**Ερώτημα 3-password cracking ελληνικής λέξης**

Το hashed password που προσπαθούμε να σπάσουμε είναι το εξής:

**23997786f8c60122a711f040a7acb4faa5ddd0681d5d658807ab0f9e987d6042**

**Από την εκφώνηση γνωρίζουμε πως το password είναι μία Ελληνική λέξη. Για αυτό τον λόγο επιλέγουμε να εφαρμόσουμε dictionary attack.**

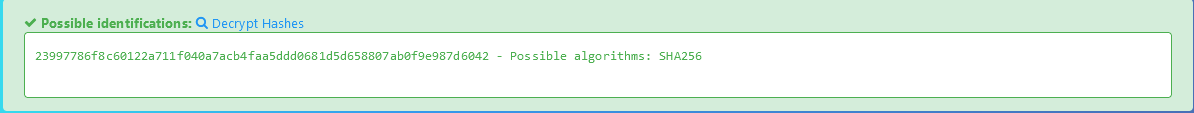
**Μεταβαίνουμε στην ιστοσελίδα:** <https://hashes.com/en/tools/hash_identifier> **για να εντοπίσουμε τον τύπο του hash αλγόριθμου που έχει εφαρμοστεί στο password.**

Graphical user interface, text, application, email

Description automatically generated

Copy-paste του hashed password

Πατάμε το κουμπί «SUBMIT & IDENTIFY» για να δούμε τα αποτελέσματα:



Πιθανός hash αλγόριθμος: SHA256

Αφού εντοπίσουμε τον hash αλγόριθμο, ανοίγουμε το περιβάλλον Cain και επιλέγουμε το tab «Cracker»:

Graphical user interface, application, table, Excel

Description automatically generated

Cracker tab στο Cain

Επιλέγουμε το SHA-2 από το αριστερό μενού καθώς ο SHA256 είναι αυτής της κατηγορίας. Πατάμε το κουμπί «+» για να εισάγουμε το hashed password:

Graphical user interface, application

Description automatically generatedGraphical user interface, application, table

Description automatically generated

Στη συνέχεια κάνουμε δεξί κλικ στο hashed password🡪Dictionary Attack🡪SHA2 256 Hashes:

Graphical user interface, application, table

Description automatically generated

Στο παράθυρο που εμφανίζεται κάνουμε δεξί κλικ στη περιοχή «Dictionary» και επιλέγουμε «Add to list» για να εισάγουμε το αρχείο με το ελληνικό λεξικό:

Graphical user interface, application

Description automatically generated

Εισαγωγή του αρχείου gr\_dic.txt από τα χρήσιμα έγγραφα του μαθήματος(gunet2)

Αλλάζοντας τα Options αφήνοντας μόνο το πρώτο κουτάκι τικαρισμένο, πατάμε «Start». Σε μερικά δευτερόλεπτα έχουμε αποτέλεσμα:

Graphical user interface, application

Description automatically generated

Επιτυχής cracking του password

Graphical user interface

Description automatically generated with medium confidence

To password δεν έχει εκτυπώσιμη τιμή στο Cain καθώς χρησιμοποιούνται Unicode χαρακτήρες(Ελληνικά)

Να σημειωθεί, πως κρατήσαμε μόνο το option «As Is (Password)» καθώς γνωρίζουμε πώς το password είναι μια λέξη του λεξικού που βγάζει νόημα. Έτσι γλυτώνουμε να ελέγξουμε πολλές περιπτώσεις.

Σαν έξτρα κομμάτι αυτής της άσκησης, υλοποιήθηκε ένα script σε python που διαβάζει μία μία τις λέξεις από το αρχείο λεξικό και βρίσκει την sha256 τιμή τους. Αν αυτή συμπίπτει με αυτήν που θέλουμε τότε τυπώνει στην κονσόλα «found» και σταματάει:

Text

Description automatically generated

Το password είναι «παράδειγμα»

**To script:**

import hashlib

import io

#hash value we are looking for

wanted\_hash = "23997786f8c60122a711f040a7acb4faa5ddd0681d5d658807ab0f9e987d6042"

for word in io.open("gr\_dic.txt", mode="r", encoding="utf-8").readlines():

m = hashlib.sha256()

m.update(word[:-1].encode()) #ascii to bytes

print(word[:-1])

print(m.digest().hex()) #byte form of hash, then hex form

print()

if(m.digest().hex() == wanted\_hash):

print("found")

break