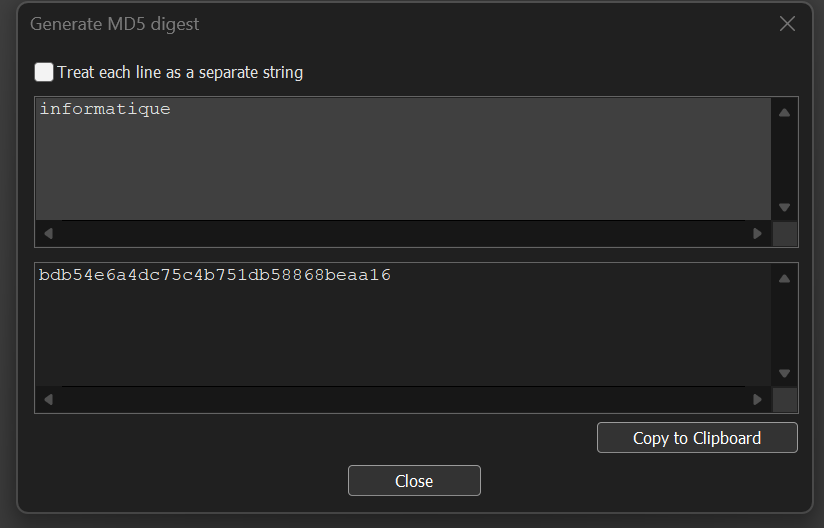
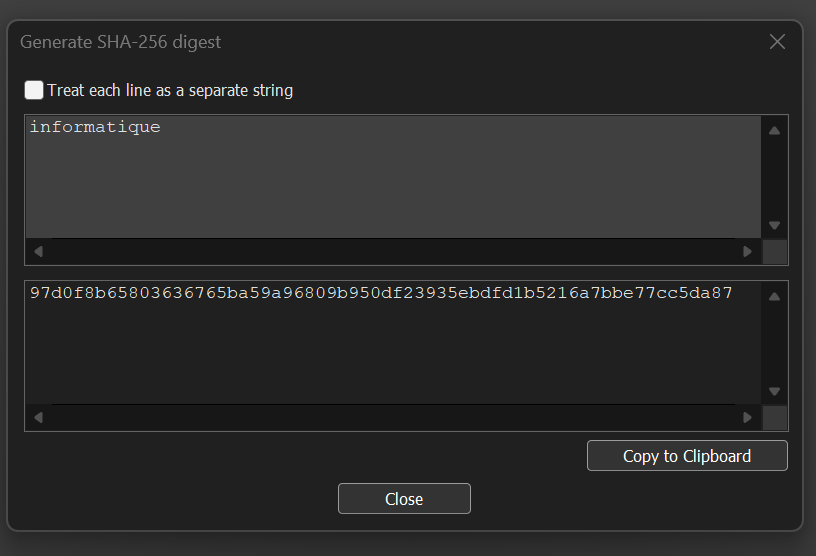
**TP HACHAGE**

Notepad++, 7-Zip, Frhed

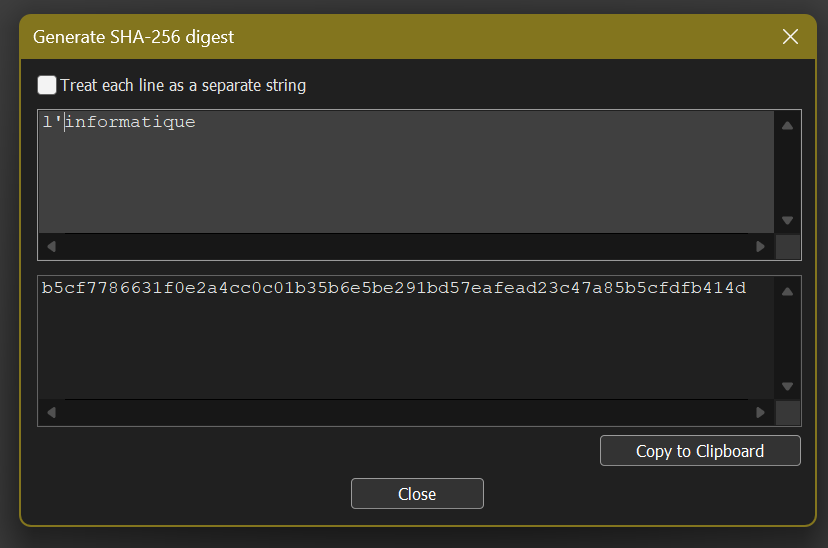
1. **Calcul d’empreintes (MD5 et SHA-256) avec Notepad++**



Quel que soit le prompt entré dans l’algorithme de hachage, le message haché sera toujours de la même longeur. L’emprinete MD5 a toujours la meme longueur, 2 prompts différnet auront toujours une empreinte différente.le meme mot génére toujours la meme empreinte



La meme logique est applicable pour SHA-256

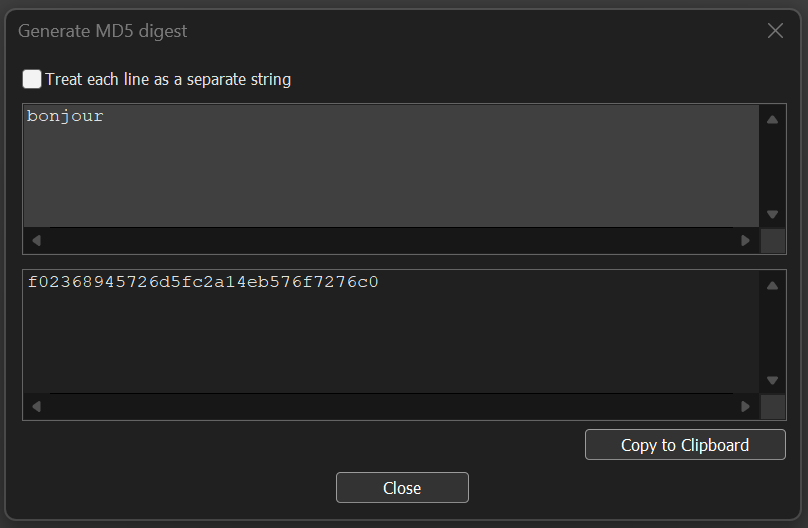


Si un caractère change, toute l'empreinte générée sera changée

Longueur d’une empreinte

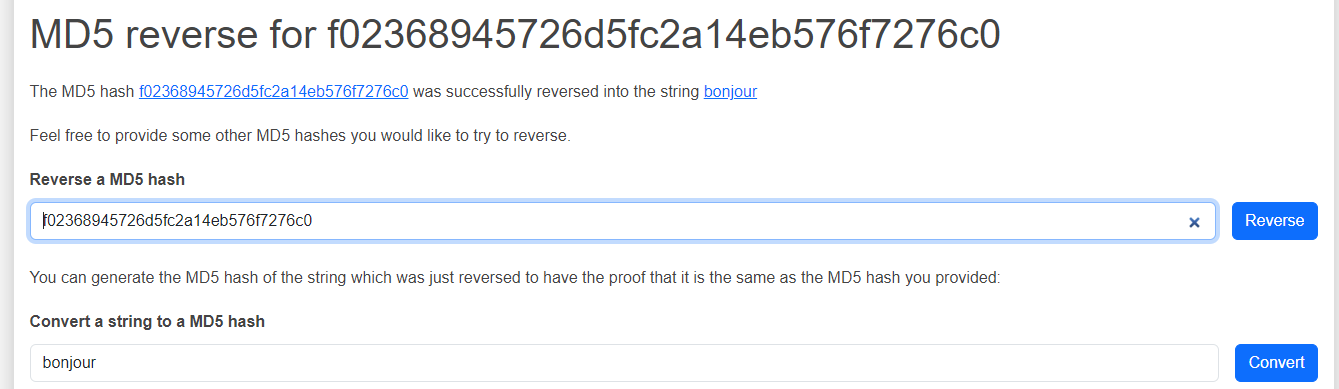
|  |  |  |
| --- | --- | --- |
| algorithm | longueur | binaire |
| MD5 | 32 | 128 |
| SHA-256 | 64 | 256 |

**MD5 du mot bonjour**



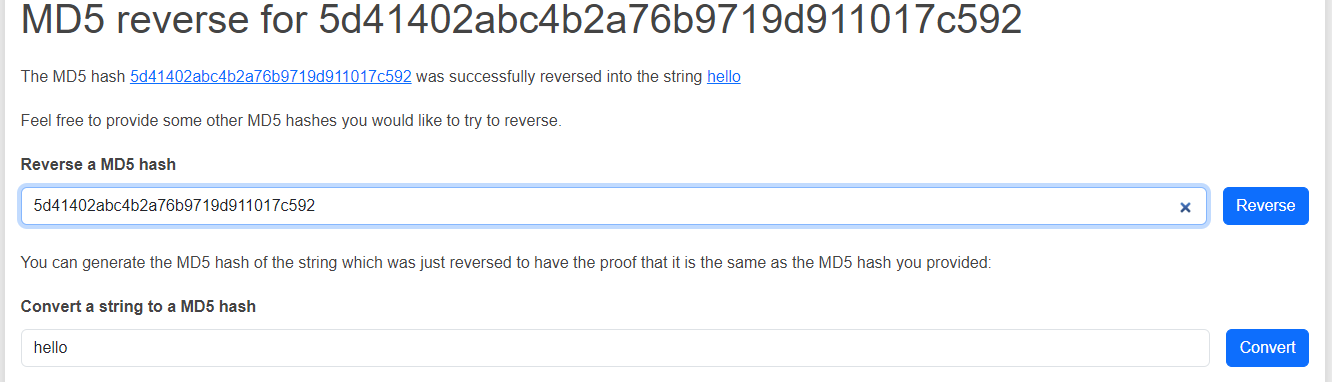
1. **Tentatives d’inversion d’empreintes**

|  |  |
| --- | --- |
| Mot | MD5 |
| bonjour | f02368945726d5fc2a14eb576f7276c0 |

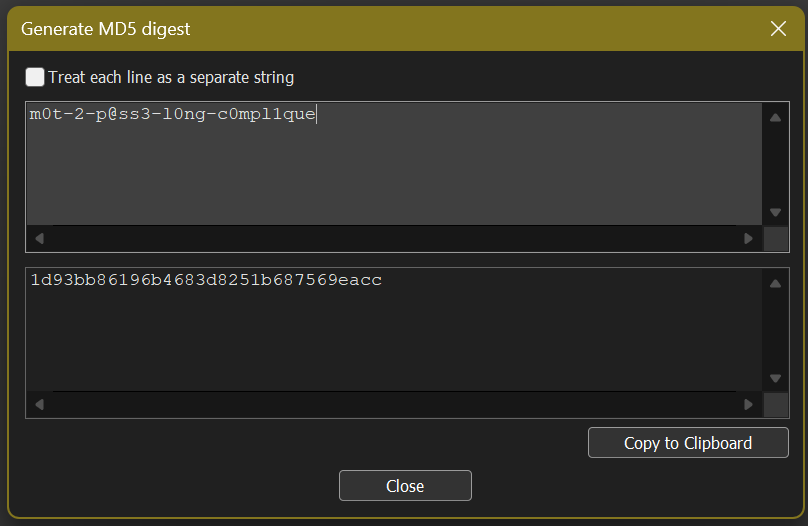


Oui le site <https://md5.gromweb.com/> permet de retrouver le texte à clair du message chiffré.

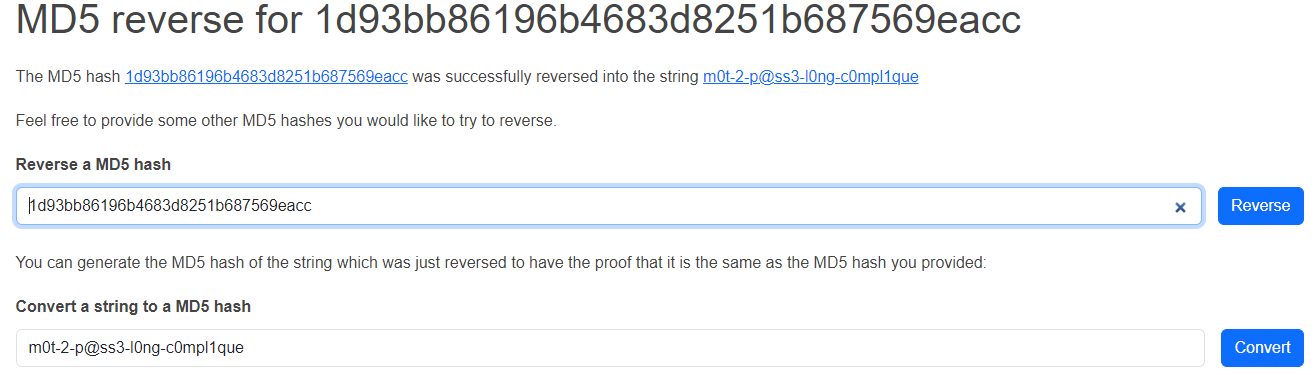
|  |  |
| --- | --- |
| Mot | MD5 |
| hello | 5d41402abc4b2a76b9719d911017c592 |



Le mot hello est retrouvé grace au site



|  |  |
| --- | --- |
| Mot | MD5 |
| m0t-2-p@ss3-l0ng-c0mpl1que | 1d93bb86196b4683d8251b687569eacc |



Le mot à clair est trouvé

La procédure de hachage se fait à partir d’un algorithme. Cet algorithme peut être connu par le public, comme l'indiquent les 3 principes de Kerckhoffs. Sauf que, afin que l'algorithme puisse fonctionner et générer des empreintes, il faut une clé. L’importance réside dans la clé.

Chaque empreinte créée est associée à une certaine clé. Sans cette clé l’empreinte ne peut pas être déchiffrée et retrouvée.

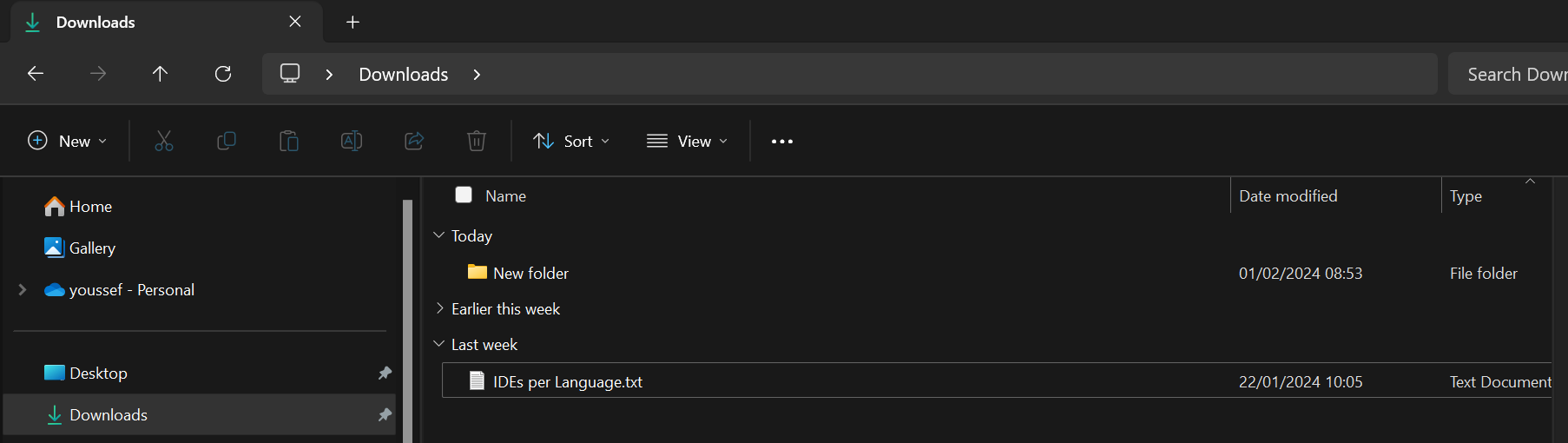
Vu que le site gromweb arrive à décrypter les empreintes du MD5, cela veut simplement dire, que l'algorithme est la clé sont implémentés dans le code source du site ce qui permet de retrouver les textes à clair des textes chiffrés.

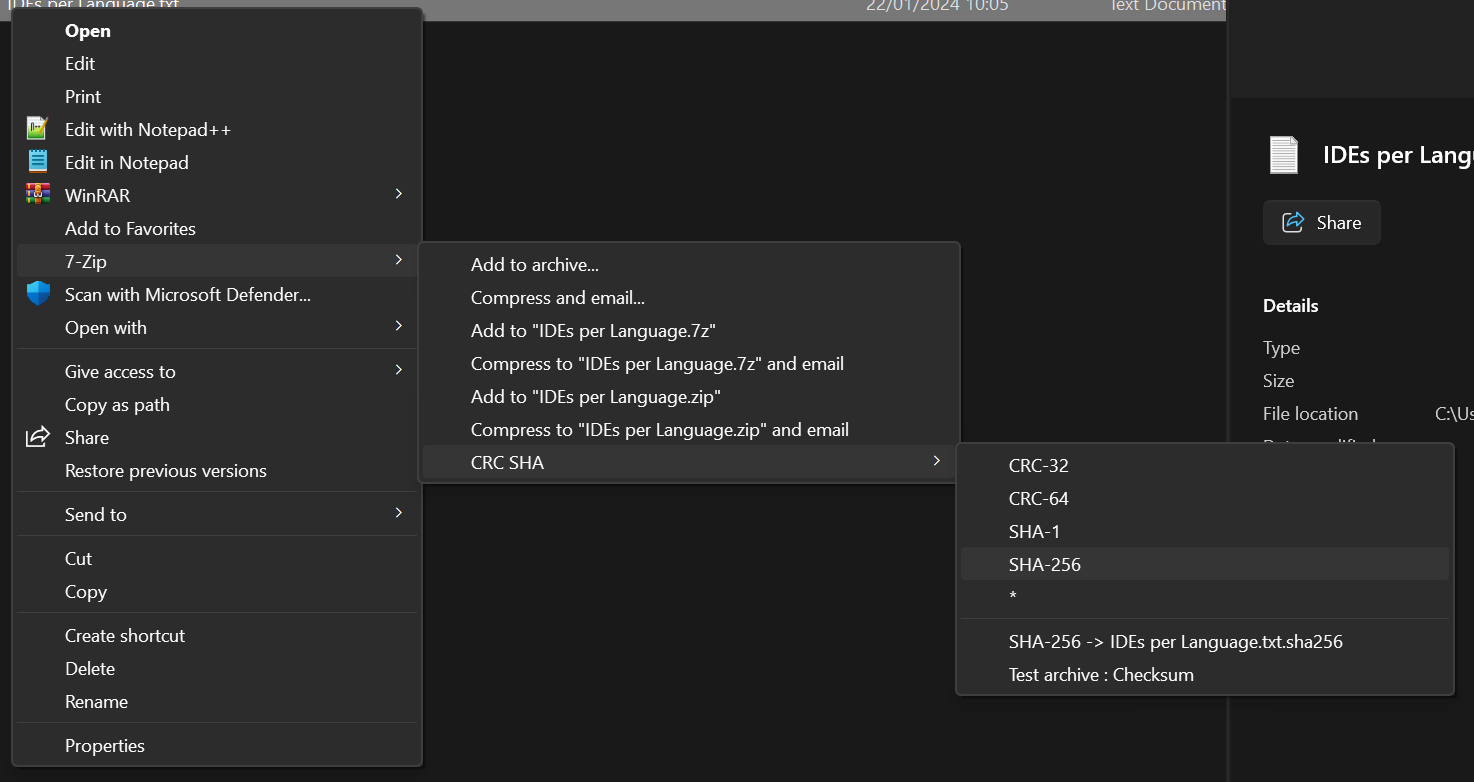
1. **Calcul de l’empreinte d’un fichier**

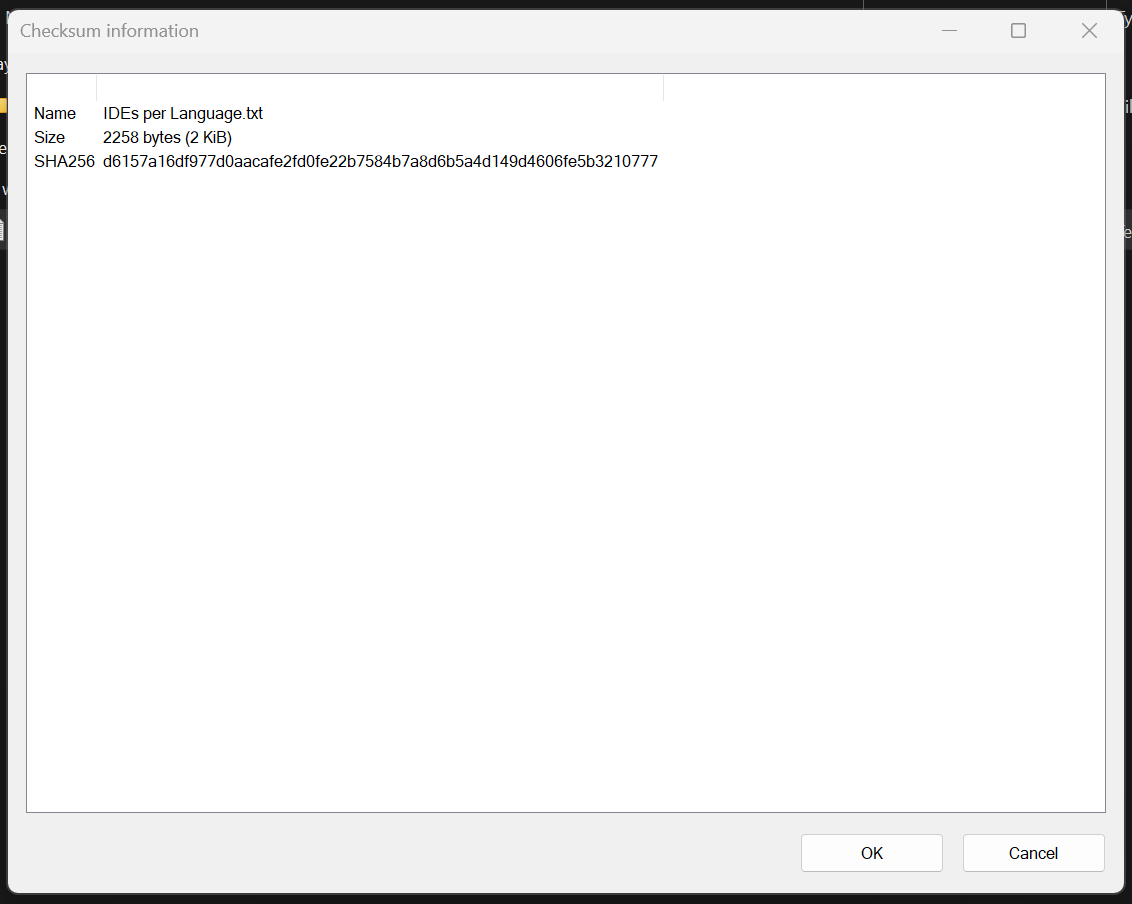
7 zip file manager doit etre installé

****

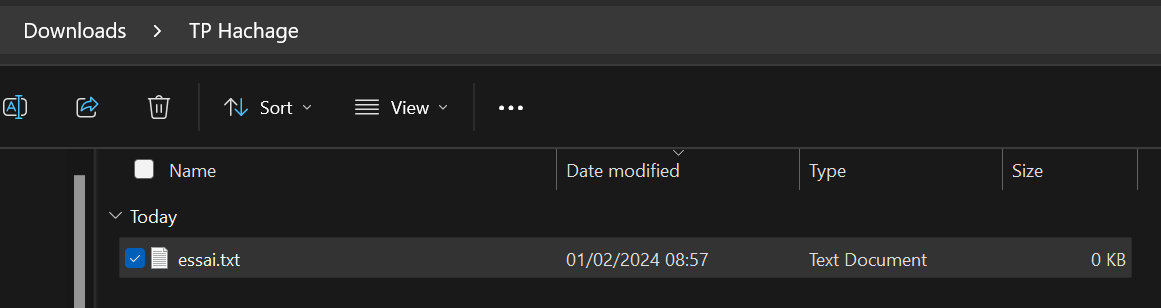
Le fichier texte IDEs per Language est choisi pour tester

****

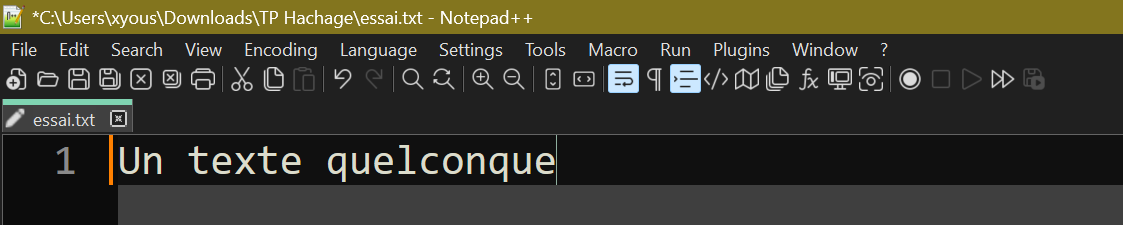
****

****

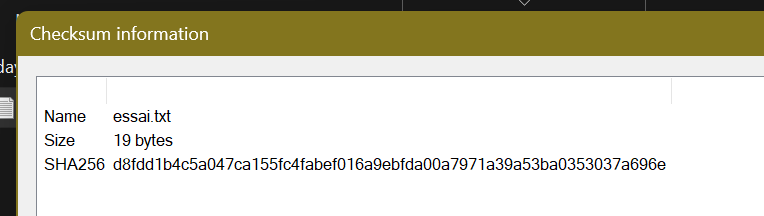
Création d’un nouveau fichier essai.txt dans le dossier TP Hachage

****

On en met du texte

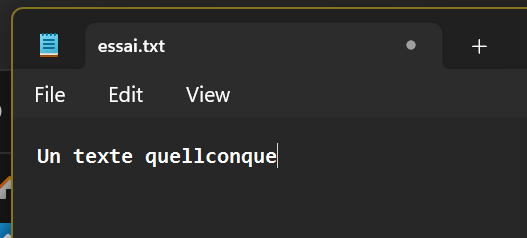
****

Essai.txt SHA-256 par 7-Zip



|  |  |
| --- | --- |
| document | SHA-256 |
| essai.txt | d8fdd1b4c5a047ca155fc4fabef016a9ebfda00a7971a39a53ba0353037a696e |

Modification du texte

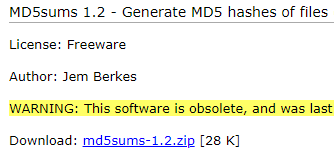


(après modification)

|  |  |
| --- | --- |
| document | SHA-256 |
| essai.txt | eac488fc12c7cdc8b6890ace47fe50869da74e1e06c627d98fbca21cbabac59b |

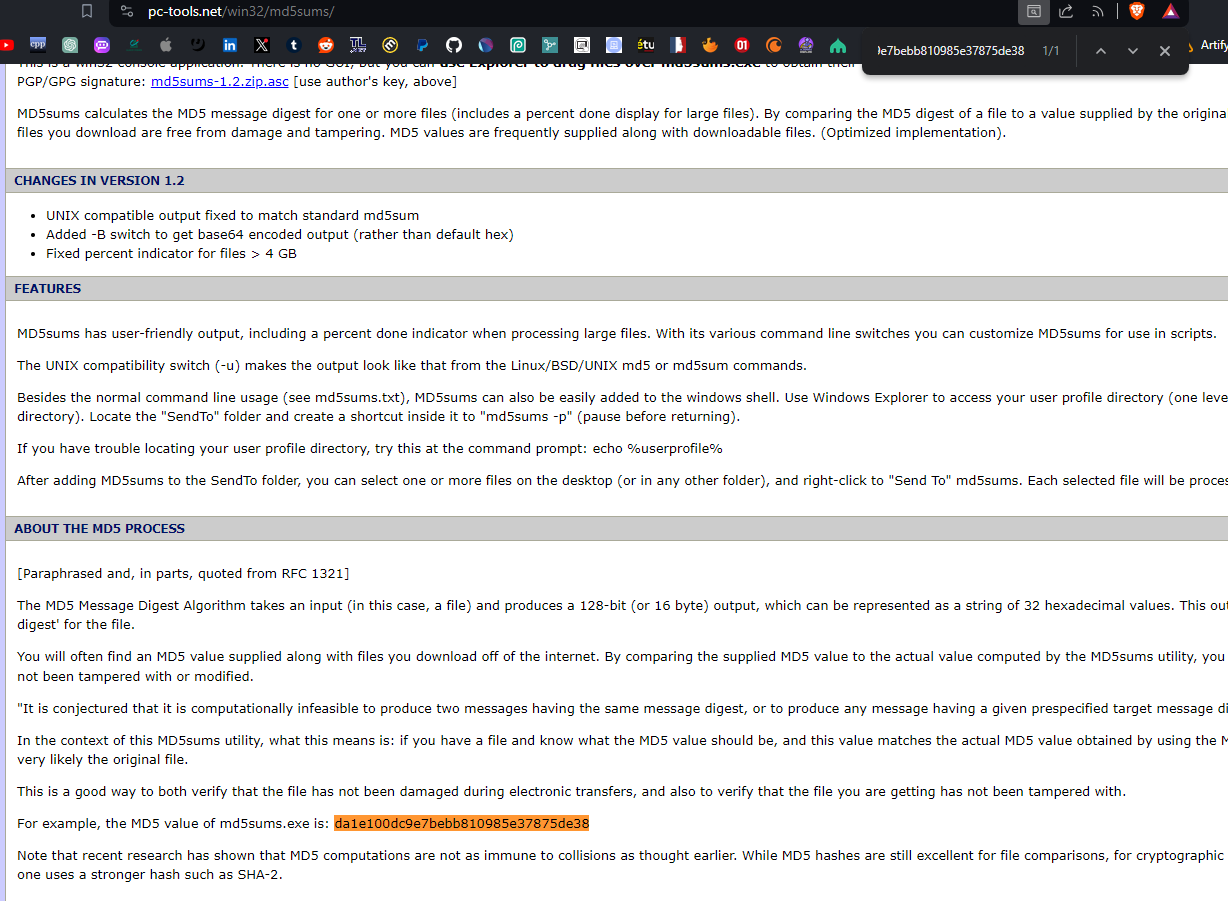
L’empreinte a été modifiée après le changement

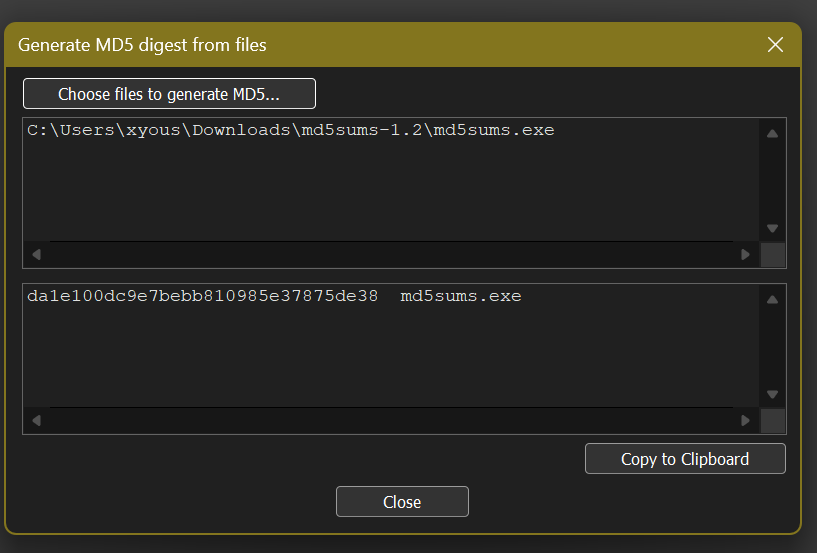
1. **Vérification de l’intégrité d’un téléchargement**



logiciel téléchargé

<http://www.pc-tools.net/win32/md5sums/>

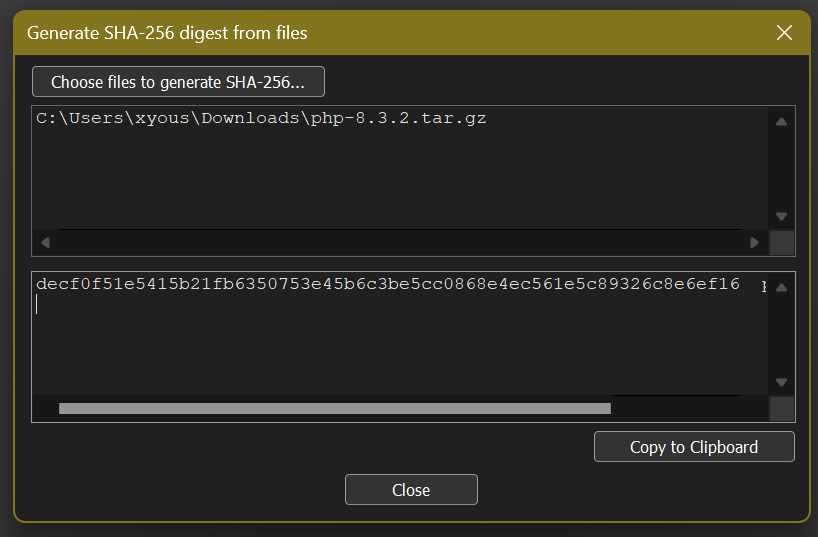




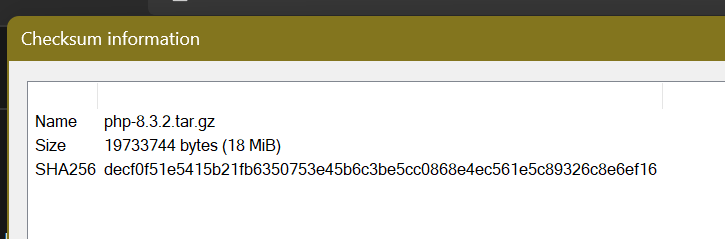
L’empreinte est retrouvé à traver ctrl+f

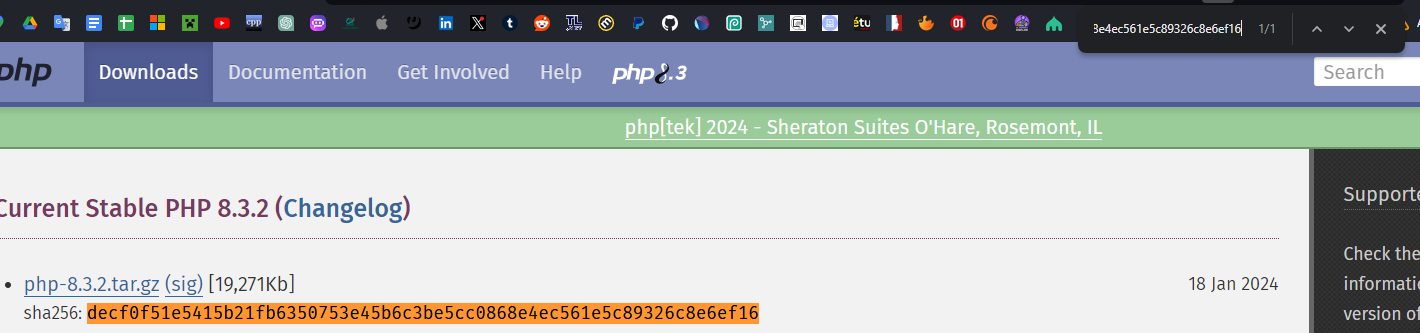
On test avec un fichier différent

**Avec notepad++**



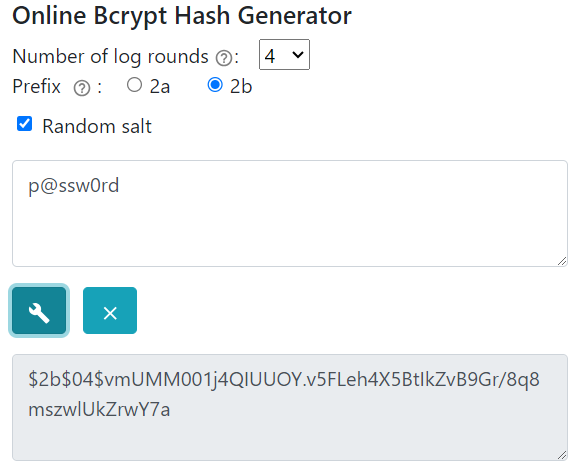
**Avec 7 zip**



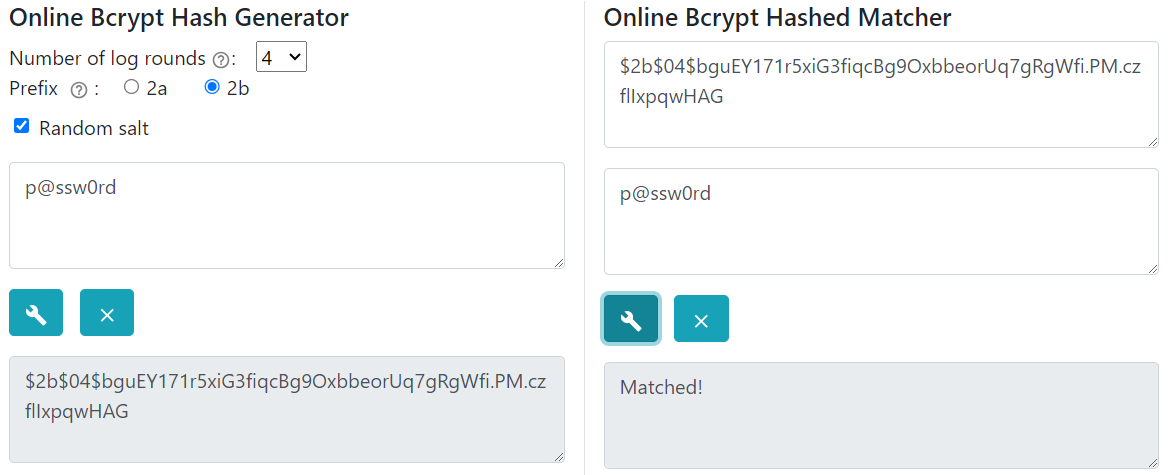


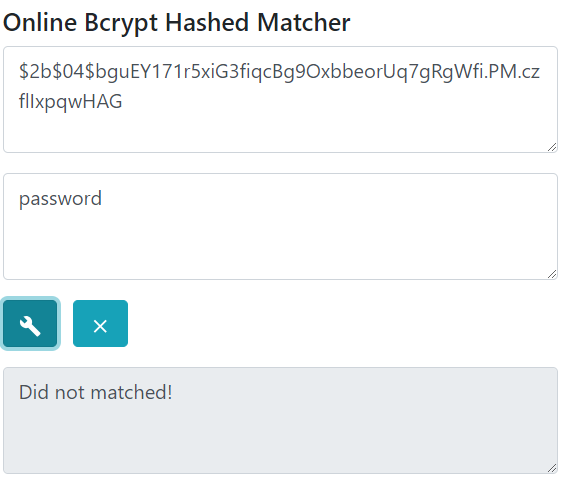
Oui c’est trouvé sur le site à travers ctrl+f

1. **Hachage de mots de passe avec Bcrypt**

****

Avec les mêmes paramètres et le même message à clair. Le message crypté à toujours différent





1. **Deviner un mot de passe haché avec Bcrypt**

