**BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT**
**YELAHANKA, BENGALURU - 560064**

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

# Report on Diffie Hellman Algorithm

| | |
|---|---|
| **Name** | Raghavendra K M |
| **USN** | 1BY18IS093 |
| **Semester/Section** | 5B |
| **Course Code** | 18CSL57 |
| **Course Name** | Computer Network Laboratory |
| **Faculty** | Prof. Gireesh babu C N |
| **Title** | Diffie Hellman Algorithm |
| **Date** | 25-11-2020 |

**Signature of a Student** **Signature of a Faculty**

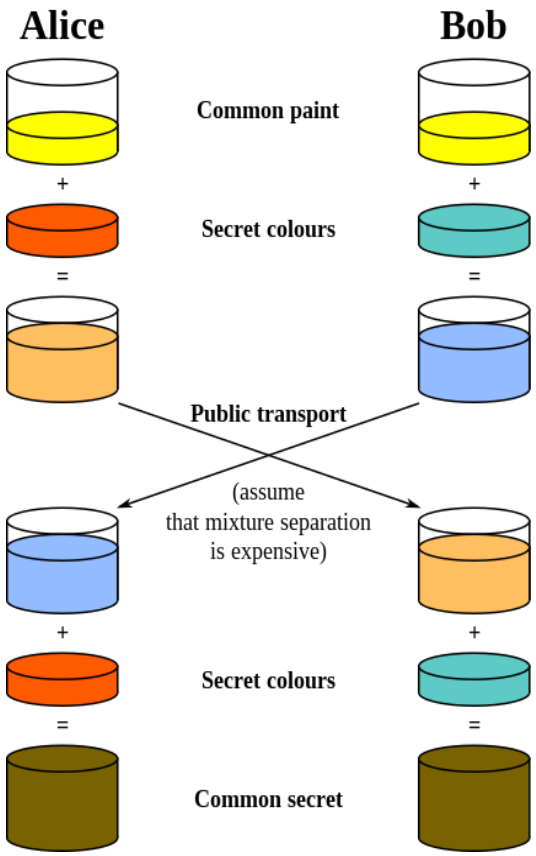
## Experiment No. 11

Write a Java Program to implement DH algorithm.

## Diffie Hellman algorithm Mechanism:

Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric key algorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric and asymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication.

## Pictorial Representation:




## Diffie Hellman (DH) Key Exchange Algorithm:

Step 1: Choose two prime numbers **g(primitive root of p)** and **p**.

Step 2: Alice selects a secret number (**a**) and computes $\mathbf{g^a}$ mod **p**, let's call it **A**.
Alice sends **A** to Bob.

Step 3: Bob selects a secret number (**b**) and computes $\mathbf{g^b}$ mod **p**, let's call it **B**.
Bob sends **B** to Alice.

Step 4: Alice computes **S_A** = $B^a$ mod p

Step 5: Bob computes **S_B** = $A^b$ mod p

Step 6: If **S_A** = **S_B** then Alice and Bob can agree for future communication.

## Source code:

DiffieHellman.java

```
import java.util.Scanner;

public class DiffieHellman {
    public static void main(String[] args) {
        Scanner scan = new Scanner(System.in);
        System.out.println("Enter modulo(p)");
        int p = scan.nextInt();
        System.out.println("Enter primitive root of " + p);
        int g = scan.nextInt();
        System.out.println("Choose 1st secret no(Alice)");
        int a = scan.nextInt();
        System.out.println("Choose 2nd secret no(BOB)");
        int b = scan.nextInt();
        int A = (int) Math.pow(g, a) % p;
        int B = (int) Math.pow(g, b) % p;
        int S_A = (int) Math.pow(B, a) % p;
        int S_B = (int) Math.pow(A, b) % p;
        if (S_A == S_B) {
            System.out.println
                ("ALice and Bob can communicate with each other!!!");
            System.out.println
                ("They share a secret no = " + S_A);
        } else {
            System.out.println
                ("ALice and Bob cannot communicate with each other!!!");
        }
    }
}
```

## Outputs:

```
C:\Windows\System32\cmd.exe

D:\1by18is093\ISE V SEM\Subjects\18CSL57 - Computer Network Laboratory\Diffie-Hellman algorithm>javac DiffieHellman.java

D:\1by18is093\ISE V SEM\Subjects\18CSL57 - Computer Network Laboratory\Diffie-Hellman algorithm>java DiffieHellman
Enter modulo(p)
5
Enter primitive root of 5
3
Choose 1st secret no(Alice)
13
Choose 2nd secret no(BOB)
15
ALice and Bob can communicate with each other!!!
They share a secret no = 2

D:\1by18is093\ISE V SEM\Subjects\18CSL57 - Computer Network Laboratory\Diffie-Hellman algorithm>
```