**PRACTICAL - 05**

**Code:**

// Ashwin Navange A-38 CSE

#include <cmath>

#include <iostream>

#define ll long long int

using namespace std;

ll power(ll a, ll b,ll P)

{

if (b == 1)

return a;

else

return (((ll)pow(a, b)) % P);

}

int main()

{

cout << "Ashwin Navange A-38 CSE" << endl;

ll P, G, x, a, y, b, ka, kb;

P = 23;

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

G = 9;

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

a = 4;

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

b = 3;

cout << "The private key b for Bob : " << b << endl;

x = power(G, a, P);

y = power(G, b, P);

ka = power(y, a, P);

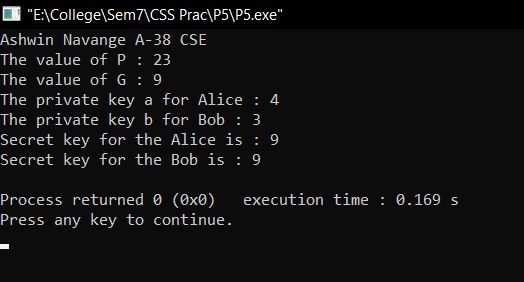
kb = power(x, b, P);

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

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

}

**Output:**

****