OTP_System Details

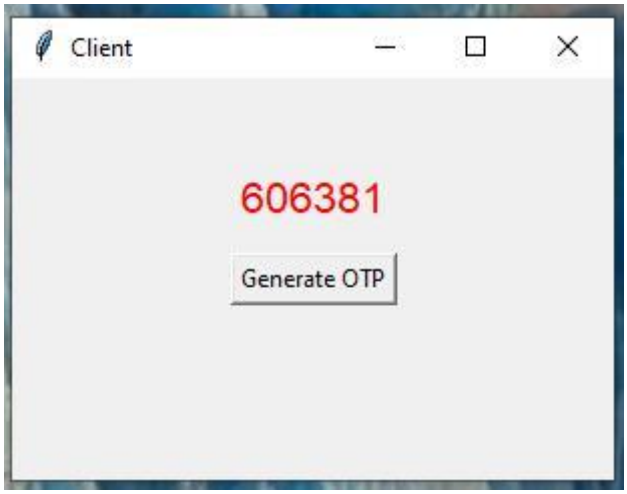
Develop an event based onetime password (OTP) system. The system consists of the following components:

1. A soft OTP token UI which consists of a push button and a display control. Clicking on the button will generate and display the onetime password.

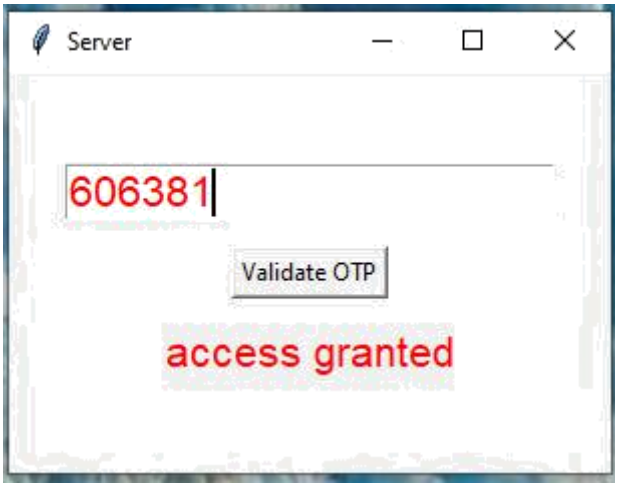
2. A test UI which will prompt the user to provide the OTP, show access granted message only if the right OTP is entered.

We have developed two UI's using python:

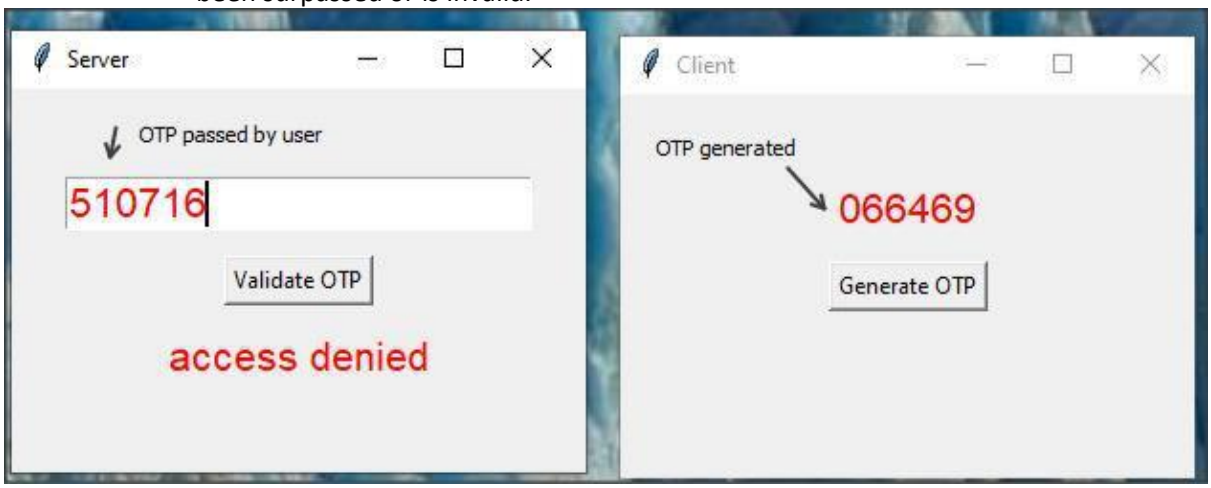
1. Soft OTP token UI which we assumed as Client, here the user will generate the OTP after clicking on the button.
    - We have implemented SHA256 for the feedback OTP algorithm in our code.
    - For the truncate function, we have taken the least significant 6 digits to get the OTP.



2. Test UI which we assumed as Server, the user will enter the generated OTP in the text field and validate the entered OTP by showing message as "access granted" or "access denied".
    - The "access granted" will be shown only when the generated and user-entered OTP matches. Refer below screenshot:



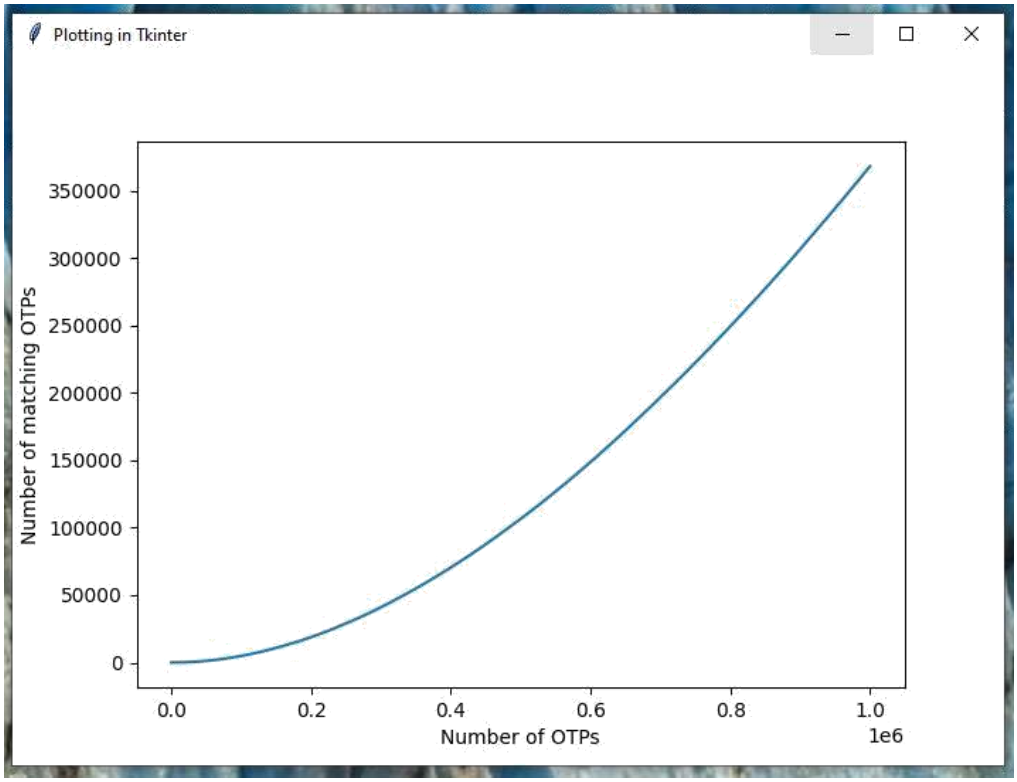
- The user will get “access denied” only when the user entered the OTP which has been surpassed or is invalid.



2. A study of the collision property. Generate 1,000,000 OTPs using your application. Show a graph describing how the collision properties evolve as the number of OTPs increases. Two metrics are calculated in N number of OTPs:

CR1: the number of matching OTPs in N.

A graph below describes the collision property to be evolved as the number of OTPs increases, the number of matching OTPs also increases.



CR2: the number of two consecutive OTPs in N (Optional +5%).

A graph below describes the collision property to be evolved as the number of OTPs increases, the number of two consecutive OTPs will also evolve.