#!/bin/python3

import hashlib

type\_of\_hash = str(input('Which type of hash do you want to bruteforce ? '))

file\_path = str(input('Enter path to the file to Bruteforce with: '))

hash\_to\_decrypt = str(input('Enter Hash Value to Brute force: '))

with open(file\_path, 'r') as file:

for line in file.readlines():

if type\_of\_hash == 'md5':

hash\_object = hashlib.md5(line.strip().encode())

hashed\_word = hash\_object.hexdigest()

if hashed\_word == hash\_to\_decrypt:

print('\n')

print('Found MD5 password: ' + line.strip())

exit(0)

if type\_of\_hash == 'sha1':

hash\_object = hashlib.sha1(line.strip().encode())

hashed\_word = hash\_object.hexdigest()

if hashed\_word == hash\_to\_decrypt:

print('\n')

print('Found SHA1 password: ' + line.strip())

exit(0)

print('Password not in file.')