Cryptographie

Table des matières

[TP2.1 :Intégrité 3](#_Toc26882047)

[TP2.2 : Hachage et Authentification 3](#_Toc26882048)

[TP2.3 :Cryptographie 3](#_Toc26882049)

[Tp2.2 : Hachage et Authentification 4](#_Toc26882050)

# TP2.1 :Intégrité

Malheureusement a l’heure ou je veux faire ce Tp moodle est inaccesseoble. Je ne peux donc pas télécharger TCPview de l’archive moodle. J’ai donc essayer de le télécharger sur le web mais impossible de le lancer.

Pour vérifier l’intégriter d’un fichier, je peux tout de même me référer a ce tutoriel.

<https://lecrabeinfo.net/verifier-integrite-calculer-empreinte-checksum-md5-sha1-sha256-fichier-windows.html>

# TP2.2 : Hachage et Authentification

Le mot de passe est badpassword.

Le mot de passe étant déjà utilisé, il a été stocker dans une basse de donnée ce qui a permis a l’algorithme d’etre décrypté.

# TP2.3 :Cryptographie

Le message en claire est : Il ne faut pas confondre Codage et Chiffrement !

J’ai pu déchiffrer facilement ce message car la base64 est un moyen de conversion générique, tandis que le hachage est fait en fonction d’une clé spécifique défini par chaque algorithme.