Bansilal Ramnath Agarwal Charitable Trust’s

Vishwakarma Institute of Technology, Pune-37

(An autonomous Institute of Savitribai Phule Pune University)

Department of Computer Engineering

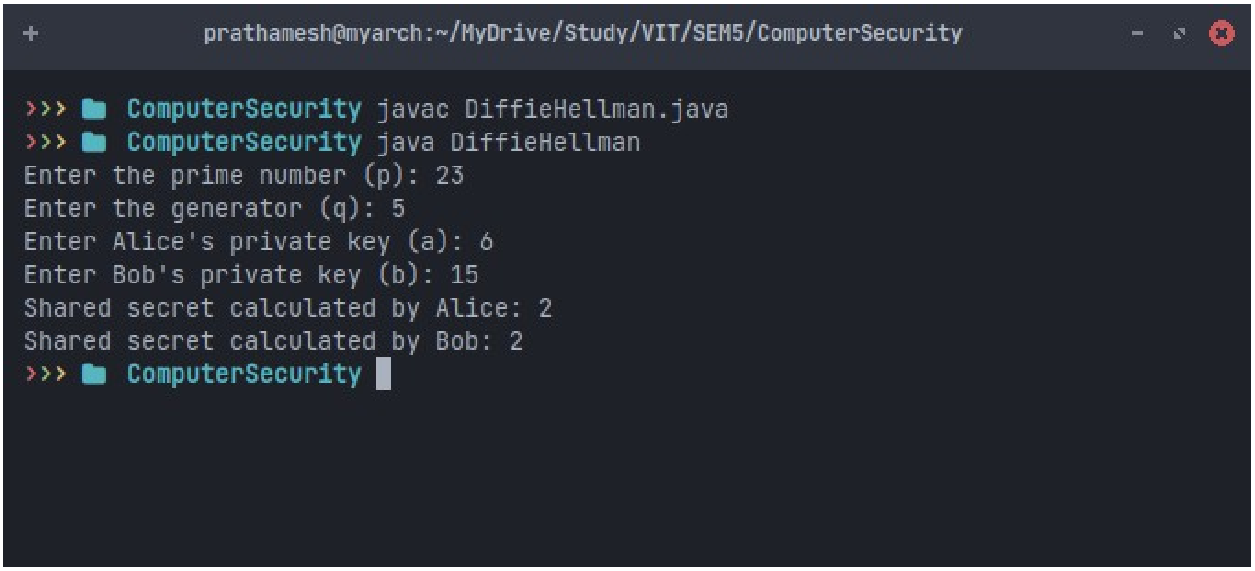
Name	Thakare Prathamesh Prabhakar
Batch	Batch - 2
PRN	12220016
Roll No	58
Division	CS-D
Subject	Cyber Security

Problem Statement: Implement Diffie HellmanAlgorithm.

Code:

```
import java.math.*;
import java.util.*;

public class DiffieHellman {

    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);

        System.out.print("Enter the prime number (p): ");
        BigInteger p = scanner.nextBigInteger();

        System.out.print("Enter the generator (q): ");
        BigInteger q = scanner.nextBigInteger();

        System.out.print("Enter Alice's private key (a): ");
        BigInteger a = scanner.nextBigInteger();

        System.out.print("Enter Bob's private key (b): ");
        BigInteger b = scanner.nextBigInteger();

        scanner.close();

        BigInteger aStar = q.modPow(a, p);
        BigInteger bStar = q.modPow(b, p);

        BigInteger sharedSecretA = bStar.modPow(a, p);
        BigInteger sharedSecretB = aStar.modPow(b, p);

        System.out.println("Shared secret calculated by Alice: " + sharedSecretA);
        System.out.println("Shared secret calculated by Bob: " + sharedSecretB);
    }
}
```

Output:



```
>>> 🗀 ComputerSecurity javac DiffieHellman.java
>>> 🗀 ComputerSecurity java DiffieHellman
Enter the prime number (p): 23
Enter the generator (q): 5
Enter Alice's private key (a): 6
Enter Bob's private key (b): 15
Shared secret calculated by Alice: 2
Shared secret calculated by Bob: 2
>>> 🗀 ComputerSecurity
```