Program28 Write a C program for Diffie-Hellman protocol,

#include <stdio.h>

#include <math.h>

int mod\_exp(int base, int exp, int modulus)

{

int result = 1;

base = base % modulus;

while (exp > 0)

{

if (exp % 2 == 1)

{

result = (result \* base) % modulus;

}

exp = exp >> 1;

base = (base \* base) % modulus;

}

return result;

}

int main()

{

int prime = 23;

int base = 5;

int alicePrivateKey = 6;

int bobPrivateKey = 15;

int alicePublicKey = mod\_exp(base, alicePrivateKey, prime);

int bobPublicKey = mod\_exp(base, bobPrivateKey, prime);

printf("Alice's Public Key: %d\n", alicePublicKey);

printf("Bob's Public Key: %d\n", bobPublicKey);

int aliceSharedSecret = mod\_exp(bobPublicKey, alicePrivateKey, prime);

int bobSharedSecret = mod\_exp(alicePublicKey, bobPrivateKey, prime);

printf("Alice's Shared Secret: %d\n", aliceSharedSecret);

printf("Bob's Shared Secret: %d\n", bobSharedSecret);

return 0;

}OUTPUT:

Alice's Public Key: 8

Bob's Public Key: 19

Alice's Shared Secret: 2

Bob's Shared Secret: 2