

```

import java.util.Scanner;
public class DFH {
    public static void ComputeDF(double q, double p)
    {
//Step 2: Compute CipherKey for Alice and Bob
        Scanner sc = new Scanner(System.in);
        System.out.println("Enter private key for Alice:");
        double pvtAlice = sc.nextInt();
        System.out.println("Enter private key for Bob:");
        double pvtBob = sc.nextInt();
        double cipherKeyAlice, cipherKeyBob;
        cipherKeyAlice = Math.pow(p, pvtAlice) % q;
        cipherKeyBob = Math.pow(p, pvtBob) % q;
        //System.out.println("Cipher Key of Alice :"+cipherKeyAlice);
        //System.out.println("Cipher Key of Bob :"+cipherKeyBob);
//Step 3: Compute Shared Secret Key
        double SecretKeyAlice = Math.pow(cipherKeyBob, pvtAlice) % q;
        double SecretKeyBob = Math.pow(cipherKeyAlice, pvtBob) % q;
        if (SecretKeyAlice == SecretKeyBob)
        {
            System.out.println("Shared Secret Key = " + (int)SecretKeyAlice);
        }
        else
            System.out.println("Your values don't match. Please try again.");
        sc.close();
    }
    public static boolean checkForPrime(double inputNumber)
    {
        boolean isItPrime = true;
        if(inputNumber <= 1)
        {
            isItPrime = false;
            return isItPrime;
        }
        else
        {
            for (int i = 2; i <= inputNumber/2; i++)
            {
                if ((inputNumber % i) == 0)
                {
                    isItPrime = false;
                    break;
                }
            }
        }
    }
}

```

```

return isItPrime;
}
}
public static void main(String[] args) {
//Step 1 : take q and p as input
Scanner sc = new Scanner(System.in);
System.out.println("Enter value for q(prime no.)- ");
double q;
q = sc.nextInt();
boolean IsPrime = checkForPrime(q);
if (IsPrime)
{
System.out.println("Enter value for p(primitive root of q)- ");
double p;
p = sc.nextInt();
ComputeDF(q, p);
}
else
System.out.println("The value you entered for
is not a prime number. Please try again.");
}
}

```

```

java -cp /tmp/ouBULonosy DFH
Enter value for q(prime no.)-
13
Enter value for p(primitive root of q)- 6
Enter private key for Alice:
3
Enter private key for Bob:
10
Shared Secret Key = 12

```