Program and Output

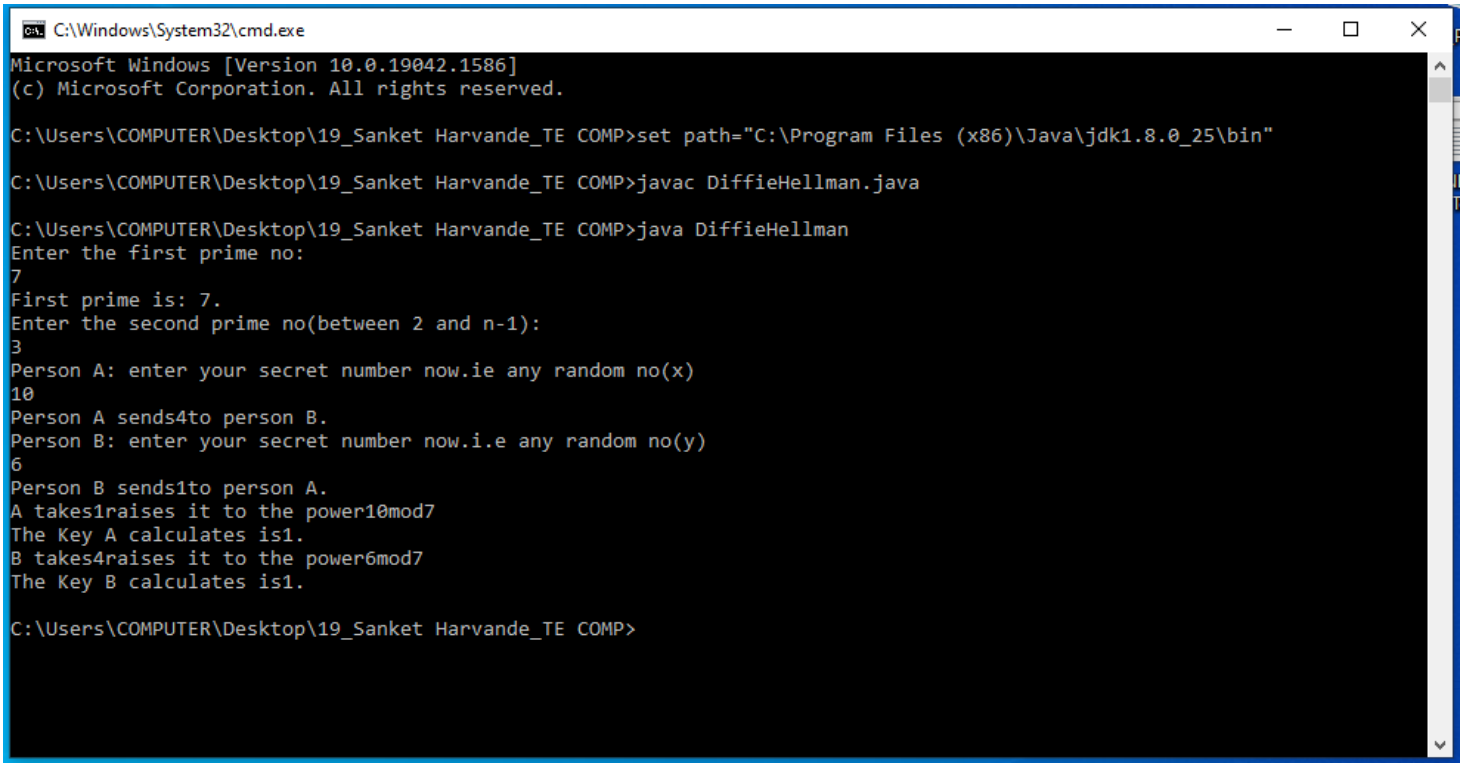
Program :

```
import java.util.*;

import java.math.BigInteger;

public class DiffieHellman {

final static BigInteger one = new BigInteger("1");
public static void main(String args[]) {

Scanner stdin=new Scanner(System.in);

BigInteger n;

// Get a start spot to pick a prime from the user.

System.out.println("Enter the first prime no:");

String ans=stdin.next();

n = getNextPrime(ans);

System.out.println("First prime is: "+n+".");

// Get the base for exponentiation from the user.

System.out.println("Enter the second prime no(between 2 and n-1):");

BigInteger g = new BigInteger(stdin.next());

// Get A's secret mumber.

System.out.println("Person A: enter your secret number now.ie any random
no(x)");

BigInteger a = new BigInteger(stdin.next());

// Make A's calculation.
```

```
BigInteger resulta = g.modPow(a, n);

// This is the value that will get sent from A to B.

// This value does NOT compromise the value of a easily.

System.out.println("Person A sends" + resulta +"to person B.");

// Get B's secret number.

System.out.println("Person B: enter your secret number now.i.e any random
no(y)");

BigInteger b= new BigInteger(stdin.next());

//Make B's calculation.

BigInteger resultb=g.modPow(b,n);

// This is the value that will get seat from B to A.

// This value does NOT compromise the value of beasily.

System.out.println("Person B sends" + resultb + "to person A.");

// Once A and B receive their values, they make their new calculations.

// This involved getting their new numbers and raising them to the // same
power as before, their secret number.

BigInteger KeyACalculates=resultb.modPow(a, n);

BigInteger KeyBCalculates=resulta.modPow(b, n);

// Print out the Key A calculates.

System.out.println("A takes" + resultb + "raises it to the power" +a+"mod"
+n);

System.out.println("The Key A calculates is" + KeyACalculates + ".");
```

```
// Print out the Key B calculates.

System.out.println("B takes" + resulta + "raises it to the power"+b+"mod" +
n);

System.out.println("The Key B calculates is" + KeyBCalculates + ".");

}

public static BigInteger getNextPrime(String ans) {

BigInteger test = new BigInteger(ans);

while (!test.isProbablePrime(99))

test=test.add(one);

return test;

}
}
```

Output :



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\COMPUTER\Desktop\19_Sanket Harvande_TE COMP>set path="C:\Program Files (x86)\Java\jdk1.8.0_25\bin"

C:\Users\COMPUTER\Desktop\19_Sanket Harvande_TE COMP>javac DiffieHellman.java

C:\Users\COMPUTER\Desktop\19_Sanket Harvande_TE COMP>java DiffieHellman
Enter the first prime no:
7
First prime is: 7.
Enter the second prime no(between 2 and n-1):
3
Person A: enter your secret number now.ie any random no(x)
10
Person A sends4to person B.
Person B: enter your secret number now.i.e any random no(y)
6
Person B sends1to person A.
A takes1raises it to the power10mod7
The Key A calculates is1.
B takes4raises it to the power6mod7
The Key B calculates is1.

C:\Users\COMPUTER\Desktop\19_Sanket Harvande_TE COMP>
```