Name: Sohel Momin

Roll No:1513126/a4

CSS EXPERIMENT 6

**Program:**

%% Diffie-Hellman Key exchange

% Available public keys -> p (prime no) and g(primitive modulo of p)

% private key of 1st party -> a

% private key of 2nd party -> b

clc;clear variables;close all;

%% Define the public,private keys

p = 23; %public (prime) modulus

g = 5; %public (prime) base

a = input('Enter the private key of 1st party ->');

b = input('Enter the private key of 2nd party ->');

%% Exchange of generated keys

A = mod(g^a,p);

B = mod(g^b,p);

%% Generation of the symmetric key at both sides

s\_a = mod(B^a,p);

s\_b = mod(A^b,p);

if s\_a == s\_b

fprintf('The Diffie-Hellman Key exchange was successful with the generated key as ->%d\n',s\_a);

end

**Output:**

Enter the private key of 1st party ->4

Enter the private key of 2nd party ->9

The Diffie-Hellman Key exchange was successful with the generated key as ->13