Date :

**PRACTICAL-12**

**Objective** – WAP to implement Diffie Hellman Key Exchange..

**Code**-

#include <stdio.h>

long long int power(int a, int b, int mod)

{

long long int t;

if (b == 1)

return a;

t = power(a, b / 2, mod);

if (b % 2 == 0)

return (t \* t) % mod;

else

return (((t \* t) % mod) \* a) % mod;

}

long long int calculateKey(int a, int x, int n)

{

return power(a, x, n);

}

int main()

{

int n, g, x, a, y, b;

// both the persons will be agreed upon the common n and g

printf("Enter the value of n and g : ");

scanf("%d%d", &n, &g);

// first person will choose the x

printf("Enter the value of x for the first person : ");

scanf("%d", &x);

a = power(g, x, n);

// second person will choose the y

printf("Enter the value of y for the second person : ");

scanf("%d", &y);

b = power(g, y, n);

printf("key for the first person is : %lld\n", power(b, x, n));

printf("key for the second person is : %lld\n", power(a, y, n));

return 0;

}

**Output-**

