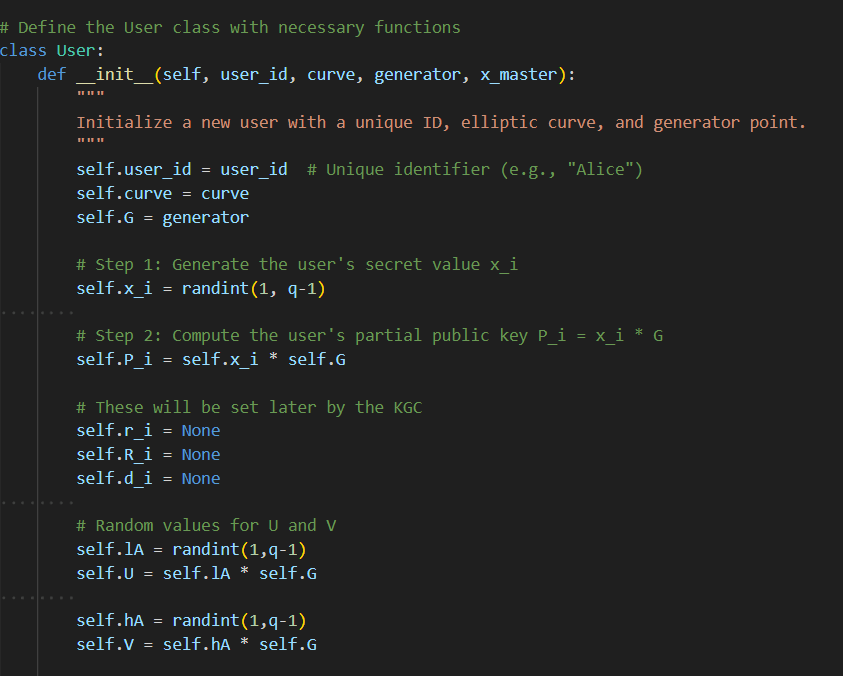
Tutorial – 9

Exercise – 1

I decided to create a class User and keep values like x\_i, P\_i and so on in it along with partial keys calculations and such.



Here we have user\_id as the unique ID for each user, curve and generators are the one already defined in the base file given to us.

Functions for partial key calculation

A computer screen shot of a computer code

Description automatically generated

Hash is calculated with user\_id, R\_i and P\_i and then d\_i is calculated.

A screen shot of a computer code

Description automatically generated

Function to calculate full keys.

A screen shot of a computer code

Description automatically generated

Initialising x\_master and Ppub\_master and user alice and bob.

Condition to create full keys also in class User

A screen shot of a computer program

Description automatically generated

Exercise – 2

A computer screen with text and symbols

Description automatically generated

Calculation of lA, hA, U and V (also done in class User)

A screenshot of a computer program

Description automatically generated

Function for computing Y and T, also printing KAB to check later.

AES encryption

A computer screen with text

Description automatically generated

Function for encapsulation

A screen shot of a computer program

Description automatically generated

Exercise – 3

A computer screen shot of text

Description automatically generated

Function to calculate Y and T again and check if they are the same.

Also, function to calculate KAB again as well and check if they match. Not sure why the H calculation needed to be done again, I skipped it.

Decryption using KAB\_reverse

A screen shot of a computer program

Description automatically generated

Working output

A computer screen shot of a computer code

Description automatically generated