

EX.NO: 2.b)

ROLL.NO: 210701275

DATE:

Diffie Hellman Algorithm

AIM:

To Implement Diffie Hellman Algorithm to find the secret key

ALGORITHM:

1. Define large prime number p and a primitive root modulo p , denoted as g .
2. Party A selects a random private key a . Party B selects a random private key b .
3. Party A computes $A = g^a \bmod p$ Party B computes $B = g^b \bmod p$.
4. Parties A and B exchange their calculated public keys A and B with each other.
5. Party A computes $s = B^a \bmod p$. Party B computes $s = A^b \bmod p$.
6. Both parties now have the same shared secret s , which they can use as a symmetric encryption key for further communication.

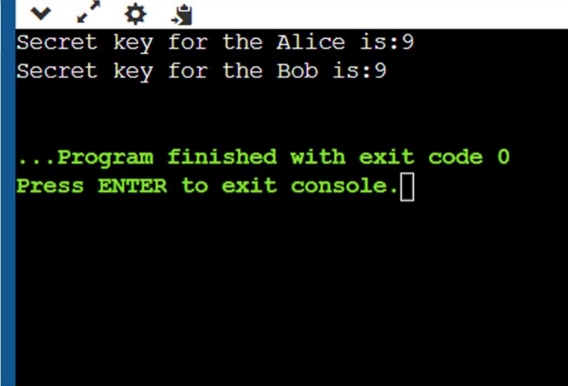
PROGRAM:

```
class Main {  
    private static long power(long a, long b, long p)  
    {  
        if (b == 1)  
            return a;  
        else  
            return (((long)Math.pow(a, b)) % p);  
    }  
    public static void main(String[] args)  
    {  
        long P, G, x, a, y, b, ka, kb;  
        P = 23;  
        G = 9;  
        a = 4;  
        x = power(G, a, P);  
        b = 3;  
        y = power(G, b, P);  
    }  
}
```

```
        ka = power(y, a, P); // Secret key for Alice
        kb = power(x, b, P); // Secret key for Bob

        System.out.println("Secret key for the Alice is:"
                            + ka);
        System.out.println("Secret key for the Bob is:"
                            + kb);
    }
}
```

OUTPUT:

A screenshot of a Java IDE's console window. The window has a title bar with standard icons (minimize, maximize, close, settings, and a document icon). The console area has a black background with white text. The output shows two lines: "Secret key for the Alice is:9" and "Secret key for the Bob is:9". Below these, there is a green message: "...Program finished with exit code 0" and a prompt "Press ENTER to exit console." followed by a cursor icon.

```
Secret key for the Alice is:9
Secret key for the Bob is:9

...Program finished with exit code 0
Press ENTER to exit console.
```

RESULT: