Information Security

Practical-7-1: Implement Diffi-Hellmen Key exchange Method.

CODE:

```
#include<stdio.h>
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;



printf("Enter the value For First Key N  : ");
scanf("%d",&n);
 printf("Enter the value For Second Key G  : ");
scanf("%d",&g);
printf("Enter the value of x for the first person : ");
scanf("%d",&x);  a=power(g,x,n);
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:

C:\Users\Arjun Vankani\Desktop\CE SEM 7\ASS\IS\Lab7\dell-man.exe

```
Enter the value For First Key N  : 23
Enter the value For Second Key G  : 5
Enter the value of x for the first person : 15
Enter the value of y for the second person : 6
key for the first person is : 2
key for the second person is : 2

--------------------------------
Process exited after 15.67 seconds with return value 0
Press any key to continue . . .
```