Walchand College Of Engineering, Sangli

Department of Computer Science and Engineering

Subject: C&NS Lab

Batch: B4

Name: Gayatri Sopan Gade **PRN:2020BTECS00210**

Assignment: 11

Title:

Implementation of Diffie – Hellman Key Exchange Method

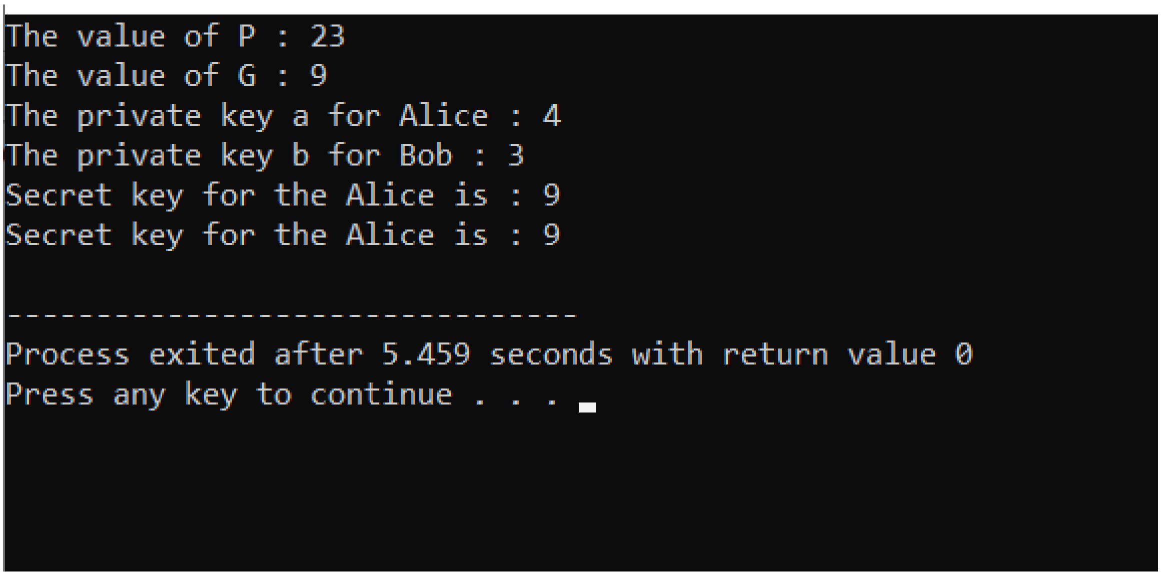
Implementation of Diffie - Hellman Key Exchange Algorithm

Code:

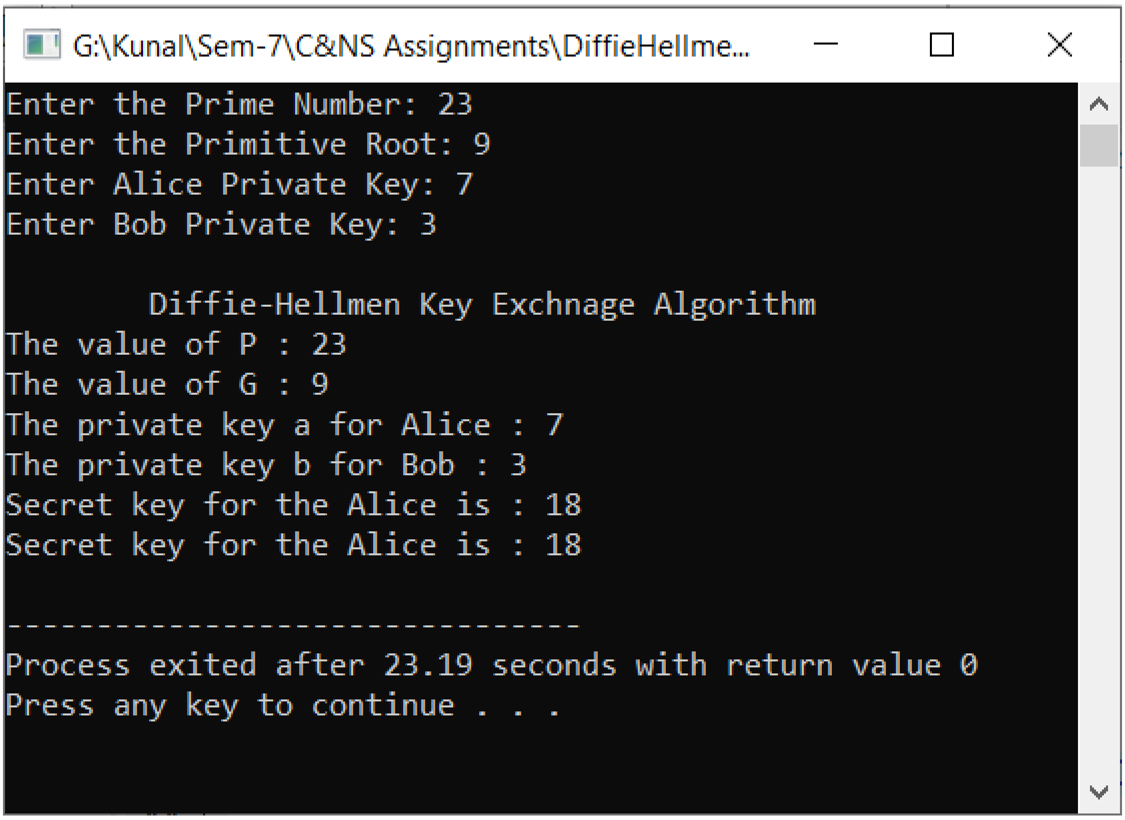
```
/* This program calculates the Key for two persons
using the Diffie-Hellman Key exchange algorithm using C++ */
#include <cmath>
#include <iostream>
using namespace std;

// Power function to return value of a ^ b mod P
long long int power(long long int a, long long int b,
                                        long long int P)
{
        if (b == 1)
                return a;

        else
                return (((long long int)pow(a, b)) % P);
}

// Driver program
```

```
int main()
{
        long long int P, G, x, a, y, b, ka, kb;

        // Both the persons will be agreed upon the
        // public keys G and P
        P = 23; // A prime number P is taken
        cout<<"Enter the Prime Number: ";
        cin>>P;

        G = 9; // A primitive root for P, G is taken'
        cout<<"Enter the Primitive Root: ";
        cin>>G;

        // Alice will choose the private key a
        a = 4; // a is the chosen private key
        cout<<"Enter Alice Private Key: ";
        cin>>a;

        // Bob will choose the private key b
        b = 3; // b is the chosen private key
        cout<<"Enter Bob Private Key: ";
        cin>>b;

        cout<<"\n\tDiffie-Hellmen Key Exchnage Algorithm\t\n";

        cout << "The value of P : " << P << endl;

        cout << "The value of G : " << G << endl;

        cout << "The private key a for Alice : " << a << endl;

        x = power(G, a, P); // gets the generated key

        cout << "The private key b for Bob : " << b << endl;
        y = power(G, b, P); // gets the generated key

        // Generating the secret key after the exchange
        // of keys
        ka = power(y, a, P); // Secret key for Alice
        kb = power(x, b, P); // Secret key for Bob
        cout << "Secret key for the Alice is : " << ka << endl;

        cout << "Secret key for the Alice is : " << kb << endl;

        return 0;
    }
```

Output:



```
The value of P : 23
The value of G : 9
The private key a for Alice : 4
The private key b for Bob : 3
Secret key for the Alice is : 9
Secret key for the Alice is : 9

--------------------------------
Process exited after 5.459 seconds with return value 0
Press any key to continue . . .
```



```
Enter the Prime Number: 23
Enter the Primitive Root: 9
Enter Alice Private Key: 7
Enter Bob Private Key: 3

        Diffie-Hellmen Key Exchnage Algorithm
The value of P : 23
The value of G : 9
The private key a for Alice : 7
The private key b for Bob : 3
Secret key for the Alice is : 18
Secret key for the Alice is : 18

--------------------------------
Process exited after 23.19 seconds with return value 0
Press any key to continue . . .
```

Conclusion:

Performed the experiment successfully.

The Diffie - Hellman theorem can be used to get the primitive number of the large Prime numbers