

## Program: Deffie Helman Key Exchange Algorithm

```
#include <stdio.h>

// Function to compute `a^m mod n`
int compute(int a, int m, int n)
{
    int r;

    int y = 1;
    while (m > 0)
    {
        r = m % 2;

        // fast exponention
        if (r == 1) {
            y = (y*a) % n;
        }

        a = a*a % n;
        m = m / 2;
    }

    return y;
}

int main()
{
    printf("Name:Vaibhav Mehar RollNo:58 Batch:B2\n");

    printf("Aim:To Implement Diffie Hellman key exchange algorithm\n\n");

    int p;

    printf("Enter Value of p: ");
    scanf("%d", &p);

    int g ;

    printf("Enter Value of g: ");
    scanf("%d", &g);

    int x, y;

    int A, B;

    printf("Enter Value of x (random no chosen by Alice): ");
```

```

scanf("%d", &x);

A = compute(g, x, p);

printf("Enter Value of y (random no chosen by by BOB): ");

scanf("%d", &y);

B = compute(g, y, p);

int keyA = compute(B, x, p);

int keyB = compute(A, y, p);

printf("value of R1 is: %d", A);

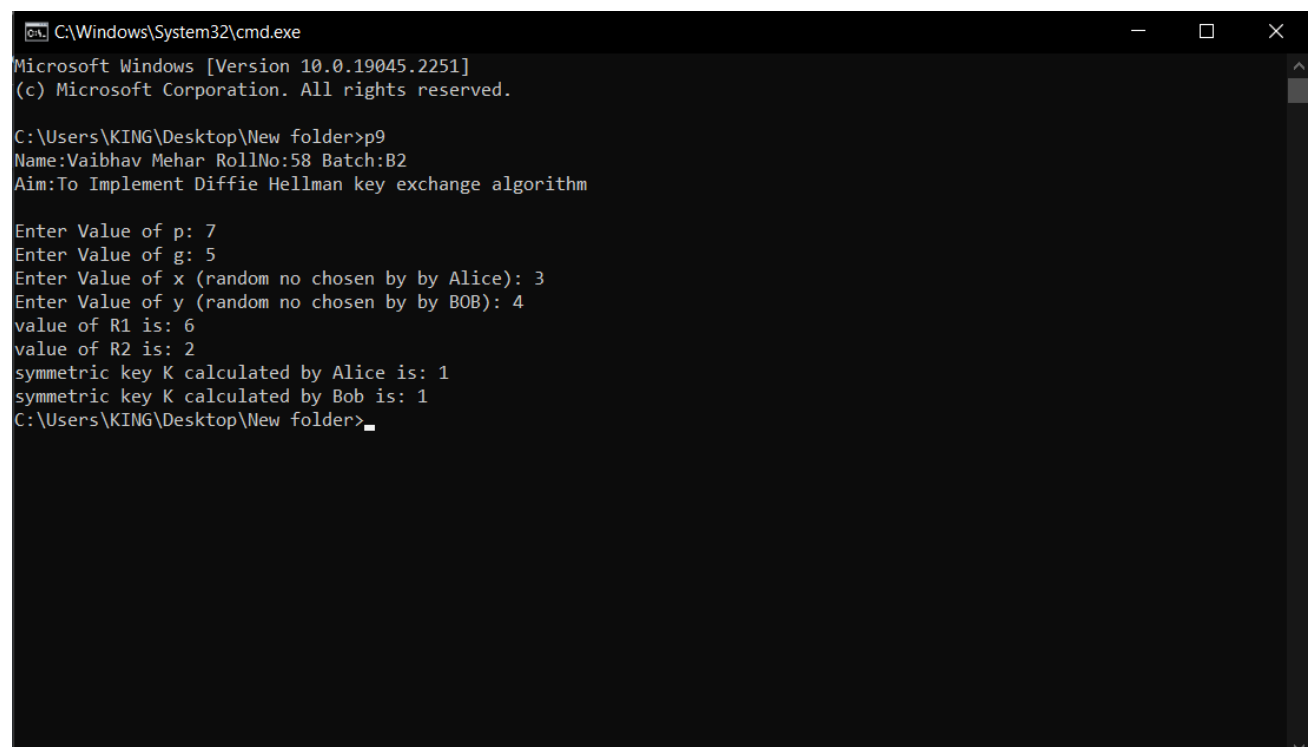
printf("\nvalue of R2 is: %d", B);

printf("\nsymmetric key K calculated by Alice is: %d\nsymmetric key K calculated by Bob is: %d",
keyA, keyB);

return 0;
}

```

### Output:



```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\KING\Desktop\New folder>p9
Name:Vaibhav Mehar RollNo:58 Batch:B2
Aim:To Implement Diffie Hellman key exchange algorithm

Enter Value of p: 7
Enter Value of g: 5
Enter Value of x (random no chosen by by Alice): 3
Enter Value of y (random no chosen by by BOB): 4
value of R1 is: 6
value of R2 is: 2
symmetric key K calculated by Alice is: 1
symmetric key K calculated by Bob is: 1
C:\Users\KING\Desktop\New folder>

```