Name: Kate Shweta Sanjay
Roll No.: 3083
Div: B Batch: T4

```
#include <iostream>
#include <cmath>
using namespace std;

int power_modulo(int alpha, int exponent, int modulus)
{
   int result = 1;
   alpha = alpha % modulus;

   while (exponent > 0)
   {
      if (exponent % 2 == 1)
      {
         result = (result * alpha) % modulus;
      }

      alpha = (alpha * alpha) % modulus;
      exponent = exponent / 2;
   }
   return result;
}

void diffie_hellman()
{
   int q, alpha, private_key_A, private_key_B, public_key_A, public_key_B, secret_key_A,
secret_key_B;

   cout << "Enter the prime number q : ";
   cin >> q;

   cout << "Enter the value of alpha : ";
   cin >> alpha;

   cout << "Enter the private key of User A (Which should be less then q): ";
   cin >> private_key_A;

   cout << "Enter the private key of User B (Which should be less then q): ";
   cin >> private_key_B;

   public_key_A = power_modulo(alpha, private_key_A, q);
   public_key_B = power_modulo(alpha, private_key_B, q);
```

```
    cout << "Public key of User A: " << public_key_A;
    cout << "\nPublic key of User B: " << public_key_B;

    secret_key_A = power_modulo(public_key_B, private_key_A, q);
    secret_key_B = power_modulo(public_key_A, private_key_B, q);

    cout << "\nSecret Key for User A: " << secret_key_A << endl;
    cout << "Secret Key for User B: " << secret_key_B << endl;
}

int main()
{
    diffie_hellman();
    return 0;
}
```

Output:

```
D:\FSWD\Projects\04 Project>cd "d:\IS\IS Practical\" && g++ Exp6dh.cpp -o Exp6dh && "d:\IS\IS Practical\"Exp6dh
Enter the prime number q : 17
Enter the value of alpha : 3
Enter the private key of User A (Which should be less then q): 4
Enter the private key of User B (Which should be less then q): 6
Public key of User A: 13
Public key of User B: 15
Secret Key for User A: 16
Secret Key for User B: 16
```