# Diffie Hellman Key Exchange(Implementation)

## Code

```
import java.util.*;

public class DiffieHellmanKeyExchange
{
  public static void main (String[]args)
  {
    Scanner sc = new Scanner (System.in);
    int publicNumberOne, publicNumberTwo, privateKeyOne, privateKeyTwo,
publicKeyOne, publicKeyTwo, symmetricKeyOne, symmetricKeyTwo;

      System.out.print("Enter person 1's public number: ");
      publicNumberOne = sc.nextInt();

      System.out.print("Enter person 2's public number: ");
      publicNumberTwo = sc.nextInt();

      System.out.print("Enter person 1's private key: ");
      privateKeyOne = sc.nextInt();

      System.out.print("Enter person 2's private key: ");
      privateKeyTwo = sc.nextInt();

    // System.out.println("Generating person 1's public key...");
    publicKeyOne = (int)Math.pow(publicNumberTwo,
privateKeyOne)%publicNumberOne;
    // System.out.println("Person 1's public key = " + publicKeyOne);

    // System.out.println("Generating person 2's public key...");
    publicKeyTwo = (int)Math.pow(publicNumberTwo,
privateKeyTwo)%publicNumberOne;
    // System.out.println("Person 2's public key = " + publicKeyTwo);

    // System.out.println("Generating symmetric key one...");
```

```
    symmetricKeyOne = (int)Math.pow(publicKeyTwo,
privateKeyOne)%publicNumberOne;

    // System.out.println("Generating symmetric key two...");
    symmetricKeyTwo = (int)Math.pow(publicKeyOne,
privateKeyTwo)%publicNumberOne;

    if(symmetricKeyOne == symmetricKeyTwo)
    {
        System.out.println("The shared secret is: " + symmetricKeyOne);
    }


  }
}
```

## Output

```
C:\Users\USER\OneDrive\Desktop\practicals\CSS\DiffieHellmanKeyExchange>javac DiffieHellmanKeyExchange.java

C:\Users\USER\OneDrive\Desktop\practicals\CSS\DiffieHellmanKeyExchange>java DiffieHellmanKeyExchange
Enter person 1's public number: 31
Enter person 2's public number: 5
Enter person 1's private key: 9
Enter person 2's private key: 3
The shared secret is: 1
```