**Name: Dhanraj Subhash Kore**

**Div : B Roll No: 60**

**Batch: B-3**

**Sub : CS LAB Assignment**

LAB 6 Implementation of ECC over Diffie Hellman Key Exchange Protocol

**Code:**

#include<stdio.h>

#include<math.h>

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);

}

int main()

{

long long int P, G, x, a, y, b, ka, kb;

P = 23;

printf("The value of P : %lld\n", P);

G = 9;

printf("The value of G : %lld\n\n", G);

a = 4;

printf("The private key a for Alice : %lld\n", a);

x = power(G, a, P);

b = 3;

printf("The private key b for Bob : %lld\n\n", b);

y = power(G, b, P);

ka = power(y, a, P);

kb = power(x, b, P);

printf("Secret key for the Alice is : %lld\n", ka);

printf("Secret Key for the Bob is : %lld\n", kb);

return 0;

}

**O/P:**

