**Name: Pradyumna Bhosale**

**Roll Number : 20141224**

# **Experiment No: 6**

**Implementation Of Diffie Hellman Key exchange algorithm.**

#include <bits/stdc++.h>

using namespace std;

#define ll long long int

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

{

 if (b == 1)

 return a;

 else

 return (((ll)pow(a, b)) % P);

}

int main()

{

 cout<<"Implementation of Diffie-Hellman Algorithm\n";

 cout<<"20141224 Pradyumna Bhosale Exp-6\n";

 ll P, G, x, a, y, b, ka, kb;

 cout<<"Enter value of P\n";

 cin>>P;

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

 cout<<"Enter value of G\n";

 cin>>G;

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

 cout<<"Enter private key for alice\n";

 cin>>a;

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

 x = power(G, a, P);

 cout<<"Enter private key for b\n";

 cin>>b;

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

 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;

 return 0;

}

**Output:**

