1. GITHUB PAGE FOR CODE:
2. https://github.com/dariusss185/Python-SHA256-Decryption.git

decrypt function.py

def passgenn():

import time

import pandas as pd

import hashlib

import random #IMPORTING ALL MODUELS

hashes=[] #LIST FOR ALL HASHES TO BE DECRYPTED

uppercase="ABCDEFGHIJKLMNOPQRSTUVWXYZ" #SETTING ALL THE CHARACTERS

lowercase=uppercase.lower()

digits="0123456789"

symbols="! `£$%^&\*()\_-=+?<>,.;:@'~#{}[]|¬\/\"" #CREATING A TABLE OF ALL CHARACTERS

upper,lower,nums,syms= True,True,True,True #SELECTING WHICH CHARACTERS

select=""

if upper:

select+=uppercase

if lower:

select+=lowercase

if nums:

select+=digits

if syms:

select+=symbols #SELECTING WHICH CHARACTERS, AND PARAMETRS OF PASSWORD - GREAT FOR DEBUGGING

found=False #SETTING A FALSE FLAG

while found!=True:

selection=str(input("Please enter CSV for csv file input or LINE for line input of hashses:\n"))

if selection=="LINE":

amount=int(input("How many hashes do you want to decrypt ? ")) # ASKING HOW MANY HASHES TO DECRYPT

for i in range(0,amount):

hashh=str(input("Please input your hash to decrypt: ")) #ASKING USERS FOR HASH TO INPUT

hashh=hashh.lower() #SETTING THE INPUT TO LOWERCASE

hashes.append(hashh) #ADDING THE INPUT TO A LIST

found=True

elif selection=="CSV":

name=input("Please input the CSV file name of the hashes you wish to decrypt, and make sure its within the same directroy as this file! \nFilename: ")

name=name+".csv" #ASKING USER FOR INPUT OF FILE NAME AND ADDDING EXTENSION

new= pd.read\_csv(name) #READING THE CSV FILE

lists=new.hash #SELECTING THE HASHES UNDERNEATH THE COLUMN ("HASH")

for i in range (0,len(lists)): #LOOPING THROUGH ALL HASHES

hashh=lists[i].lower() #CONVERTING TO LOWER CASE

hashes.append(hashh) #APPENDING TO LIST

found=True #BREAKING THE WHILE LOOP

for i in range(0,len(hashes)): #SETTING A LOOP FOR HOWEVER MANY HASHES ARE NEEDED TO BE DECRYPTED

print("currenctly decrypting", hashes[i])

start\_time=time.time() #SETTING THE START TIIME

while found!=False:

password = ''.join(random.choice(select) for i in range(5)) #CREATING A RANDOM WORD, LENGTH IS SET BY RANGE

password=str(password) # STORING THE WORD IN A STRING VARIABLE

string = hashlib.sha256(password.encode('utf-8'))

password\_hashed = (string.hexdigest()) #CREATING A HASH FOR THE GENERATED WORD

if password\_hashed==hashes[i]: #COMPARING THE GENERATED HASH WITH THE INPUT FOR HASHH TO BE DECRYPTED\

print(password\_hashed, "FOUND") #NOTYFING USER THAT THE HASH HAS BEEN FOUND

print(hashes[i], "decrypted is \n"+password) #NOTYFYING THE USER THAT THE HASH IS THE GENERATED WORD

elapsed\_time = (time.time() - start\_time) #CALCULATING TOTAL TIME IT HAS TAKEN TO DECRYPT

print("TOTAL SECONDS ELAPSED FOR THIS HASH TO BE CRACKED: ", elapsed\_time) #NOTYFYING THE USER OF THE TOTAL TIME

if i==len(hashes): #CHECKING TO SEE IF ITS THE LAST HASH NEEDED TO BE DECRYPTED

found=False #SETTING THE FLAG THAT ALL HASHES HAVE BEEN FOUND AND BREAKING THE LOOP

break #BREAKING THE LOOP

passgenn()