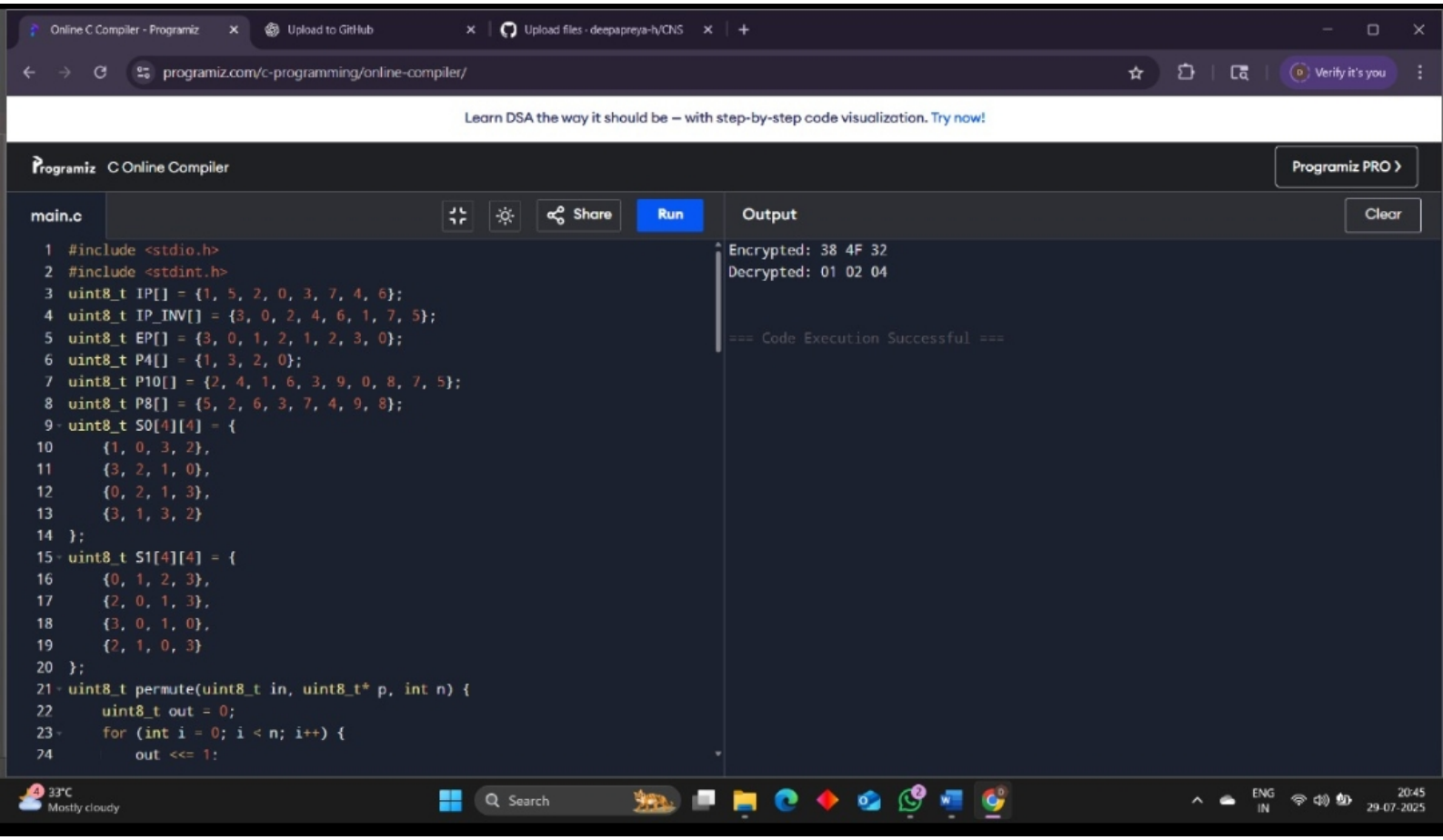
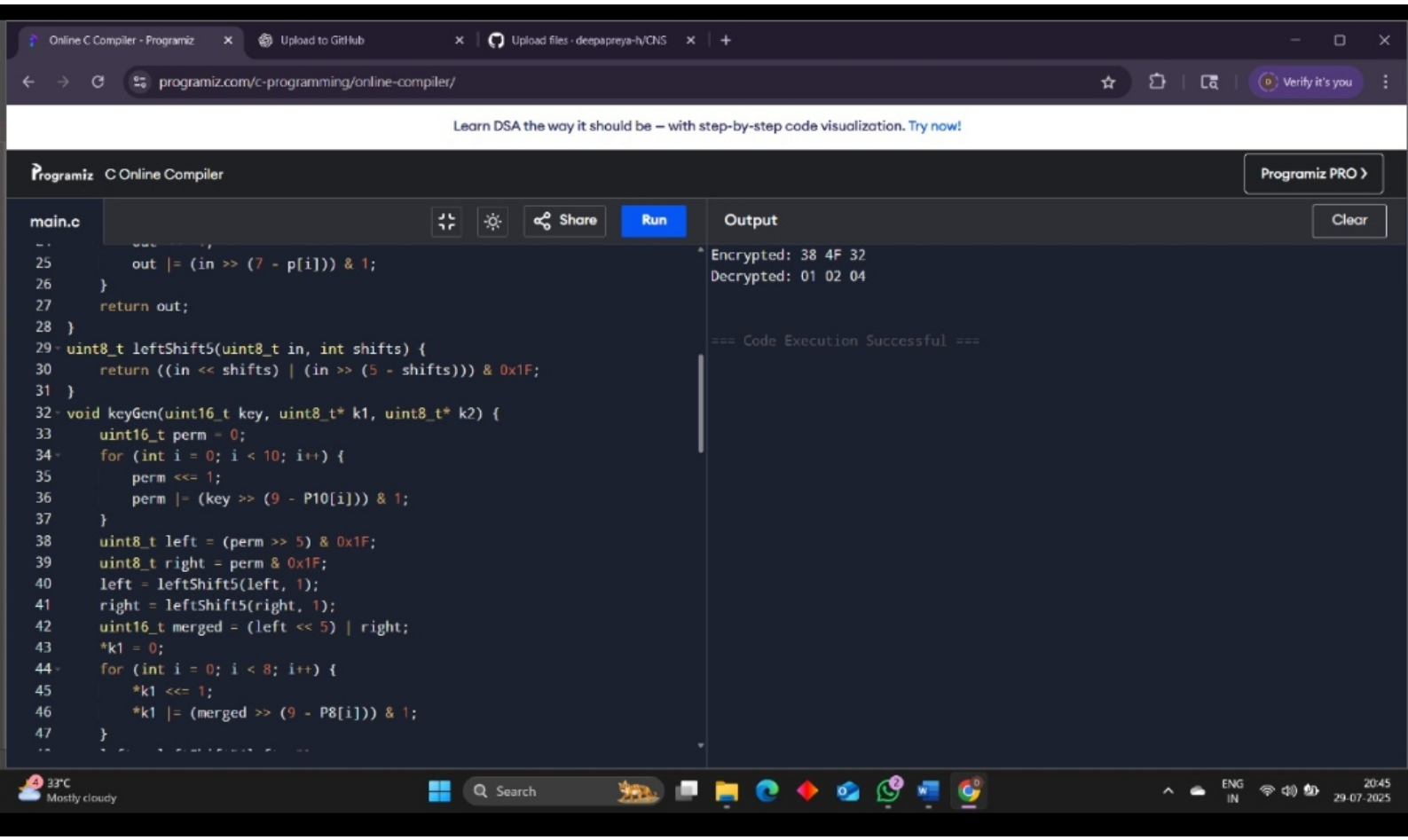
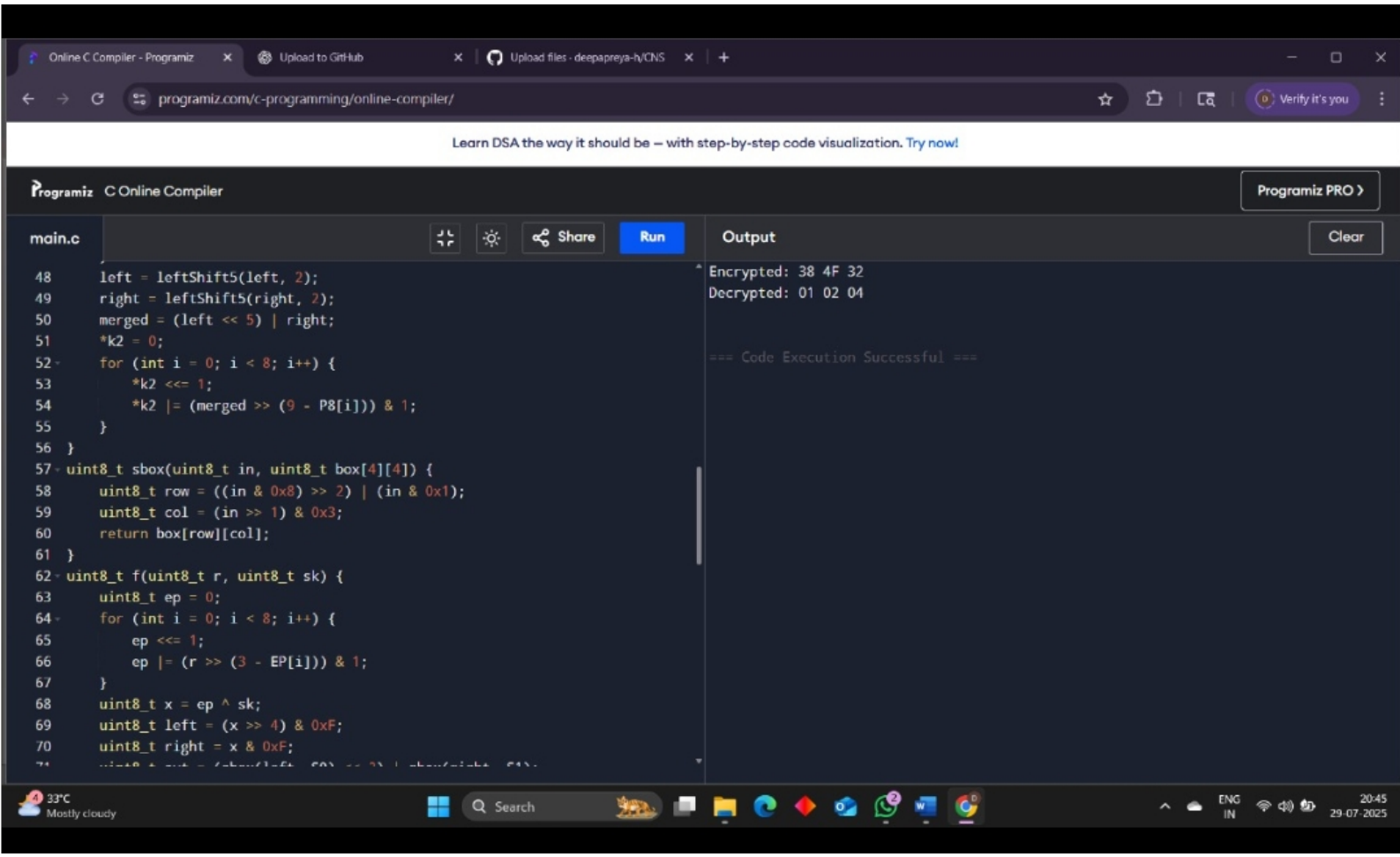
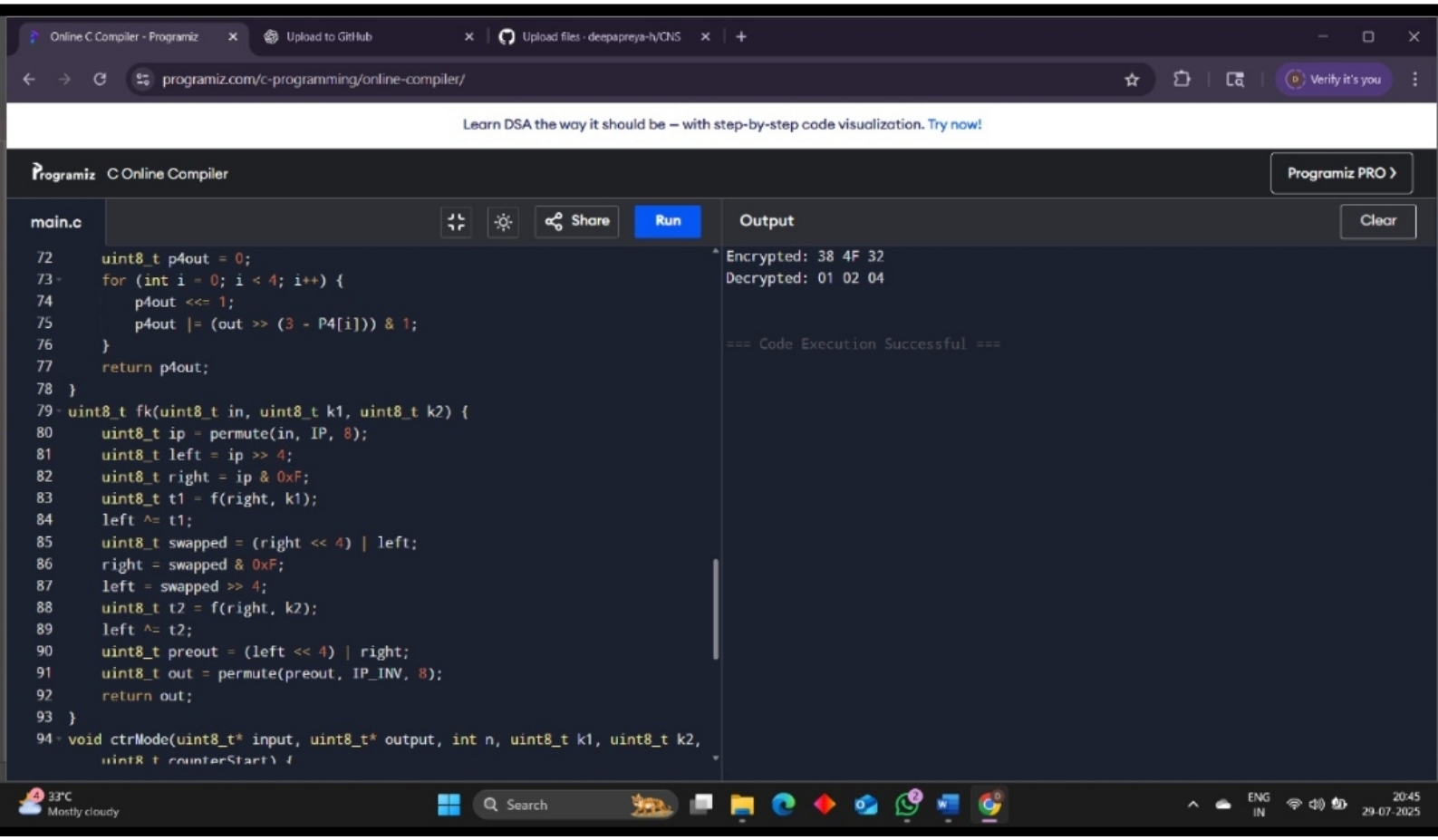

Online C Compiler - Programiz
Upload to GitHub
Upload files · deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <stdint.h>
uint8_t IP[] = {1, 5, 2, 0, 3, 7, 4, 6};
uint8_t IP_INV[] = {3, 0, 2, 4, 6, 1, 7, 5};
uint8_t EP[] = {3, 0, 1, 2, 1, 2, 3, 0};
uint8_t P4[] = {1, 3, 2, 0};
uint8_t P10[] = {2, 4, 1, 6, 3, 9, 0, 8, 7, 5};
uint8_t P8[] = {5, 2, 6, 3, 7, 4, 9, 8};
uint8_t S0[4][4] = {
{1, 0, 3, 2},
{3, 2, 1, 0},
{0, 2, 1, 3},
{3, 1, 3, 2}
};
uint8_t S1[4][4] = {
{0, 1, 2, 3},
{2, 0, 1, 3},
{3, 0, 1, 0},
{2, 1, 0, 3}
};
uint8_t permute(uint8_t in, uint8_t* p, int n) {
uint8_t out = 0;
for (int i = 0; i < n; i++) {
out <<= 1;
Encrypted: 38 4F 32
Decrypted: 01 02 04
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
20:45
29-07-2025


Online C Compiler - Programiz
Upload to GitHub
Upload files · deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
out |= (in >> (7 - p[i])) & 1;
}
return out;
}
uint8_t leftShift5(uint8_t in, int shifts) {
return ((in << shifts) | (in >> (5 - shifts))) & 0x1F;
}
void keyGen(uint16_t key, uint8_t* k1, uint8_t* k2) {
uint16_t perm = 0;
for (int i = 0; i < 10; i++) {
perm <<= 1;
perm |= (key >> (9 - P10[i])) & 1;
}
uint8_t left = (perm >> 5) & 0x1F;
uint8_t right = perm & 0x1F;
left = leftShift5(left, 1);
right = leftShift5(right, 1);
uint16_t merged = (left << 5) | right;
*k1 = 0;
for (int i = 0; i < 8; i++) {
*k1 <<= 1;
*k1 |= (merged >> (9 - P8[i])) & 1;
}
Encrypted: 38 4F 32
Decrypted: 01 02 04
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
20:45
29-07-2025


Online C Compiler - Programiz
Upload to GitHub
Upload files - deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
48 left = leftShift5(left, 2);
49 right = leftShift5(right, 2);
50 merged = (left << 5) | right;
51 *k2 = 0;
52 for (int i = 0; i < 8; i++) {
53 *k2 <<= 1;
54 *k2 |= (merged >> (9 - P8[i])) & 1;
55 }
56 }
57 uint8_t sbox(uint8_t in, uint8_t box[4][4]) {
58 uint8_t row = ((in & 0x8) >> 2) | (in & 0x1);
59 uint8_t col = (in >> 1) & 0x3;
60 return box[row][col];
61 }
62 uint8_t f(uint8_t r, uint8_t sk) {
63 uint8_t ep = 0;
64 for (int i = 0; i < 8; i++) {
65 ep <<= 1;
66 ep |= (r >> (3 - EP[i])) & 1;
67 }
68 uint8_t x = ep ^ sk;
69 uint8_t left = (x >> 4) & 0xF;
70 uint8_t right = x & 0xF;
Encrypted: 38 4F 32
Decrypted: 01 02 04
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
20:45
29-07-2025


Online C Compiler - Programiz
Upload to GitHub
Upload files · deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
uint8_t p4out = 0;
for (int i = 0; i < 4; i++) {
p4out <<= 1;
p4out |= (out >> (3 - P4[i])) & 1;
}
return p4out;
}
uint8_t fk(uint8_t in, uint8_t k1, uint8_t k2) {
uint8_t ip = permute(in, IP, 8);
uint8_t left = ip >> 4;
uint8_t right = ip & 0xF;
uint8_t t1 = f(right, k1);
left ^= t1;
uint8_t swapped = (right << 4) | left;
right = swapped & 0xF;
left = swapped >> 4;
uint8_t t2 = f(right, k2);
left ^= t2;
uint8_t preout = (left << 4) | right;
uint8_t out = permute(preout, IP_INV, 8);
return out;
}
void ctrMode(uint8_t* input, uint8_t* output, int n, uint8_t k1, uint8_t k2,
Encrypted: 38 4F 32
Decrypted: 01 02 04
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
20:45
29-07-2025