DAY-5

P. Salma

192110570

1. Write a C program for Diffie-Hellman protocol, each participant selects a secret number x and sends

The other participant ax mod q for some public number a. What would happen if the participants Sent

each other xa for some public number a instead? Give at least one method Alice and Bob could use to

Agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the Secret

Numbers?

Code:

#include <stdio.h>

#define V 5

int path[V];

int isSafe(int v, int graph[V][V], int path[], int pos) {

if (graph[path[pos - 1]][v] == 0)

return 0;

for (int i = 0; i < pos; i++)

if (path[i] == v)

return 0;

return 1;

}

int hamiltonianCycleUtil(int graph[V][V], int path[], int pos) {

if (pos == V) {

if (graph[path[pos - 1]][path[0]] == 1)

return 1;

else

return 0;

}

for (int v = 1; v < V; v++) {

if (isSafe(v, graph, path, pos)) {

path[pos] = v;

if (hamiltonianCycleUtil(graph, path, pos + 1))

return 1;

path[pos] = -1;

}

}

return 0;

}

int hamiltonianCycle(int graph[V][V]) {

for (int i = 0; i < V; i++)

path[i] = -1;

path[0] = 0;

if (hamiltonianCycleUtil(graph, path, 1) == 0) {

printf("No Hamiltonian Cycle found.\n");

return 0;

}

printf("Hamiltonian Cycle: ");

for (int i = 0; i < V; i++)

printf("%d ", path[i]);

printf("%d\n", path[0]);

return 1;

}

int main() {

int graph[V][V] = {

{0, 1, 0, 1, 0},

{1, 0, 1, 1, 1},

{0, 1, 0, 0, 1},

{1, 1, 0, 0, 1},

{0, 1, 1, 1, 0},

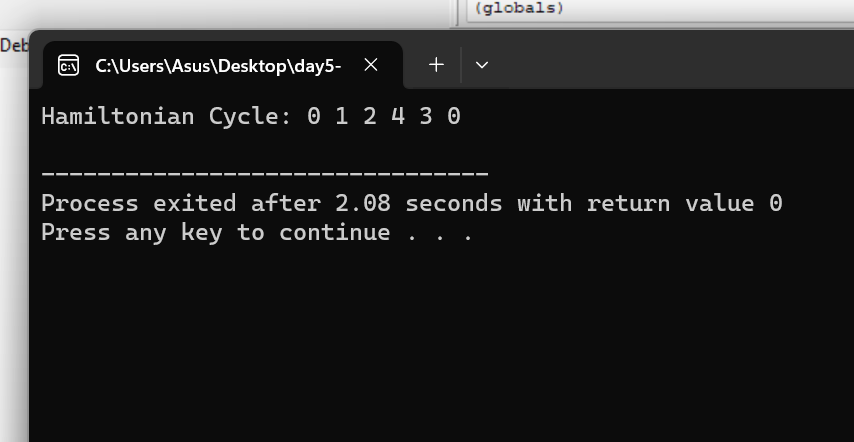
};

hamiltonianCycle(graph);

return 0;

}

Output:



1. Write a C program for SHA-3 option with a block size of 1024 bits and assume that each of the lanes

in the first message block (P0) has at least one nonzero bit. To start, all of the lanes in the internal state

matrix that correspond to the capacity portion of the initial state are all zeros. Show how long it will take

before all of these lanes have at least one nonzero bit. Note: Ignore the permutation. That is, keep track of

the original zero lanes even after they have changed position in the matrix.

Code: