# COMP8760 Assessment 2: Practical Report

# Week 16 Class

Week 16 was about working on some password cracking exercises to gain a better understanding of password security and usability.

The following exercises were attempted: -

* Password hashing and salting
* General dictionary attacks
* Personalised dictionary attack
* Breaking a graphical password (an Android unlock pattern)

## How did I do the exercises and what did I learn about?

## All of these exercises were attempted and completed through implementation of the same through Python 3.x.

## Exercise 1 was done by implementing 2 important functions: one for user registration and the other for user login. Another function was implemented to perform necessary multiple SHA256 hashing on the password. User Registration took username, password and profile as parameters, concatenated the password and a randomly generated salt, this string was hashed using the multiple hashing function. The username, hashed value and profile are written and stored in a file. User Login takes username and password as input, searches the stored file for the username, reads the salt and does multiple hashing the string combining the password and salt, reads the stored hash value and compares with the calculated hash to see if they match. If they match, user authentication is successful else failed. Learnt how hashing with salt is useful to secure passwords and how it can be authenticated.

## Exercise 2 was done by implementing a system that could crack a password based on a given hash value. Tried single to multiple hashing at most 4 times. The given data was from a leaked password database called phpbb. All values were hit with SHA256 hashing from 1 to 4 times and one of the hashes matched with the given hash and the password was found. Learnt how to crack a password from a leaked database given the hash value.

## Exercise 3 was done by implementing a password cracking system which followed multiple hashing similar to exercise 2 and the passwords tried were based on keywords of a given information about the user, plus added with given salt and hashed to check for which combination of guessed passwords were the hash values matched for the given hash and bonus hash values. Learnt to try different permutation and combination of passwords based on information leaked from a user and to try hashing with salt to crack the passwords.

## Exercise 4 was done by trying different permutations and combinations of the letters a,b,c,d,e,f,g,h and i with a length of 9 characters and no letters repeating to crack the alphabetical passcode of a user’s phone given the hash value. Matched hash value with the hashes of different possible passcode combinations. Hashing was done using SHA1 hash function once. Learnt how to generate different combinations of an alphabetical passcode and hashed to crack the passcode of the user.

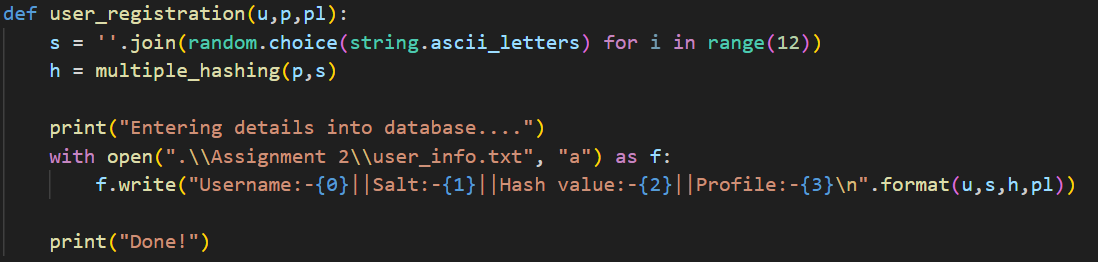
## What difficulties / problems did I encounter? / What observations and/or thoughts did you have on the exercises?

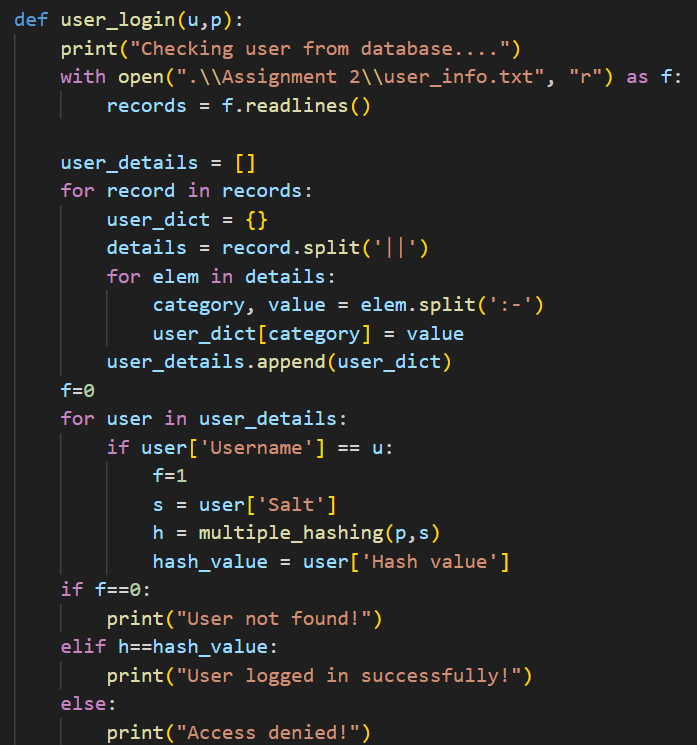
## Other than some syntax errors, file path, file read and write errors, did not face much challenges in exercises 1,2 and 4. Exercise 3 however was quite cumbersome, especially in coming up with keywords and combining all those in all ways plus considering lower and camel cases. Despite so many keywords, had a hard time cracking the passwords at first. Then realised there was a space in the salt added by mistake and removed it. Was able to finally crack the passwords then.

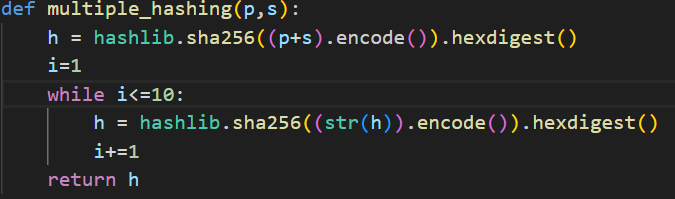
## My observations were that these exercises could suggest a maximum limit on trying multiple hashing, because for password I started with 10 times hashing then gradually reduced it to a few. Also, the 4th exercise confused me a bit with the letter-number code and I thought the hashing was to be done on the corresponding numbers instead of the letters which was of course a futile effort.

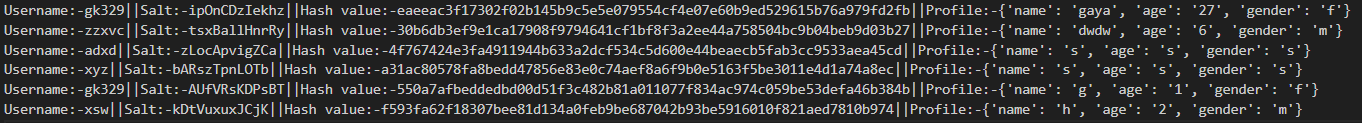
**Snippets of Code and Output**

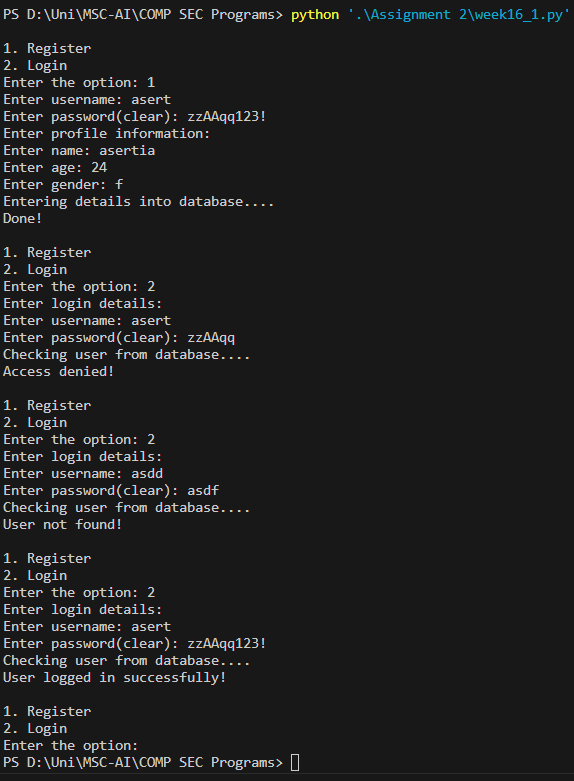
**Exercise 1**

****

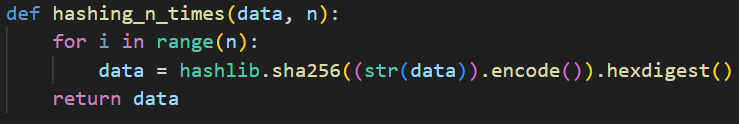
****

****

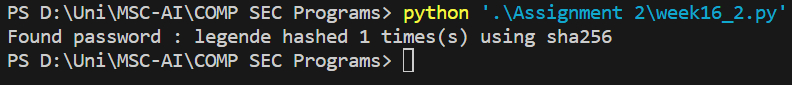
****

****

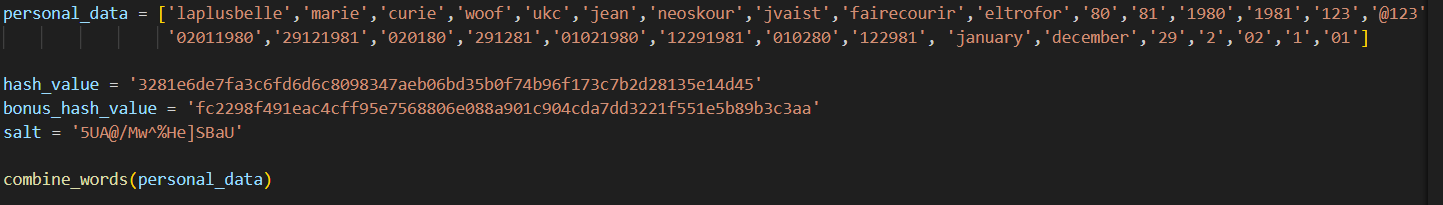
**Exercise 2**

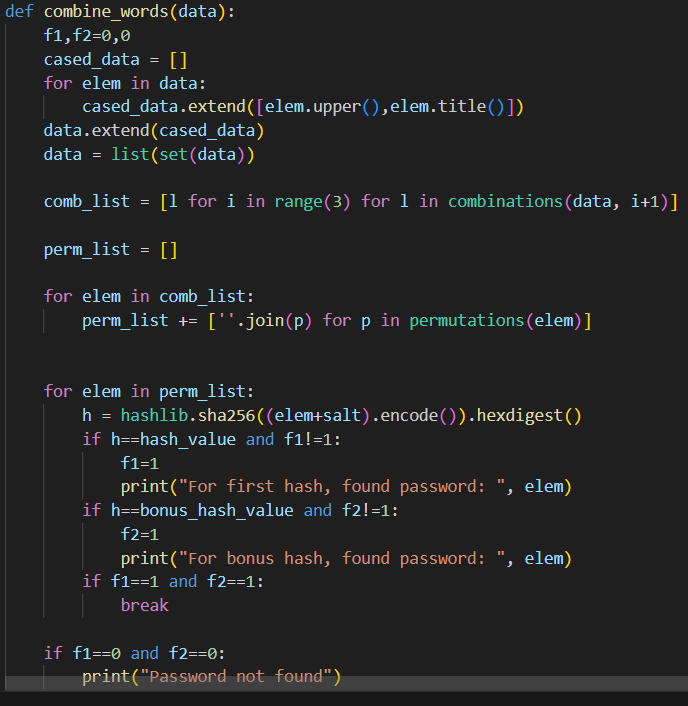
****

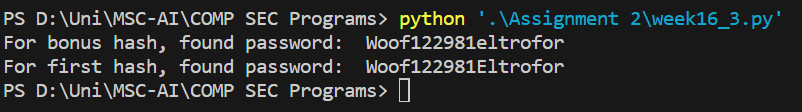
****

****

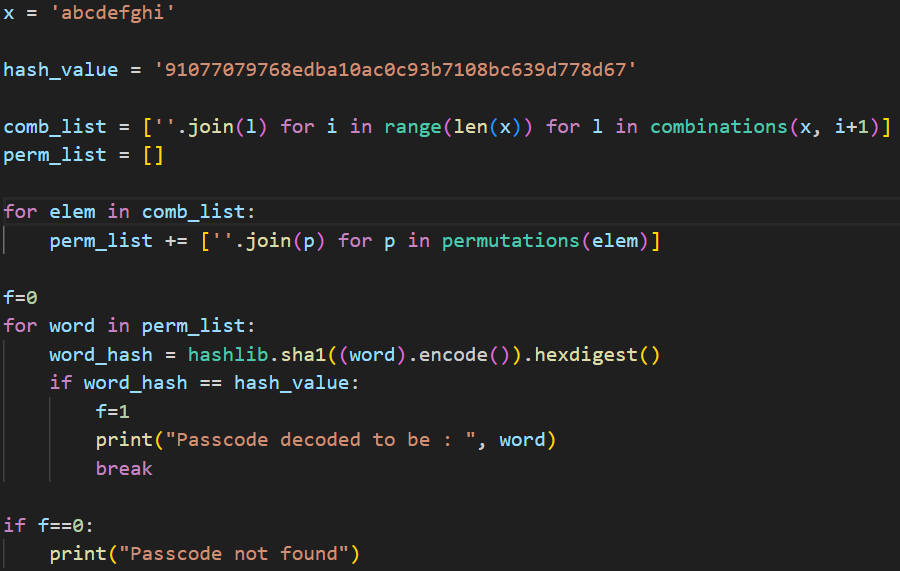
**Exercise 3**

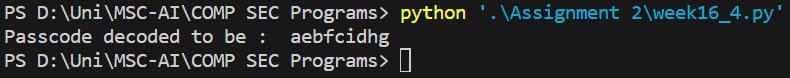
****

****

****

**Exercise 4**

****

****

# Week 17 Class

Week 17 was about working on some exercises beyond just cracking passwords to gain a better understanding of user authentication as a whole.

The following exercises were attempted: -

* Password with emojis
* Password as a file on your computer
* A toy one-time-password (OTP) generator
* Evaluating performance of a mock biometric-based authentication system

## How did I do the exercises and what did I learn about?

## All of these exercises were attempted and completed through implementation of the same through Python 3.x.

## Exercise 1 was done by using the same implementation system as that of week 16’s first exercise. It was able to take in passwords with emojis for user registration as well as user login as I had made the practice of encoding the password+salt before hashing in the same exercise which helped to incorporate the emojis. Learnt that we can use passwords with one or more combinations of emojis and hash and store the values.

## Exercise 2 was done by implementing a system similar to exercise 1 but it asks for file name as input for file password. The corresponding file was read, its contents stored in a variable and then hashed and stored. When user logs in, the given file for password is read and hashed with the salt and compared to the stored hash value. Learnt that even files can be stored as passwords.

## Exercise 3 was done by implementing previous exercise’s system but one that makes sure during user login - to add the user login time to the existing hash value password of the user, hashing it again using SHA256 and storing the new hash in the user details file. The last 6 bytes of this hash is then sent as OTP. When user enters the correct OTP, authentication is successful. Learnt that hash values need not be constant till password changes, can use login datetime as a factor and understood a method of OTP generation and verification.

Exercise 4 was done by implementing a system to read the provided data of similarities of biometric templates of a user and attacker, and come up with different threshold values of similarities to check for which thresholds to accept user Alice with a small false reject rate and reject attacker Eve with a small false accept rate. Threshold values were chosen based on Alice’s and Eve’s average values from the given data. Learnt how to analyse performance of similarity checking and suggest thresholds from provided datasets.

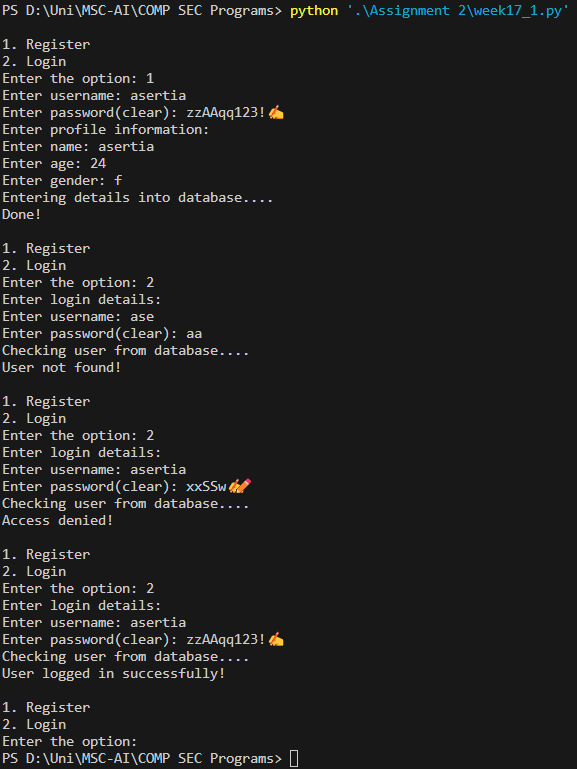
## What difficulties / problems did I encounter? / What observations and/or thoughts did you have on the exercises?

## Other than some syntax errors, file path, file read and write errors, did not face much challenges in these. Exercise 3 was a bit challenging, with coming up on how to compare password with hash value after each login and to decide whether to use password along with OTP for user login or just login with OTP and the latter was decided.

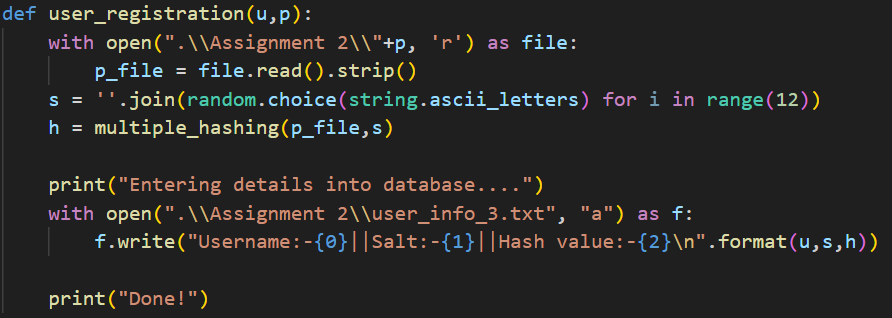
## My observations were that the second exercise could have specified on how to input the password: whether to pass file name or create a UI to upload the file. I have implemented based on the latter.

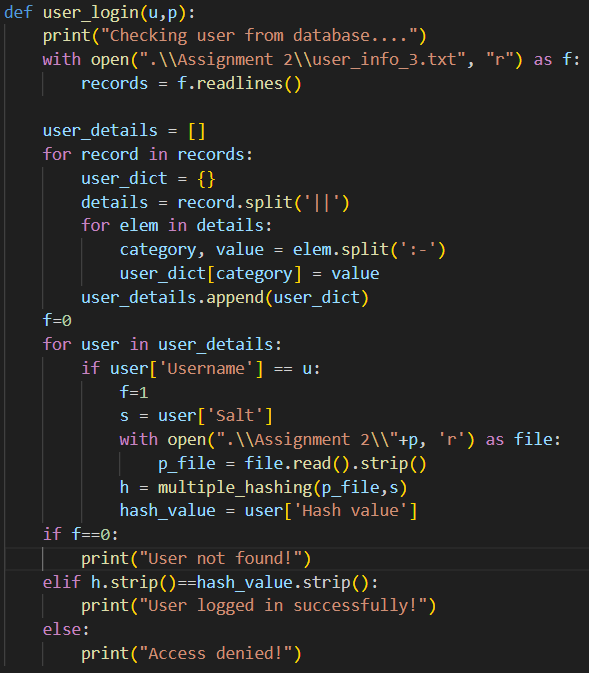
**Snippets of Code and Output**

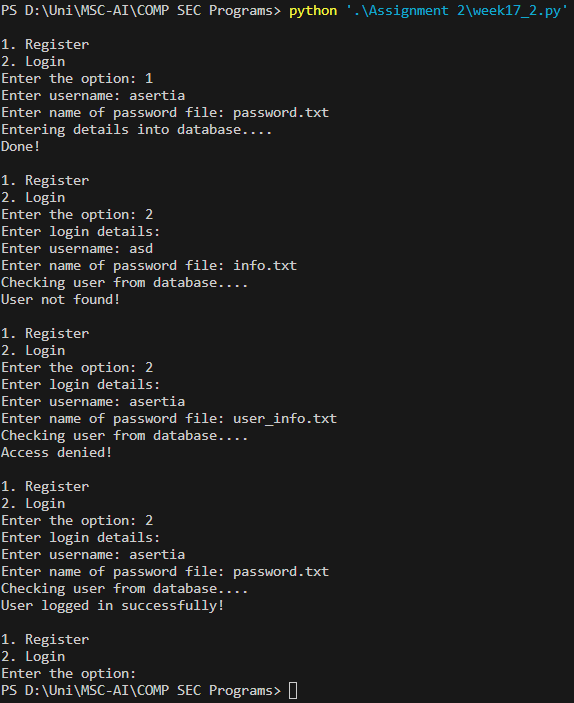
**Exercise 1**

****

**Exercise 2**

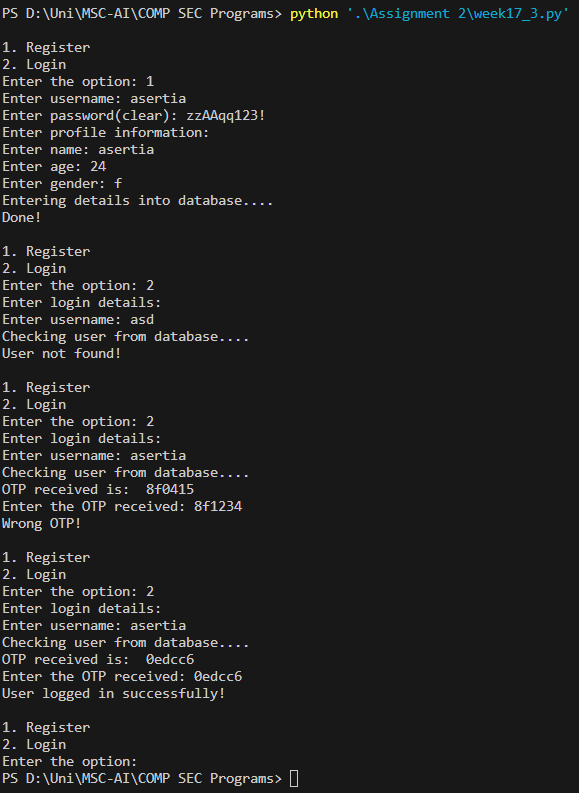
****

****

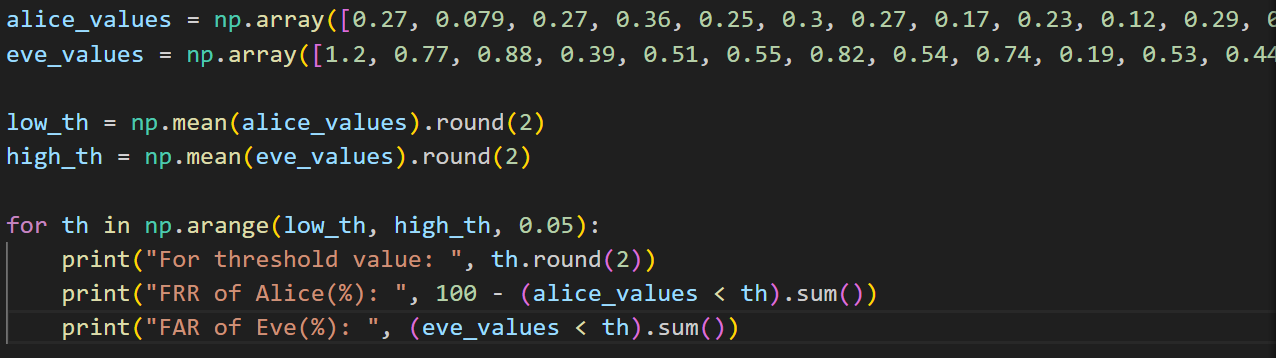
****

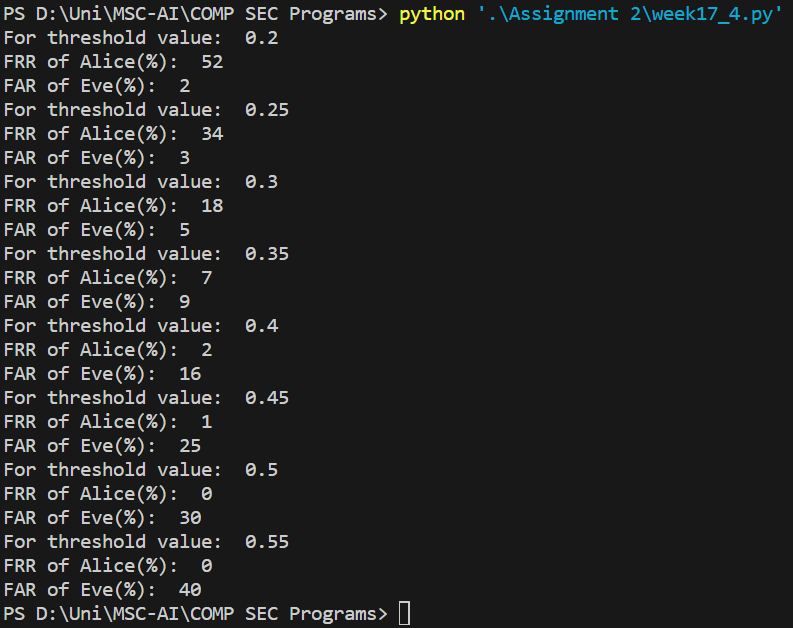
**Exercise 3**

****

****

**Exercise 4**

****

****

# Week 18 Class

Week 18 was about working on some exercises beyond user authentication to gain a better

understanding of authentication in the wider sense.

The following exercises were attempted: -

* Message authentication with HMAC
* Needham-Schroeder protocol
* Attacking Needham-Schroeder protocol

## How did I do the exercises and what did I learn about?

## All of these exercises were attempted and completed through implementation of the same through Python 3.x.

## Exercise 1 was done by implementing a system to generate 16-bit HMAC to authenticate between user and banking system. Also implemented a method for an attacker to manipulate the message between user and server depending on different values of money to be transferred and crack which for which value server accepts the message. Learnt a way of cracking authentication key as an attacker.

## Exercise 2 was done by implementing a simulation of the Needham-Schroeder protocol between 2 users, Alice and Bob and a Server. Implementations were done to define a random key generator using SHA256 hashing, encryption and decryption of messages with these keys and steps to show how the protocol works. Learnt how 2 users do encryption and decryption of data and how the server generates a key for them to use to communicate with each other.

## Exercise 3 was done by implementing a simulation of how someone can attack the Needham-Schroeder protocol, provided they recorded the K\_AB and Message 3 from a previous session of the protocol. Implementations were done to define encryption and decryption of messages with given keys and steps to show how the protocol gets attacked. Learnt how an attacker can manipulate a user to communicate with them thinking it is another authorised user.

## What difficulties / problems did I encounter? / What observations and/or thoughts did you have on the exercises?

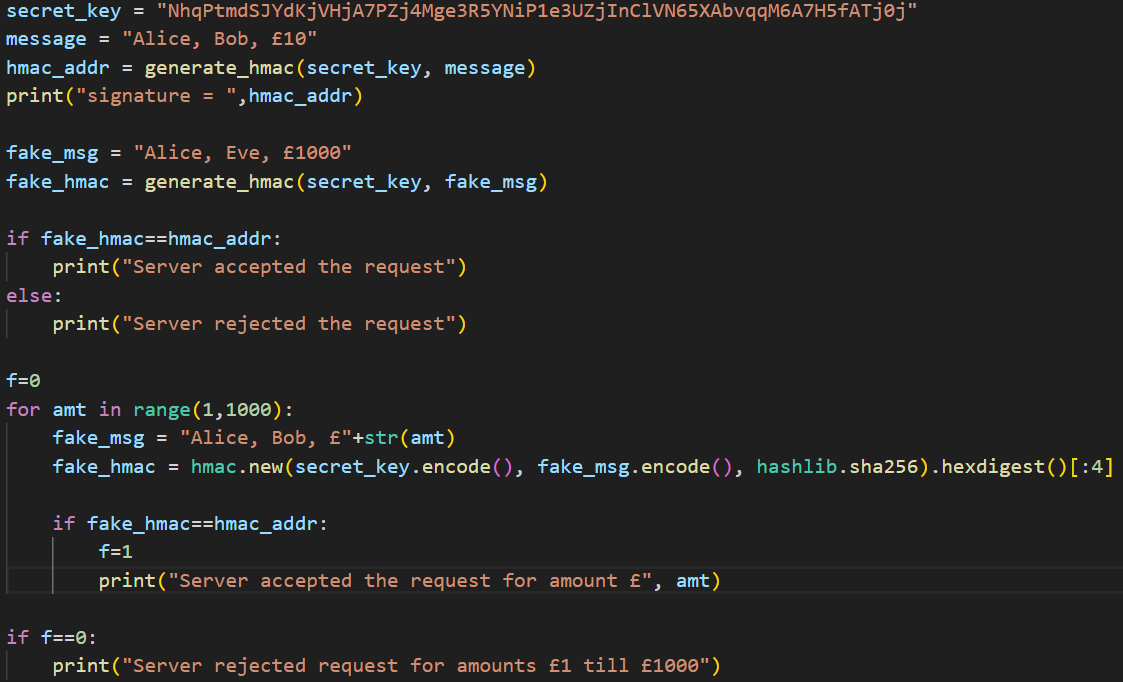
## Other than some syntax errors and the time-consuming efforts of observing and coding each and every step, did not face much challenges in these.

## My thoughts were that these were interesting exercises to demonstrate HMAC message authentication and the working and limitations of Needham-Schroeder protocol.

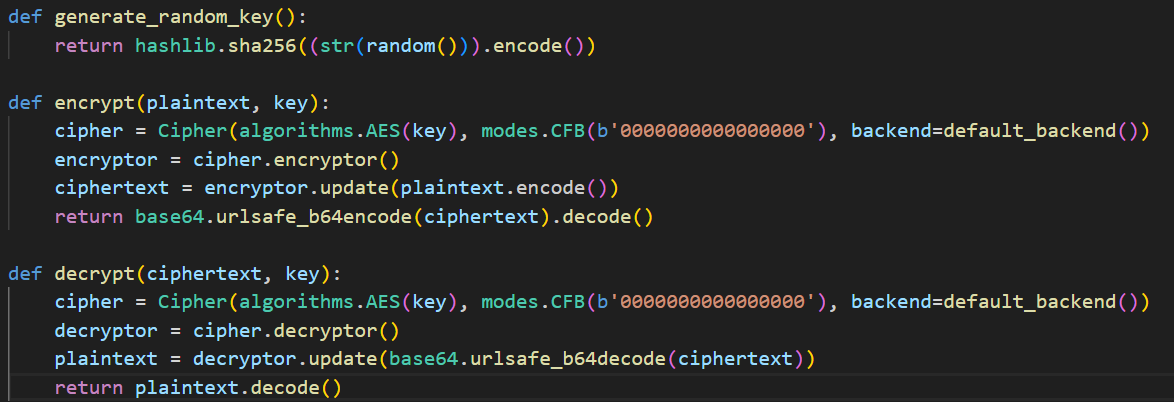
**Snippets of Code and Output**

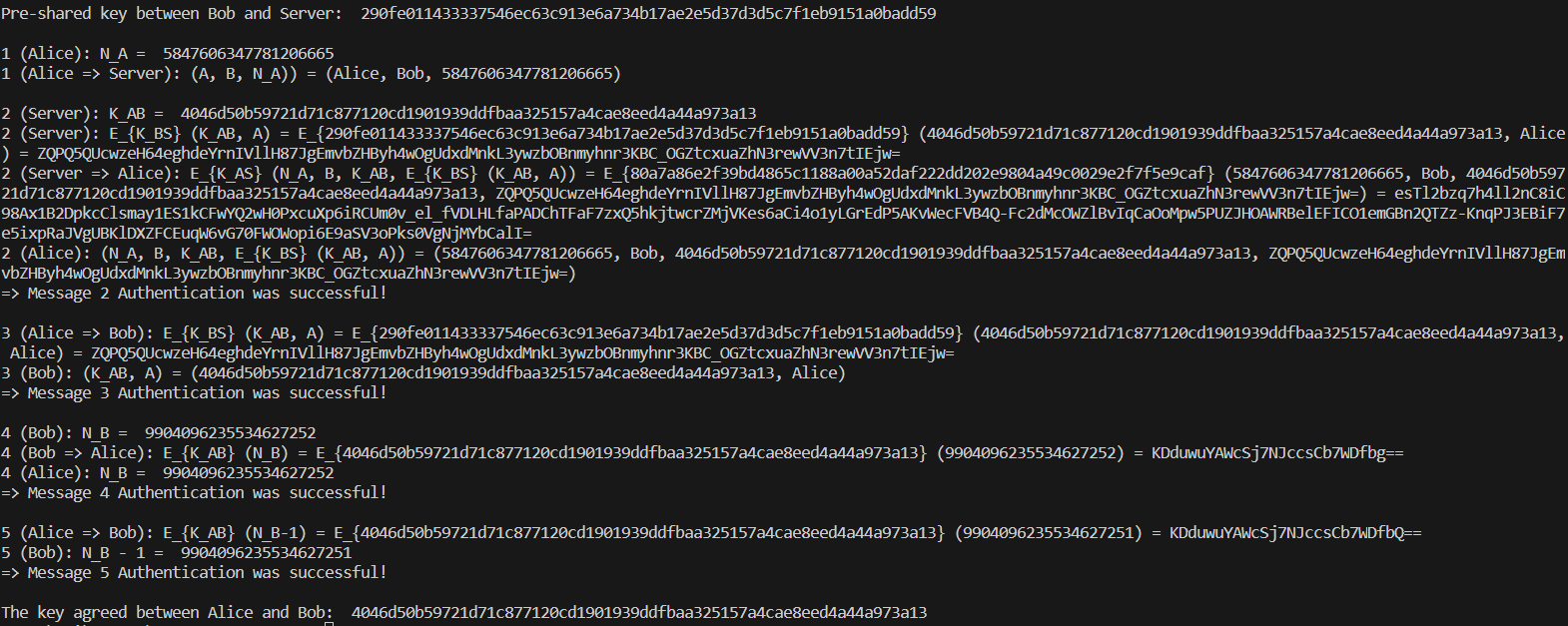
**Exercise 1**

****

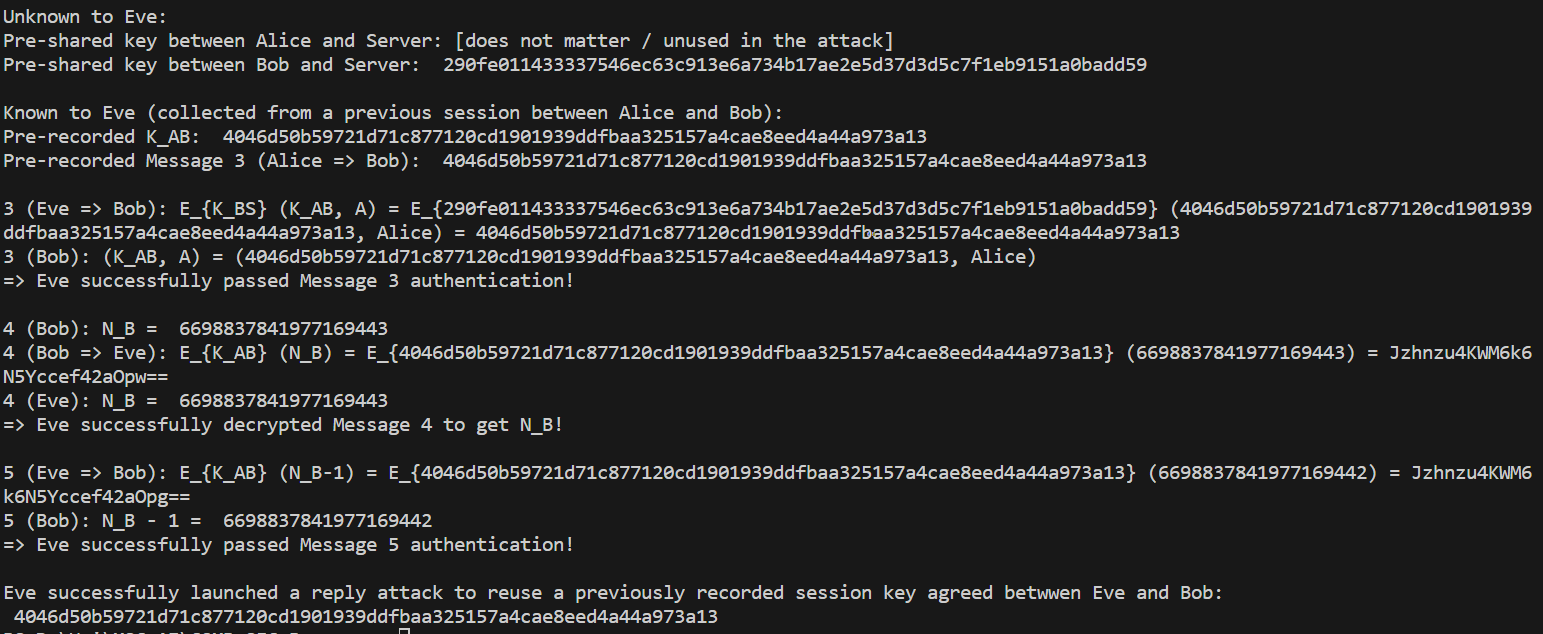
****

**Exercise 2**

****

****

**Exercise 3**

****

# Week 19 Class

Week 18 was about work on some exercises beyond user authentication to gain a better

understanding of authentication in the wider sense.

The following exercises were attempted: -

* Setting Linux file and folder permissions
* Investigating a real-world example of role-based access control
* Learning about same-origin policies (SOP) and cross-site scripting (XSS) attacks
* Playing with a sandbox
* Examining a real-world federated identity management (FIM) system

## How did I do the exercises and what did I learn about?

## Exercise 1 was attempted and completed through implementation of the same through Python 3.x. Exercises 2,3,4 and 5 were attempted and completed through research on windows system application and other applications mentioned to use.

## Exercise 1 was done by implementing a system that converts linux based file permission code into its octal representation. It understands if the size of the code is longer/shorter than the actual format and it it uses wrong characters or wrong order in the format.

Exercise 2 was done by .

Exercise 3 was done by.

Exercise 4 was done by.

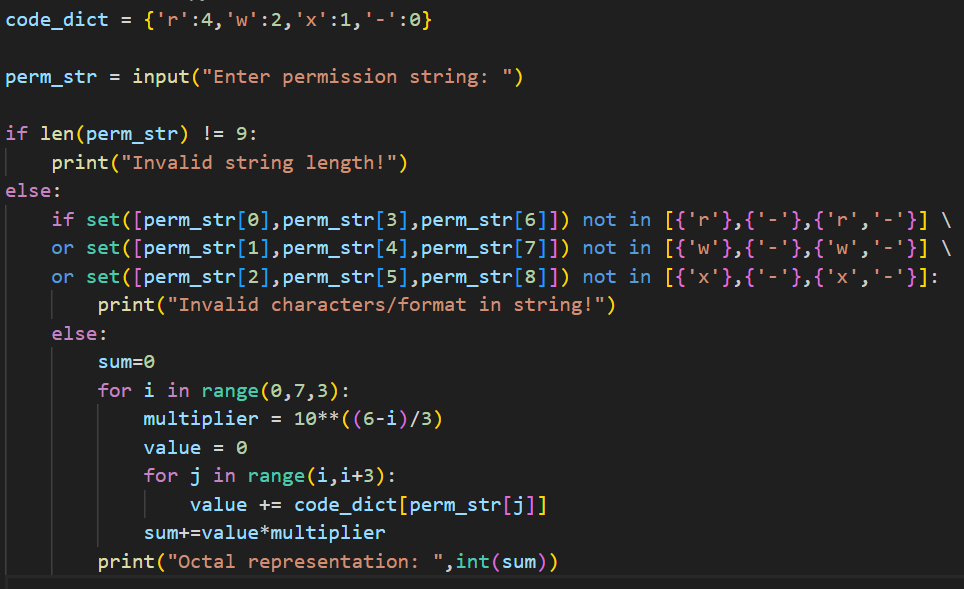
Exercise 5 was done by.

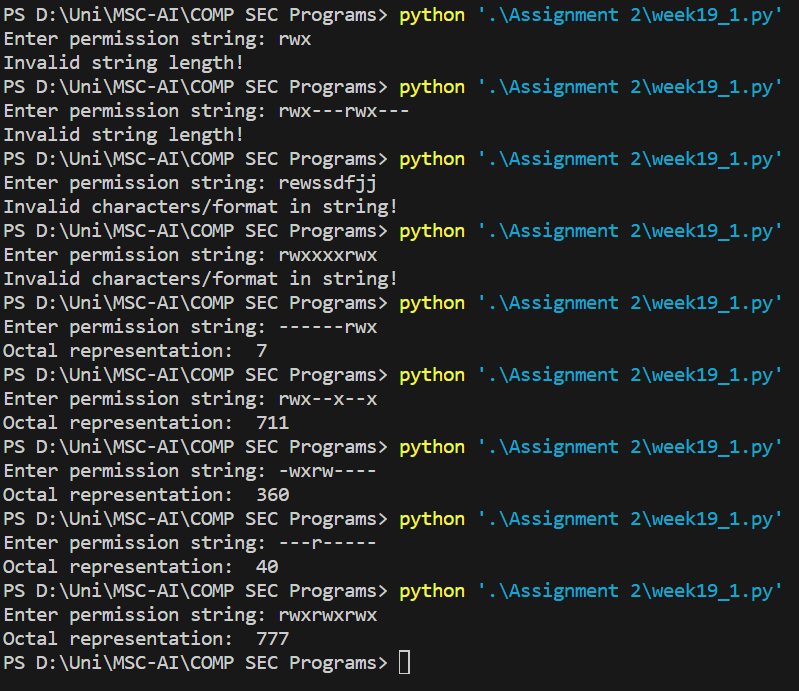
## What difficulties / problems did I encounter? / What observations and/or thoughts did you have on the exercises?

## Other than some syntax errors did not face much challenges in Exercise 1. Exercises 2-5 was able to attempt but there were some limitations within the system while doing research.

## My thoughts were that these were interesting exercises to demonstrate coding of permissions files in Linux as well as understand how XSS attacks on SOPs and various roles and their permissions in different applications of Windows system and beyond.

**Snippets of Code and Output of Exercise 1**

****

****