PRACTICAL-7

AIM: Write a C program to implement Diffie Hellman Key Exchange Algorithm.

INRODUCTION:

- Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel. Keys are not actually exchanged – they are jointly derived. It is named after their inventors Whitfield Diffie and Martin Hellman.

- If Alice and Bob wish to communicate with each other, they first agree between them a large prime number p, and a generator (or base) g (where 0 < g < p).

- Alice chooses a secret integer a (her private key) and then calculates g^a mod p (which is her public key). Bob chooses his private key b, and calculates his public key in the same way.

- Bob knows b and g^a, so he can calculate (g^a)^b mod p = g^ab mod p. Therefore both Alice and Bob know a shared secret g^ab mod p. An eavesdropper Eve who was listening in on the communication knows p, g, Alice’s public key (g^a mod p) and Bob’s public key (g^b mod p). She is unable to calculate the shared secret from these values.

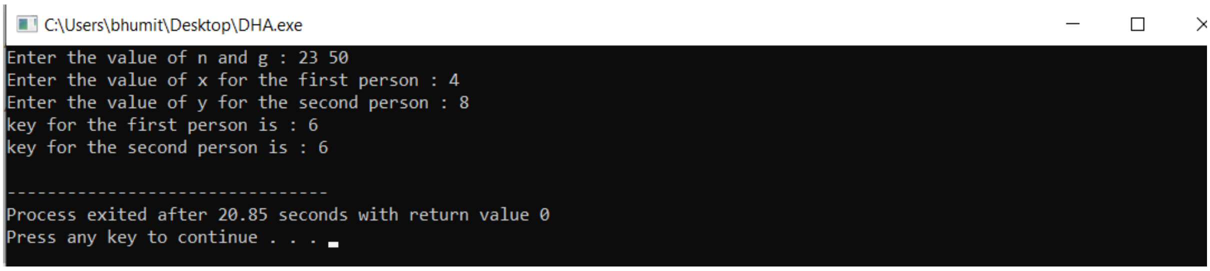
- In static-static mode, both Alice and Bob retain their private/public keys over multiple communications. Therefore the resulting shared secret will be the same every time. In ephemeral-static mode one party will generate a new private/public key every time, thus a new shared secret will be generated.

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;

// 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;     }
```

<u>OUTPUT</u>:



```
Enter the value of n and g : 23 50
Enter the value of x for the first person : 4
Enter the value of y for the second person : 8
key for the first person is : 6
key for the second person is : 6

--------------------------------
Process exited after 20.85 seconds with return value 0
Press any key to continue . . .
```