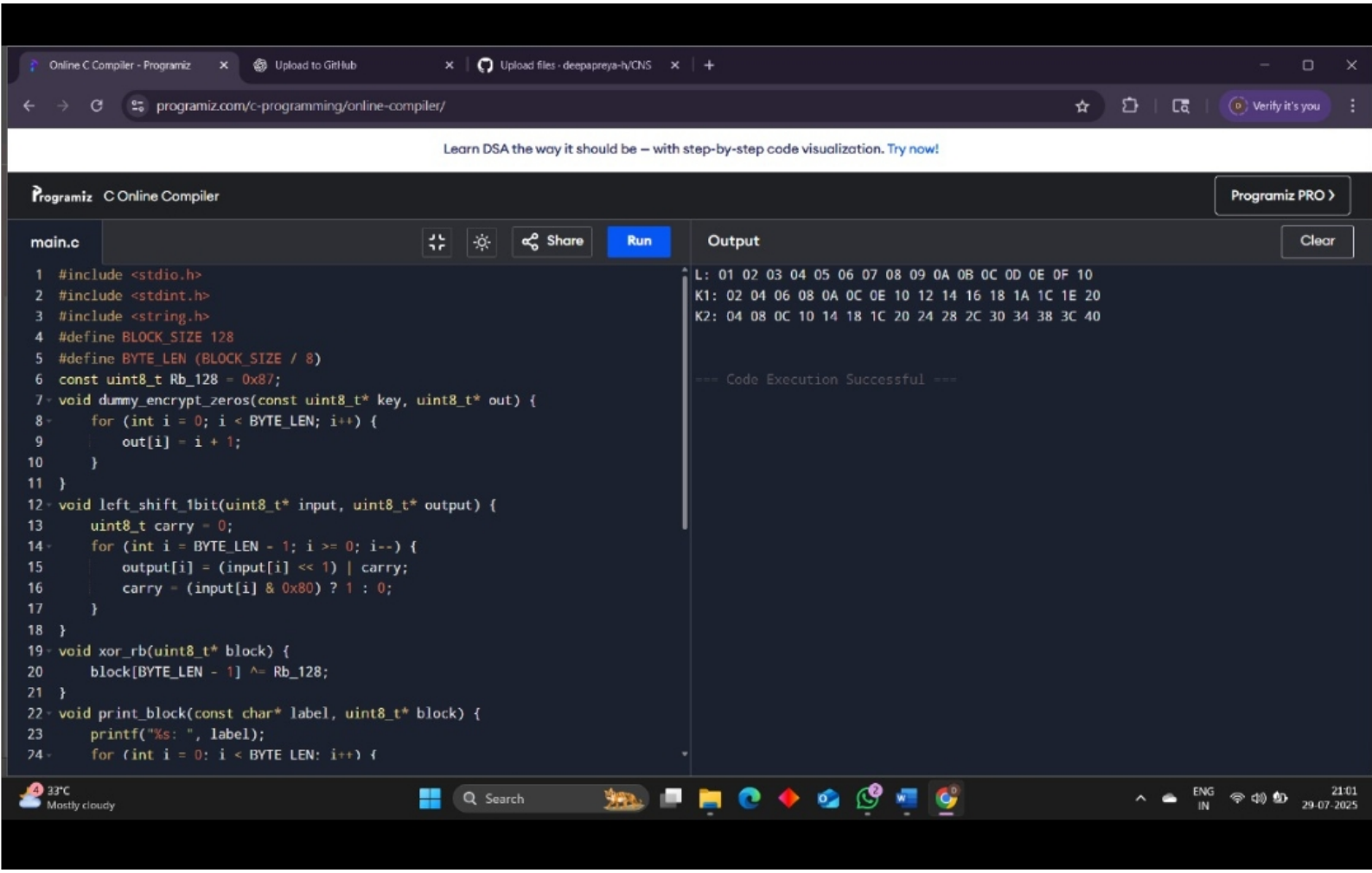
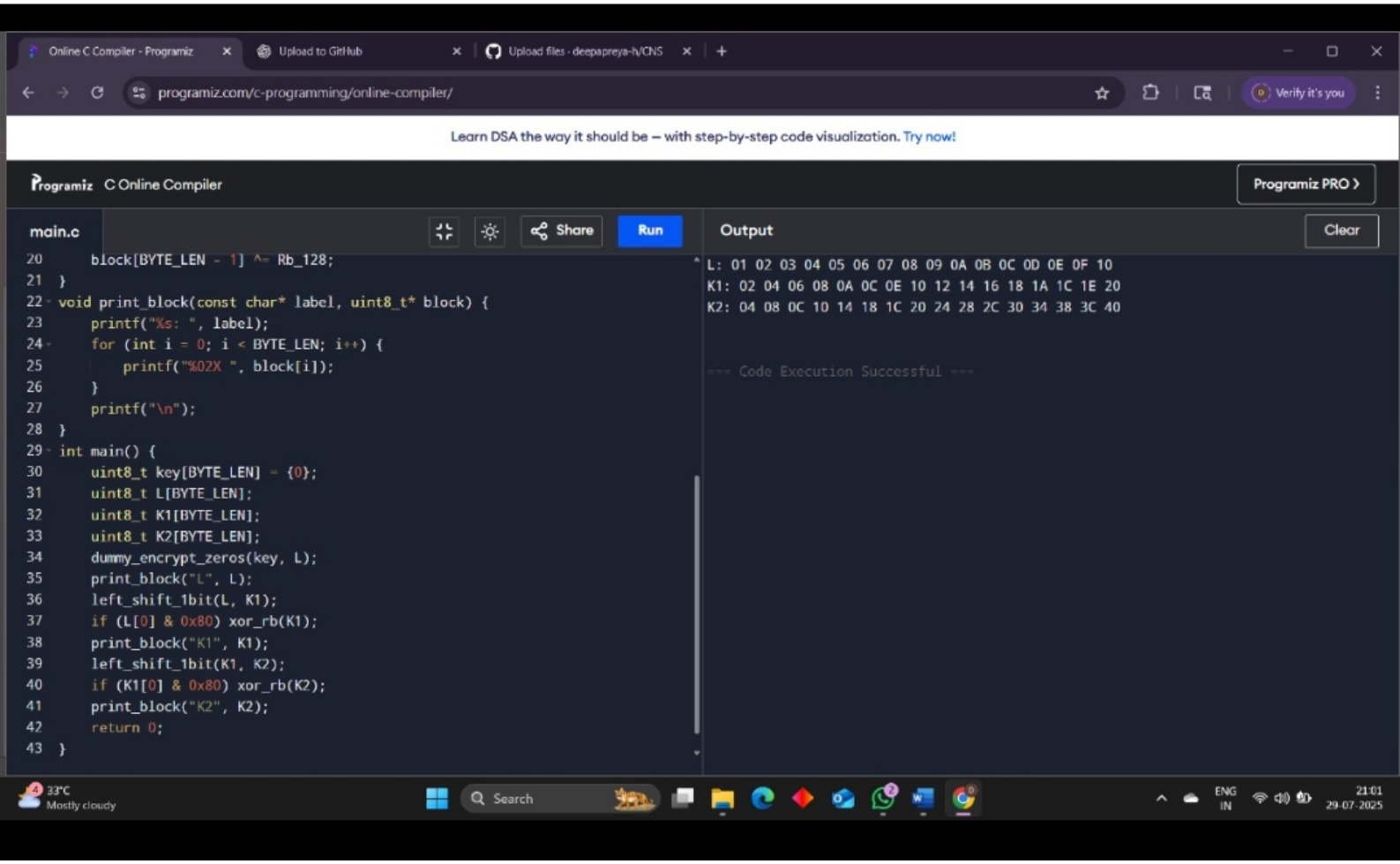

Online C Compiler - Programiz
Upload to GitHub
Upload files - deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <stdint.h>
#include <string.h>
#define BLOCK_SIZE 128
#define BYTE_LEN (BLOCK_SIZE / 8)
const uint8_t Rb_128 = 0x87;
void dummy_encrypt_zeros(const uint8_t* key, uint8_t* out) {
for (int i = 0; i < BYTE_LEN; i++) {
out[i] = i + 1;
}
}
void left_shift_1bit(uint8_t* input, uint8_t* output) {
uint8_t carry = 0;
for (int i = BYTE_LEN - 1; i >= 0; i--) {
output[i] = (input[i] << 1) | carry;
carry = (input[i] & 0x80) ? 1 : 0;
}
}
void xor_rb(uint8_t* block) {
block[BYTE_LEN - 1] ^= Rb_128;
}
void print_block(const char* label, uint8_t* block) {
printf("%s: ", label);
for (int i = 0; i < BYTE_LEN; i++) {
L: 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
K1: 02 04 06 08 0A 0C 0E 10 12 14 16 18 1A 1C 1E 20
K2: 04 08 0C 10 14 18 1C 20 24 28 2C 30 34 38 3C 40
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
21:01
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
block[BYTE_LEN - 1] ^= Rb_128;
}
void print_block(const char* label, uint8_t* block) {
printf("%s: ", label);
for (int i = 0; i < BYTE_LEN; i++) {
printf("%02X ", block[i]);
}
printf("\n");
}
int main() {
uint8_t key[BYTE_LEN] = {0};
uint8_t L[BYTE_LEN];
uint8_t K1[BYTE_LEN];
uint8_t K2[BYTE_LEN];
dummy_encrypt_zeros(key, L);
print_block("L", L);
left_shift_1bit(L, K1);
if (L[0] & 0x80) xor_rb(K1);
print_block("K1", K1);
left_shift_1bit(K1, K2);
if (K1[0] & 0x80) xor_rb(K2);
print_block("K2", K2);
return 0;
}
L: 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
K1: 02 04 06 08 0A 0C 0E 10 12 14 16 18 1A 1C 1E 20
K2: 04 08 0C 10 14 18 1C 20 24 28 2C 30 34 38 3C 40
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
21:01
29-07-2025