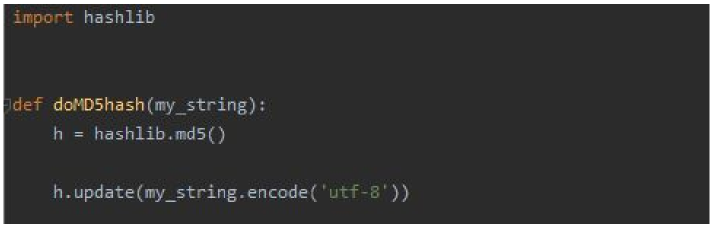
Jhante Charles

Prof. Anu

Cyber Security

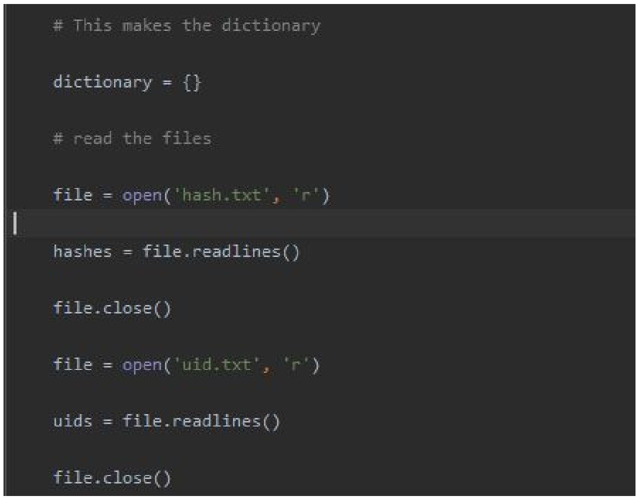
Assignment 2

For the following assignment the first part of my code sets up my md5 hash library as my function to call when I'm ready to put things through the md5 as well as the utf-8.



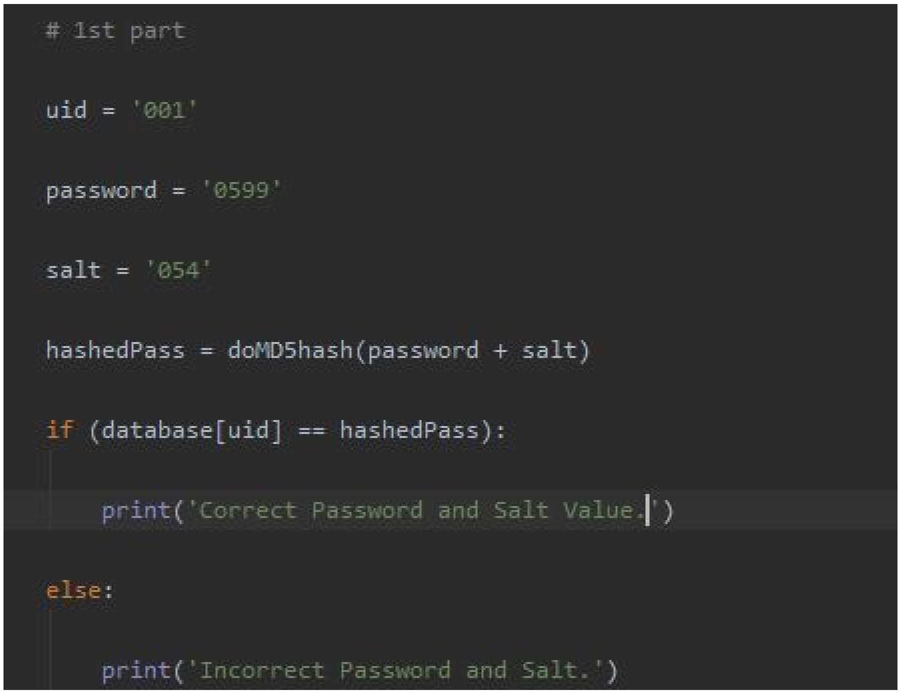
```
import hashlib


def doMD5hash(my_string):
    h = hashlib.md5()

    h.update(my_string.encode('utf-8'))
```

The following part of my code creates a dictionary to store the files in as well as opens the provided files, "uid" and "hash" that was provided with the assignment. Once they are opened the files are read and the values are then stored in the dictionary that was created.



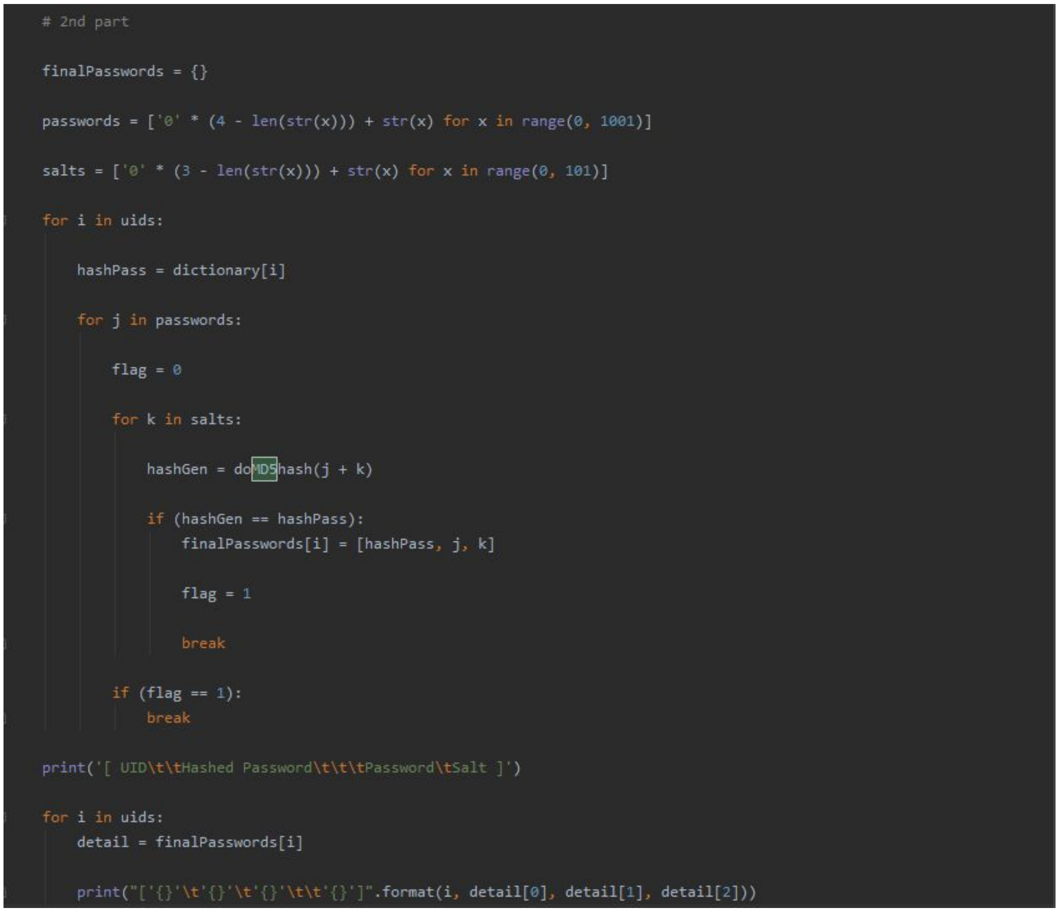
```
    # This makes the dictionary

    dictionary = {}

    # read the files

    file = open('hash.txt', 'r')

    hashes = file.readlines()

    file.close()

    file = open('uid.txt', 'r')

    uids = file.readlines()

    file.close()
```

In task one I verify that the hashed password matches up with the password and salt combo. I am able to execute and check this with an 'if else' statement.



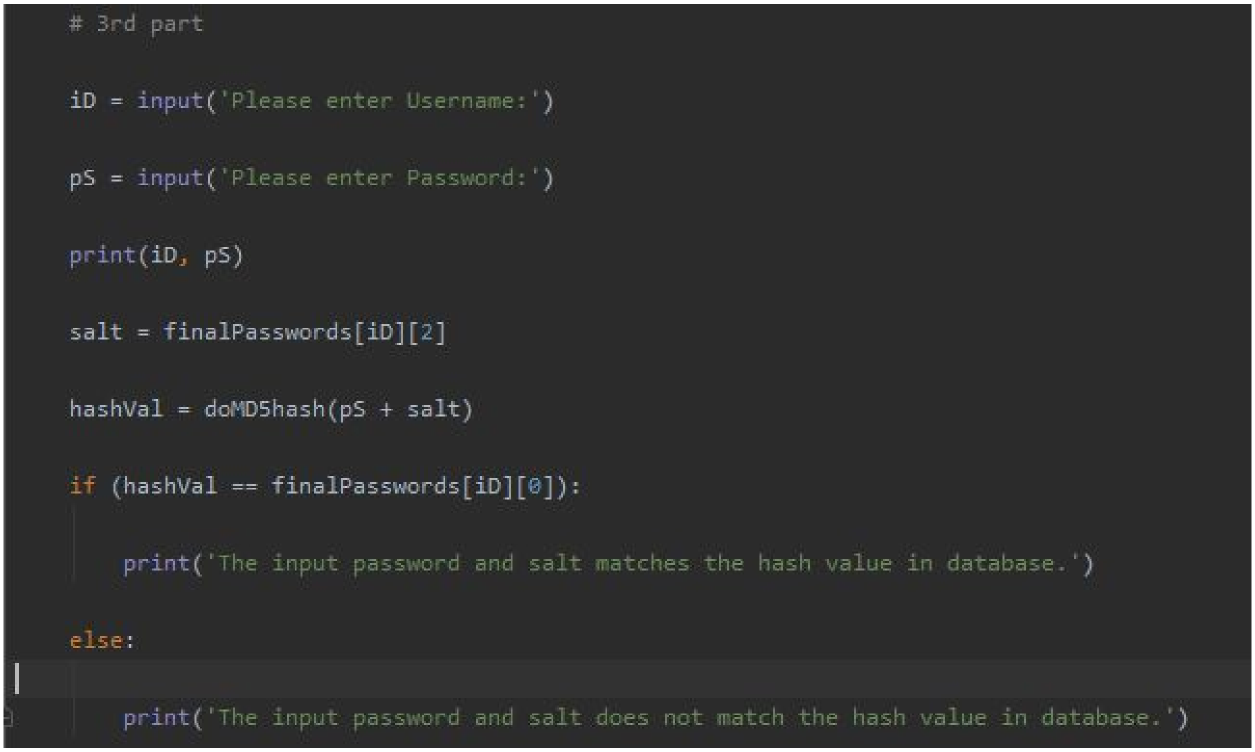
```python
# 1st part

uid = '001'

password = '0599'

salt = '054'

hashedPass = doMD5hash(password + salt)

if (database[uid] == hashedPass):

    print('Correct Password and Salt Value.')

else:

    print('Incorrect Password and Salt.')
```

In task two I create another dictionary for the final passwords that are completed. I utilize for loops to store the hashed passwords into the dictionary, compute the md5 hash of the uids and the passwords, as well as check if the final passwords and the hashed passwords of the uids and the passwords are equal.

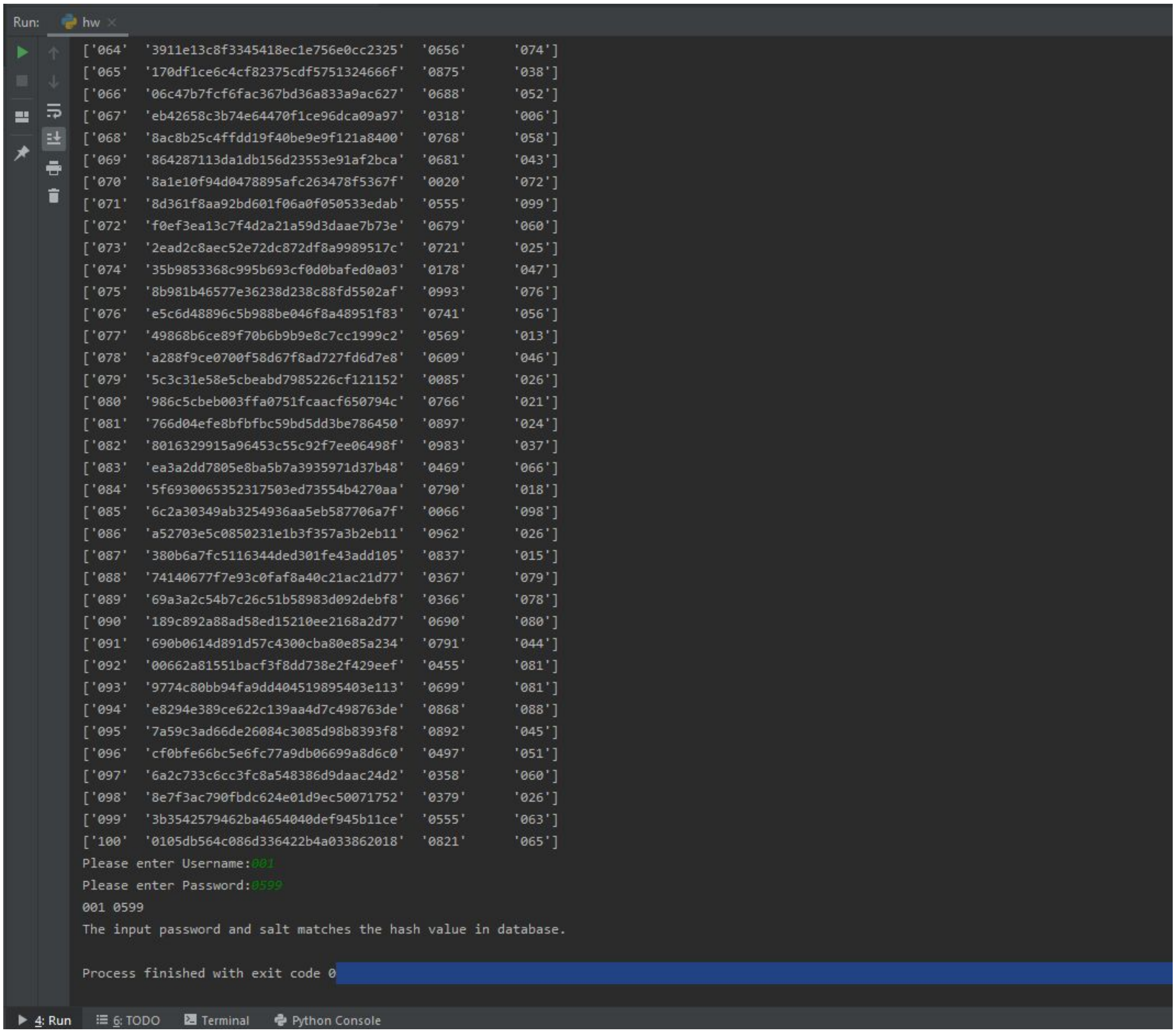


```
# 2nd part

finalPasswords = {}

passwords = ['0' * (4 - len(str(x))) + str(x) for x in range(0, 1001)]

salts = ['0' * (3 - len(str(x))) + str(x) for x in range(0, 101)]

for i in uids:

    hashPass = dictionary[i]

    for j in passwords:

        flag = 0

        for k in salts:

            hashGen = doMD5hash(j + k)

            if (hashGen == hashPass):
                finalPasswords[i] = [hashPass, j, k]

                flag = 1

                break

        if (flag == 1):
            break

print('[ UID\t\tHashed Password\t\t\tPassword\tSalt ]')

for i in uids:
    detail = finalPasswords[i]

    print("['{}'\t'{}'\t'{}'\t\t'{}']".format(i, detail[0], detail[1], detail[2]))
```

For the final task I prompt the user to enter their user id and password to see if it is valid or not using if else statements.



```python
# 3rd part

iD = input('Please enter Username:')

pS = input('Please enter Password:')

print(iD, pS)

salt = finalPasswords[iD][2]

hashVal = doMD5hash(pS + salt)

if (hashVal == finalPasswords[iD][0]):

    print('The input password and salt matches the hash value in database.')

else:

    print('The input password and salt does not match the hash value in database.')
```



```
['064'  '3911e13c8f3345418ec1e756e0cc2325'  '0656'      '074']
['065'  '170df1ce6c4cf82375cdf5751324666f'  '0875'      '038']
['066'  '06c47b7fcf6fac367bd36a833a9ac627'  '0688'      '052']
['067'  'eb42658c3b74e64470f1ce96dca09a97'  '0318'      '006']
['068'  '8ac8b25c4ffdd19f40be9e9f121a8400'  '0768'      '058']
['069'  '864287113da1db156d23553e91af2bca'  '0681'      '043']
['070'  '8a1e10f94d0478895afc263478f5367f'  '0020'      '072']
['071'  '8d361f8aa92bd601f06a0f050533edab'  '0555'      '099']
['072'  'f0ef3ea13c7f4d2a21a59d3daae7b73e'  '0679'      '060']
['073'  '2ead2c8aec52e72dc872df8a9989517c'  '0721'      '025']
['074'  '35b9853368c995b693cf0d0bafed0a03'  '0178'      '047']
['075'  '8b981b46577e36238d238c88fd5502af'  '0993'      '076']
['076'  'e5c6d48896c5b988be046f8a48951f83'  '0741'      '056']
['077'  '49868b6ce89f70b6b9b9e8c7cc1999c2'  '0569'      '013']
['078'  'a288f9ce0700f58d67f8ad727fd6d7e8'  '0609'      '046']
['079'  '5c3c31e58e5cbeabd7985226cf121152'  '0085'      '026']
['080'  '986c5cbeb003ffa0751fcaacf650794c'  '0766'      '021']
['081'  '766d04efe8bfbfbc59bd5dd3be786450'  '0897'      '024']
['082'  '8016329915a96453c55c92f7ee06498f'  '0983'      '037']
['083'  'ea3a2dd7805e8ba5b7a3935971d37b48'  '0469'      '066']
['084'  '5f6930065352317503ed73554b4270aa'  '0790'      '018']
['085'  '6c2a30349ab3254936aa5eb587706a7f'  '0066'      '098']
['086'  'a52703e5c0850231e1b3f357a3b2eb11'  '0962'      '026']
['087'  '380b6a7fc5116344ded301fe43add105'  '0837'      '015']
['088'  '74140677f7e93c0faf8a40c21ac21d77'  '0367'      '079']
['089'  '69a3a2c54b7c26c51b58983d092debf8'  '0366'      '078']
['090'  '189c892a88ad58ed15210ee2168a2d77'  '0690'      '080']
['091'  '690b0614d891d57c4300cba80e85a234'  '0791'      '044']
['092'  '00662a81551bacf3f8dd738e2f429eef'  '0455'      '081']
['093'  '9774c80bb94fa9dd404519895403e113'  '0699'      '081']
['094'  'e8294e389ce622c139aa4d7c498763de'  '0868'      '088']
['095'  '7a59c3ad66de26084c3085d98b8393f8'  '0892'      '045']
['096'  'cf0bfe66bc5e6fc77a9db06699a8d6c0'  '0497'      '051']
['097'  '6a2c733c6cc3fc8a548386d9daac24d2'  '0358'      '060']
['098'  '8e7f3ac790fbdc624e01d9ec50071752'  '0379'      '026']
['099'  '3b3542579462ba4654040def945b11ce'  '0555'      '063']
['100'  '0105db564c086d336422b4a033862018'  '0821'      '065']
Please enter Username:001
Please enter Password:0599
001 0599
The input password and salt matches the hash value in database.

Process finished with exit code 0
```