Assignment B3

Roll No-41449

Title: Implementation of Diffie-Hellman key exchange

Problem Statement : Implementation of Diffie-Hellman key exchange

Objective : To understand how Diffie-Hellman key exchange algorithm works

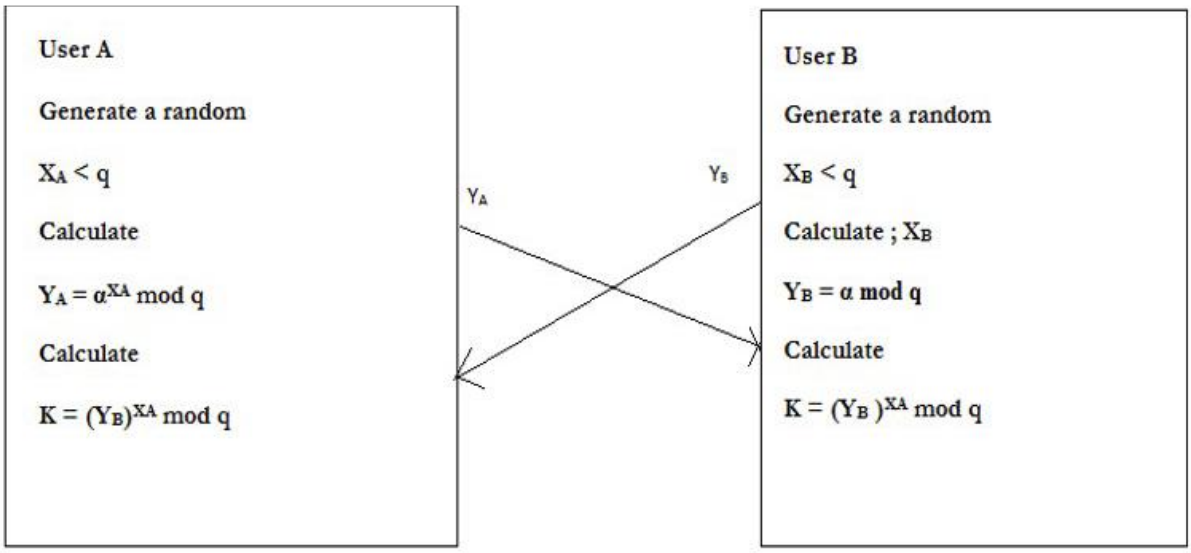
Outcome : Understanding and implementation of key distribution algorithm

Concept related Theory:

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel. Keys are not actually exchanged – they are jointly derived. It is named after their inventors Whitfield Diffie and Martin Hellman.

Silent Features of Diffie-Hellman key Exchange (DH)

1. Developed to address shortfalls of *key distribution* in symmetric key distribution.
2. A *key exchange algorithm*, not an encryption algorithm
3. Allows two users to share a *secret key* securely over a public network
4. Once the key has been shared Then both parties can use it to encrypt and decrypt messages using symmetric cryptography
5. Algorithm is based on “difficulty of calculating discrete logarithms in a finite field”
6. These keys are mathematically related to each other.
7. ‘’Using the public key of users, the session key is generated without transmitting the private key of the users.’’



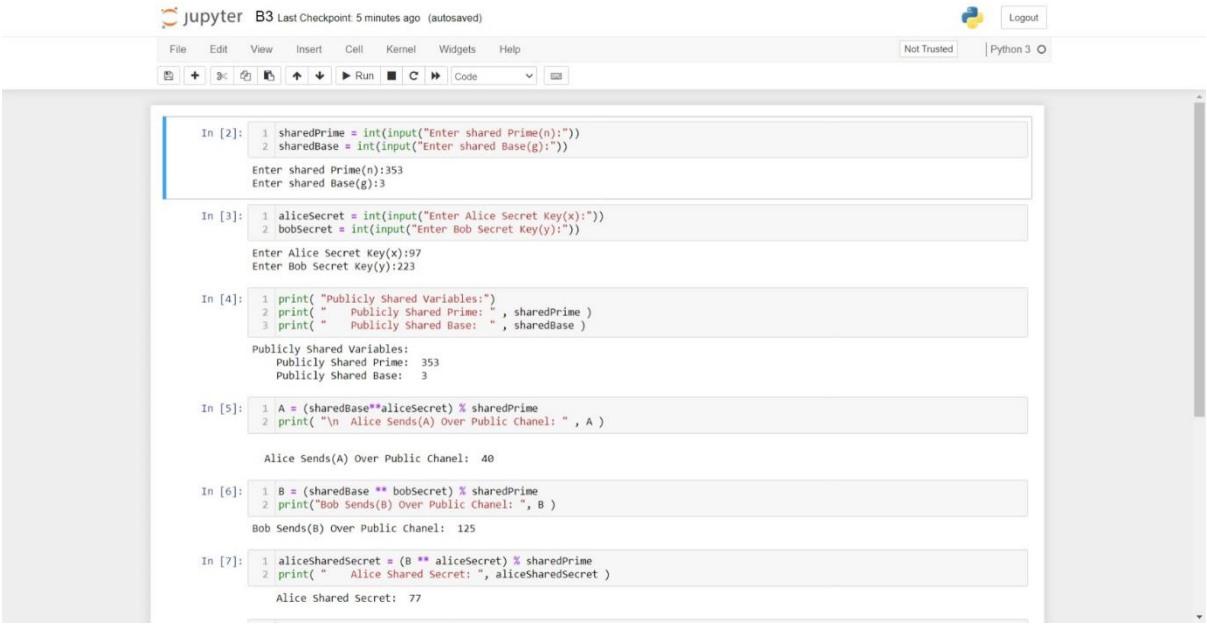
Diffie-Hellman Key exchange

1. Public values:large prime p, generator g (primitive root of p)
2. Alice has secret value x, Bob has secret y
3. Discrete logarithm problem:
   given x, g, and n, find A
4. A → B: $g^x \pmod n$
5. B → A: $g^y \pmod n$
6. Bob computes $(g^x)^y = g^{xy} \pmod n$
7. Alice computes $(g^y)^x = g^{xy} \pmod n$
8. Symmetric key= $g^{xy} \pmod n$

Conclusion:

Successfully implemented Diffie-Hellman key exchange

Result:


jupyter B3 Last Checkpoint: 5 minutes ago (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Not Trusted
Python 3
Run
Code
In [2]:
sharedPrime = int(input("Enter shared Prime(n):"))
sharedBase = int(input("Enter shared Base(g):"))
Enter shared Prime(n):353
Enter shared Base(g):3
In [3]:
aliceSecret = int(input("Enter Alice Secret Key(x):"))
bobSecret = int(input("Enter Bob Secret Key(y):"))
Enter Alice Secret Key(x):97
Enter Bob Secret Key(y):223
In [4]:
print("Publicly Shared Variables:")
print("   Publicly Shared Prime: " , sharedPrime)
print("   Publicly Shared Base: " , sharedBase)
Publicly Shared Variables:
Publicly Shared Prime: 353
Publicly Shared Base: 3
In [5]:
A = (sharedBase**aliceSecret) % sharedPrime
print("\n Alice Sends(A) Over Public Chanel: " , A)
Alice Sends(A) Over Public Chanel: 40
In [6]:
B = (sharedBase ** bobSecret) % sharedPrime
print("Bob Sends(B) Over Public Chanel: ", B)
Bob Sends(B) Over Public Chanel: 125
In [7]:
aliceSharedSecret = (B ** aliceSecret) % sharedPrime
print("   Alice Shared Secret: ", aliceSharedSecret)
Alice Shared Secret: 77