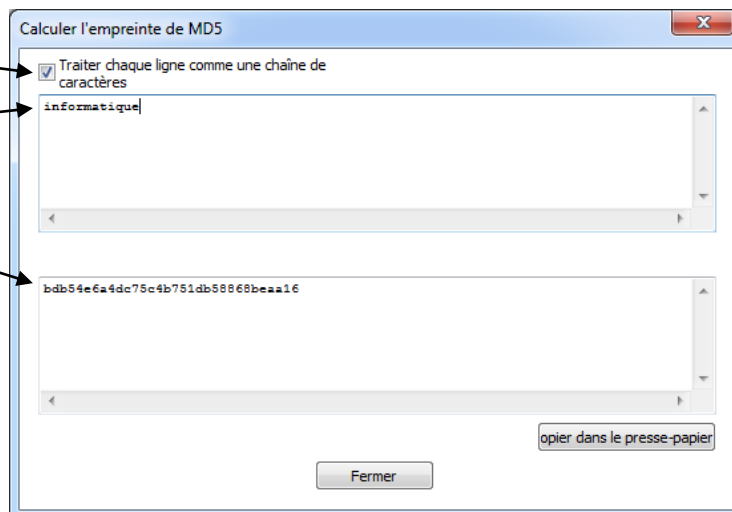
<https://openclassrooms.com/fr/courses/1757741-securisez-vos-donnees-avec-la-cryptographie/6031693-hachez-vos-donnees-menu-menu>

Lien utile au TP : <https://www.malekal.com/hash-md5-sha1-sha256/>

1 Calcul d'empreintes (MD5 et SHA-256) avec Notepad++

Travail à faire :

1. Ouvrir Notepad++ et le configurer en Français si besoin (Menu **Settings / Preferences / Localization : Français / Fermer**) ;
2. Aller dans le menu **Outils / MD5 / Générer...**
3. Cocher la case
4. Saisir un mot comme « *informatique* »
5. L'empreinte **MD5** sera calculée
6. Vérifier que si on change une lettre dans le mot, par exemple *informatiquf* ou *informatique*, l'empreinte change complètement.
7. Fermer la fenêtre
8. De même, calculer l'empreinte SHA-256 du mot *informatique* (Menu **Outils / SHA-256 / Générer...**). Vérifiez que si vous changez une lettre dans le mot, l'empreinte change complètement.
9. Quelles est la longueur d'une empreinte ?



MD5 . . . bits

SHA-256 . . . bits

10. Laisser Notepad++ ouvert.

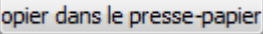
TP Cyber sécurité : Hachage

2 Tentatives d'inversion d'empreintes

Travail à faire :

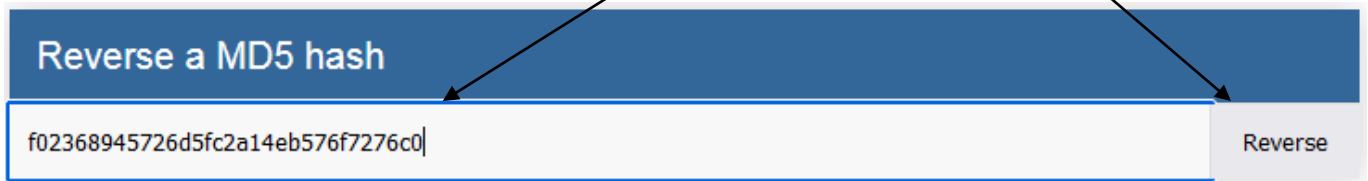
1. Avec Notepad++, calculer l'empreinte MD5 du mot *bonjour*.

Vérifier que l'on obtient bien : `f02368945726d5fc2a14eb576f7276c0`

2. Copiez l'empreinte ()

3. Allez sur le site <https://md5.gromweb.com/> et essayez d'inverser l'empreinte précédente :

`f02368945726d5fc2a14eb576f7276c0` collez-la et cliquez sur **Reverse**



Est-ce qu'on retrouve le mot d'origine ?

4. Avec Notepad++ calculer l'empreinte d'un autre mot de passe simple comme *hello*
5. Essayez ensuite de retrouver le mot de passe à partir de l'empreinte sur gromweb.com

Est-ce que l'inversion marche ?

6. Calculez de nouveau avec Notepad++ l'empreinte d'un mot de passe long et complexe comme :

`m0t-2-p@ss3-10ng-c0mpl1que`

7. Essayez ensuite de retrouver le mot de passe à partir de l'empreinte.

Est-ce que le site arrive à retrouver le mot de passe ?

8. Avec Notepad++ calculez l'empreinte d'un mot de passe compliqué.

Notez ce mot de passe :

9. Essayez d'inverser l'empreinte sur le site précédent.

Est-ce que l'inversion marche ?

Q.2.1 – Comme on l'a vu en cours, il est théoriquement impossible, à partir d'une empreinte, de retrouver les données d'origine.

Comment peut-on expliquer le fait que le site gromweb arrive parfois à retrouver un mot à partir de son empreinte, et parfois pas ?

. . . .

TP Cyber sécurité : Hachage

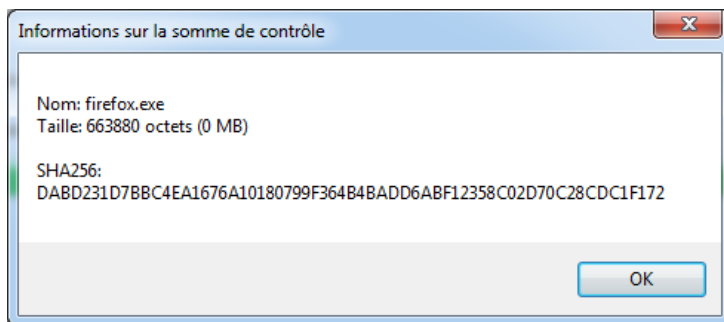
3 Calcul de l'empreinte d'un fichier

Objectif : calculer l'empreinte SHA-256 d'un fichier dans Windows.

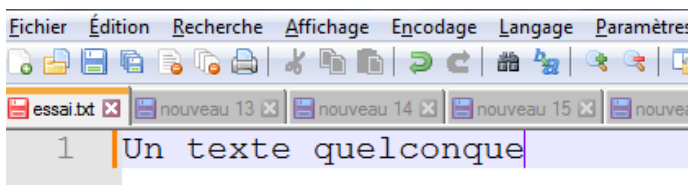
Pré requis : 7-zip doit être installé.

Travail à faire :

1. Ouvrez l'explorateur Windows, trouvez un fichier quelconque ;
2. Faites un clic droit sur le fichier, menu **7-Zip** puis **CRC SHA**, puis **SHA-256**. Résultat (par exemple pour firefox.exe) :



3. Créer dans vos documents un dossier « TP Hachage ».
4. Dans ce dossier, créez un fichier texte : clic droit **Nouveau / Document texte** et nommez-le `essai.txt`
5. Ouvrez `essai.txt` avec Notepad++
6. Tapez un texte quelconque dans le fichier et enregistrez-le.



7. Dans Windows calculer l'empreinte SHA-256 du fichier (clic droit : menu **7-Zip / CRC SHA / SHA-256**).

Notez le début de l'empreinte : . . .

8. Modifier une seule lettre du fichier. Enregistrez-le.

9. Recalculez l'empreinte SHA-256.

A-t-elle été modifiée par rapport à la première version du fichier ? . . .

TP Cyber sécurité : Hachage

4 Vérification de l'intégrité d'un téléchargement

Objectif : vérifier l'intégrité d'un fichier téléchargé sur internet, au moyen de son empreinte.

Travail à faire :

1. Télécharger le logiciel md5sums : <http://www.pc-tools.net/win32/md5sums/>

WIN32: MD5SUMS

MD5sums 1.2 - Generate MD5 hashes of files (with progress indicator)


License: Freeware


Author: [Jem Berkes](#)

Download: [md5sums-1.2.zip](#) [28 K]

2. Vérifiez que l'empreinte donnée sur le site – en bas de la page – est :
da1e100dc9e7bebb810985e37875de38

3. Quand le fichier est téléchargé, dézippez l'archive ; vous obtenez :

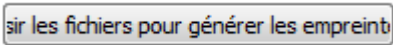
 md5sums.exe

 md5sums.txt

4. Calculez l'empreinte MD5 de md5sums.exe :

- a. Allez dans Notepad++

- b. Allez dans le menu **Outils / MD5 / Générer depuis les fichiers**

- c. Cliquer sur  pour sélectionner le fichier md5sums.exe

- d. Résultat : l'empreinte du fichier s'affiche :

da1e100dc9e7bebb810985e37875de38 md5sums.exe

- e. Est-ce que vous retrouvez l'empreinte donnée par le site ?

OUI / NON

- f. Sinon, quel peut-être l'origine du problème ?

. . .

5. Recommencez avec PHP ; allez sur le site de PHP : <https://www.php.net/downloads.php>

6. Téléchargez la dernière version, par exemple :

Current Stable PHP 8.1.12 (Changelog)

• [php-8.1.12.tar.gz \(sig\)](#) [19,302Kb]

27 Oct 2022

sha256: e0e7c823c9f9aa4c021f5e34ae1a7acafc2a9f3056ca60eb70a8af8f33da3fdf

7. Calculez l'empreinte SHA-256 du fichier téléchargé (php-8.1.12.tar.gz) en faisant dans Windows clic droit **7-Zip / CRC-SHA / SHA-256** (comme dans l'exercice précédent).

8. Est-ce que vous retrouvez l'empreinte donnée par le site ?

OUI / NON

9. Sinon, quel peut-être l'origine du problème ?

. . .

TP Cyber sécurité : Hachage

5 Hachage de mots de passe avec Bcrypt

Objectif : l'algorithme de hachage **Bcrypt** est très utilisé pour hacher des mots de passe. L'objectif ici est de hacher un mot de passe et de vérifier ensuite si le mot de passe saisi est bon.

Travail à faire :

1. Aller sur le site :

<https://bcrypthashgenerator.tool-kit.dev/>

2. Calculer la valeur de hachage (l'empreinte) d'un mot de passe de votre choix :

Nombre de fois que le mot de passe sera haché successivement (ça sert à ralentir l'algorithme et donc les attaques par force brute)

Votre mot de passe (au choix)

Cliquer pour lancer le calcul

Résultat : mot de passe haché

Cliquer pour copier le résultat



Online Bcrypt Hash Generator

Number of log rounds ⓘ: 4


Prefix ⓘ: ☐ 2a ☒ 2b

☒ Random salt

p@ssw0rd

\$2b\$04\$xYD5AppKwTBRtpjgOHzzE.KR5SVspBSzB2d.QEsKNstY6jrXoTlk2



3. Vérifiez maintenant que l'empreinte obtenue correspond bien à votre mot de passe :

Collez l'empreinte dans le champ de droite

Saisissez le bon mot de passe

Cliquer pour vérifier

Résultat



Online Bcrypt Hash Generator

Number of log rounds ⓘ: 4


Prefix ⓘ: ☒ 2b

☒ Random salt

p@ssw0rd



\$2b\$04\$xYD5AppKwTBRtpjgOHzzE.KR5SVspBSzB2d.QEsKNstY6jrXoTlk2



Online Bcrypt Hashed Matcher

\$2b\$04\$xYD5AppKwTBRtpjgOHzzE.KR5SVspBSzB2d.QEsKNstY6jrXoTlk2

Enter the Plain Text Password

Output result..

4. Est-ce que votre mot de passe correspond (ça « match ») ? . . .
5. Re faites l'étape 3 avec un mauvais mot de passe. Normalement ça ne doit pas correspondre : **Did not matched!** .

TP Cyber sécurité : Hachage

6 Deviner un mot de passe haché avec Bcrypt

Objectif : vous êtes un.e pirate et suite à une faille de sécurité vous avez obtenu le mot de passe haché (avec Bcrypt) d'un utilisateur :

\$2b\$04\$1ElGphqck5kn.5/t7PYiIOK8Ty.zeQYoHJjdQoTVYR2n/bx5rwWPS

Vous savez de plus que le mot de passe est constitué des deux éléments suivants :

- le nom d'une capitale d'un pays frontalier à la France (en commençant par une majuscule)
- suivi de l'année actuelle.

Travail à faire :

6.1 – Retrouver le mot de passe original.

Réponse : . . .