1. To implement Diffie-Hellman Key Exchange algorithm using C language

**Program:**

#include <stdio.h>

#include <stdlib.h>

#include <math.h>

int power(int a, int b, int p)

{

int res = 1;

while (b > 0)

{

if (b & 1)

res = (res \* a) % p;

a = (a \* a) % p;

b = b >> 1;

}

return res;

}

int main()

{

int p, g, a, b;

int A, B;

// read inputs from user

printf("Enter value of p: ");

scanf("%d", &p);

printf("Enter value of g: ");

scanf("%d", &g);

printf("Enter value of a: ");

scanf("%d", &a);

printf("Enter value of b: ");

scanf("%d", &b);

// Generate A and B

A = power(g, a, p);

B = power(g, b, p);

// Generate shared key for Alice

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

printf("Shared Key for Alice: %d\n", keyA);

// Generate shared key for Bob

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

printf("Shared Key for Bob: %d\n", keyB);

return 0;

}

