**Program 8th**

#include <stdio.h>

// Function to compute a^m mod n

int compute(int a, int m, int n)

{

int r;

int y = 1;

while (m > 0)

{

r = m % 2;

// fast exponention

if (r == 1)

y = (y\*a) % n;

a = a\*a % n;

m = m / 2;

}

return y;

}

// C program to demonstrate Diffie-Hellman algorithm

int main()

{

int p = 23; // modulus

int g = 5; // base

int a, b; // a - Alice's Secret Key, b - Bob's Secret Key.

int A, B; // A - Alice's Public Key, B - Bob's Public Key.

printf("the value of p and g are %d and %d\n",p,g);

// choose secret integer for Alice's Pivate Key (only known to Alice)

printf("enter alice's private key:");

scanf("%d",&a); // or use rand()

// Calculate Alice's Public Key (Alice will send A to Bob)

A = compute(g, a, p);

// choose secret integer for Bob's Pivate Key (only known to Bob)

printf("\nenter bob's key:");

scanf("%d",&b); // or use rand()

// Calculate Bob's Public Key (Bob will send B to Alice)

B = compute(g, b, p);

// Alice and Bob Exchanges their Public Key A & B with each other

// Find Secret key

int keyA = compute(B, a, p);

int keyB = compute(A, b, p);

printf("\nAlice's Secret Key is %d\nBob's Secret Key is %d\n", keyA, keyB);

return 0;

}

**OUTPUT**

