**ITEC 111**

A screenshot of a computer

Description automatically generated**Laboratory Report**

In this laboratory exercise, I learned how to use a brute-force method for guessing a 4-digit password by testing all possible combinations until the correct one was found. Brute-force, as I recall, is a technique often used in password-cracking attacks where each possible option is tried sequentially until the correct password is found.

For this lab, we were instructed to hardcode the password, so I set it to password = "1534". Next, I set up all the possible digits by defining a list called num\_list = ['1', '2', '3', '4', '5']. Then, I used nested for loops, with each loop representing one digit of the password. Each loop iterates through the list of possible digits, covering every combination of four digits.

For each combination, I created a 4-digit string guess to represent the attempted password using guess = i + j + k + l. I printed each attempted guess to monitor the brute-forcing process and see how the program cycles through possibilities. Finally, I used an if statement to check if guess was equal to the predefined password. If they matched, the program printed "Password found: {guess}", showing the correct password, and then exited the program to stop further attempts.

This exercise taught me the logic of brute-force attacks and how nested loops can systematically generate all possible combinations from a set of values. I also realized how computationally intensive this method can be, especially as the number of possible digits or password length increases.