|  |
| --- |
|  |
| Assignment 5 |
| Network Security (UCS727) |

|  |
| --- |
|  |

*Name:*  Sachleen Singh Chani

*Roll No.:* 101506143

*Date:* May 2021

## Q1. Write a program to implement the Diffie-Hellman key exchange algorithm.

### Answer:

**Code –**

#give public values q and alpha

#where alpha is the primitive root of q

q **=** 353

alpha **=** 3

**print(**"\nPublic access numbers q and alpha have values, q="**+str(**q**)+**" and alpha="**+str(**alpha**)+**"\n"**)**

#user A and B select their private key which shoulf be less than q and greater than 1

ar **=** **int(input(**"Select Private key for User A from set {2,3,...,"**+str(**q**-**2**)+**"}, AR="**))**

br **=** **int(input(**"Select Private key for User B from set {2,3,...,"**+str(**q**-**2**)+**"}, BR="**))**

#calcuation for public key of User A

**print(**"\n---Calculating the Public key for User A---"**)**

au **=** alpha**\*\***ar **%** q

**print(**"AU = ("**+str(**alpha**)+**"\*\*"**+str(**ar**)+**") MOD "**+str(**q**)+**" ="**,**au**)**

#public and private key of A

**print(**"\nThe Choosen Private key for User A, AR= "**+str(**ar**))**

**print(**"The calculated Public key for User A, AU= "**+str(**au**))**

#calcuation for public key of User A

**print(**"\n---Calculating the Public key for User B---"**)**

bu **=** alpha**\*\***br **%** q

**print(**"AU = ("**+str(**alpha**)+**"\*\*"**+str(**br**)+**") MOD "**+str(**q**)+**" ="**,**bu**)**

#public and private key of A

**print(**"\nThe Choosen Private key for User B, BR= "**+str(**br**))**

**print(**"The calculated Public key for User B, BU= "**+str(**bu**))**

#key exchange | A and B exchange public keys

**print(**"\n---User A and B exchange public numbers AU and BU---"**)**

**print(**"\n---Symmetric key calculation for user A from BU---"**)**

keyA **=** bu**\*\***ar **%** q

**print(**"KeyA = ("**+str(**bu**)+**"\*\*"**+str(**ar**)+**") MOD "**+str(**q**)+**" ="**,**keyA**)**

**print(**"\n---Symmetric key calculation for user B from AU---"**)**

keyB **=** au**\*\***br **%** q

**print(**"KeyB = ("**+str(**au**)+**"\*\*"**+str(**br**)+**") MOD "**+str(**q**)+**" ="**,**keyB**)**

**print(**"\nWe see that both KeyA and KeyB have the same value, thus keys have been exchanged!\n"**)**

**Result –**

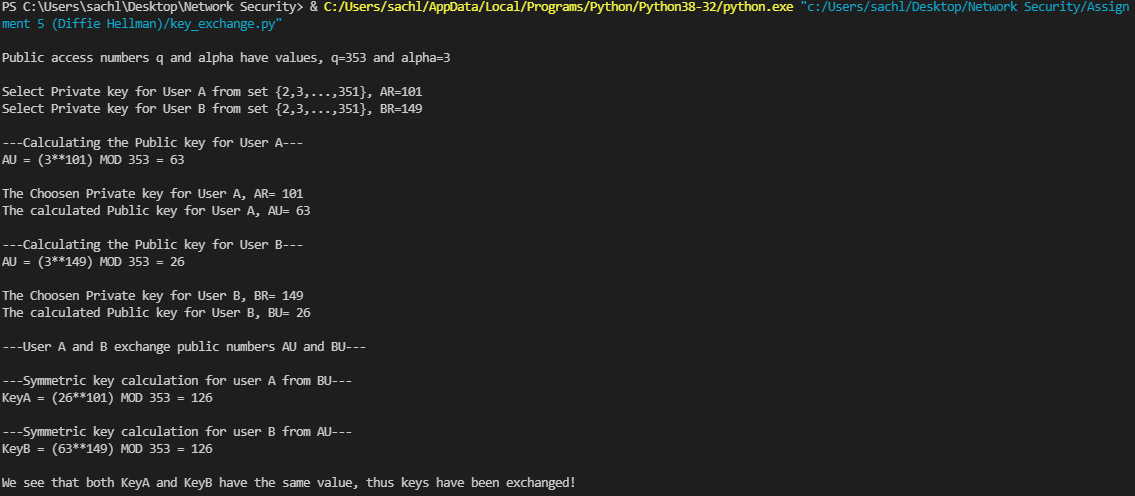


Figure 1 Result for Diffie- Hellman key exchange