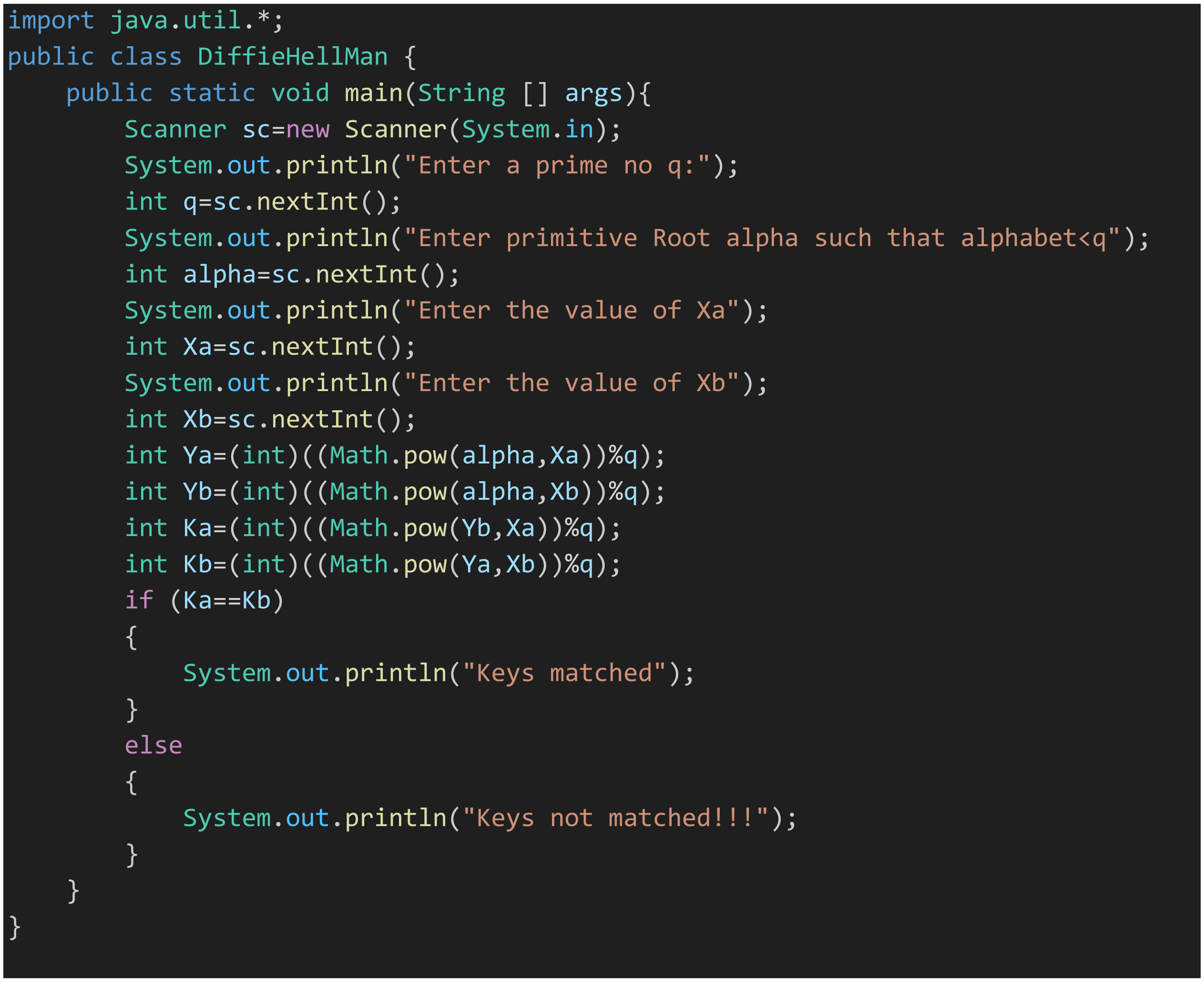
PRACTICAL 5

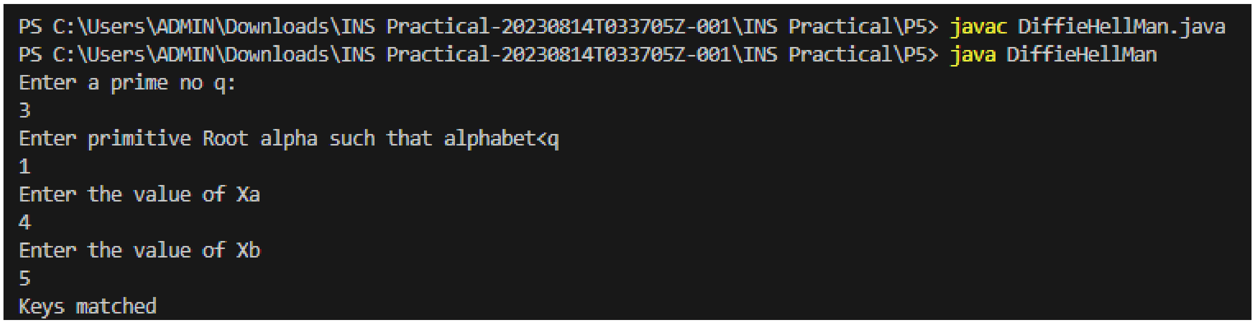
Aim: Write a program to implement Diffie-Hellman algorithm.

Code:



```java
import java.util.*;
public class DiffieHellMan {
    public static void main(String [] args){
        Scanner sc=new Scanner(System.in);
        System.out.println("Enter a prime no q:");
        int q=sc.nextInt();
        System.out.println("Enter primitive Root alpha such that alphabet<q");
        int alpha=sc.nextInt();
        System.out.println("Enter the value of Xa");
        int Xa=sc.nextInt();
        System.out.println("Enter the value of Xb");
        int Xb=sc.nextInt();
        int Ya=(int)((Math.pow(alpha,Xa))%q);
        int Yb=(int)((Math.pow(alpha,Xb))%q);
        int Ka=(int)((Math.pow(Yb,Xa))%q);
        int Kb=(int)((Math.pow(Ya,Xb))%q);
        if (Ka==Kb)
        {
            System.out.println("Keys matched");
        }
        else
        {
            System.out.println("Keys not matched!!!");
        }
    }
}
```

Output:



```
PS C:\Users\ADMIN\Downloads\INS Practical-20230814T033705Z-001\INS Practical\P5> javac DiffieHellMan.java
PS C:\Users\ADMIN\Downloads\INS Practical-20230814T033705Z-001\INS Practical\P5> java DiffieHellMan
Enter a prime no q:
3
Enter primitive Root alpha such that alphabet<q
1
Enter the value of Xa
4
Enter the value of Xb
5
Keys matched
```