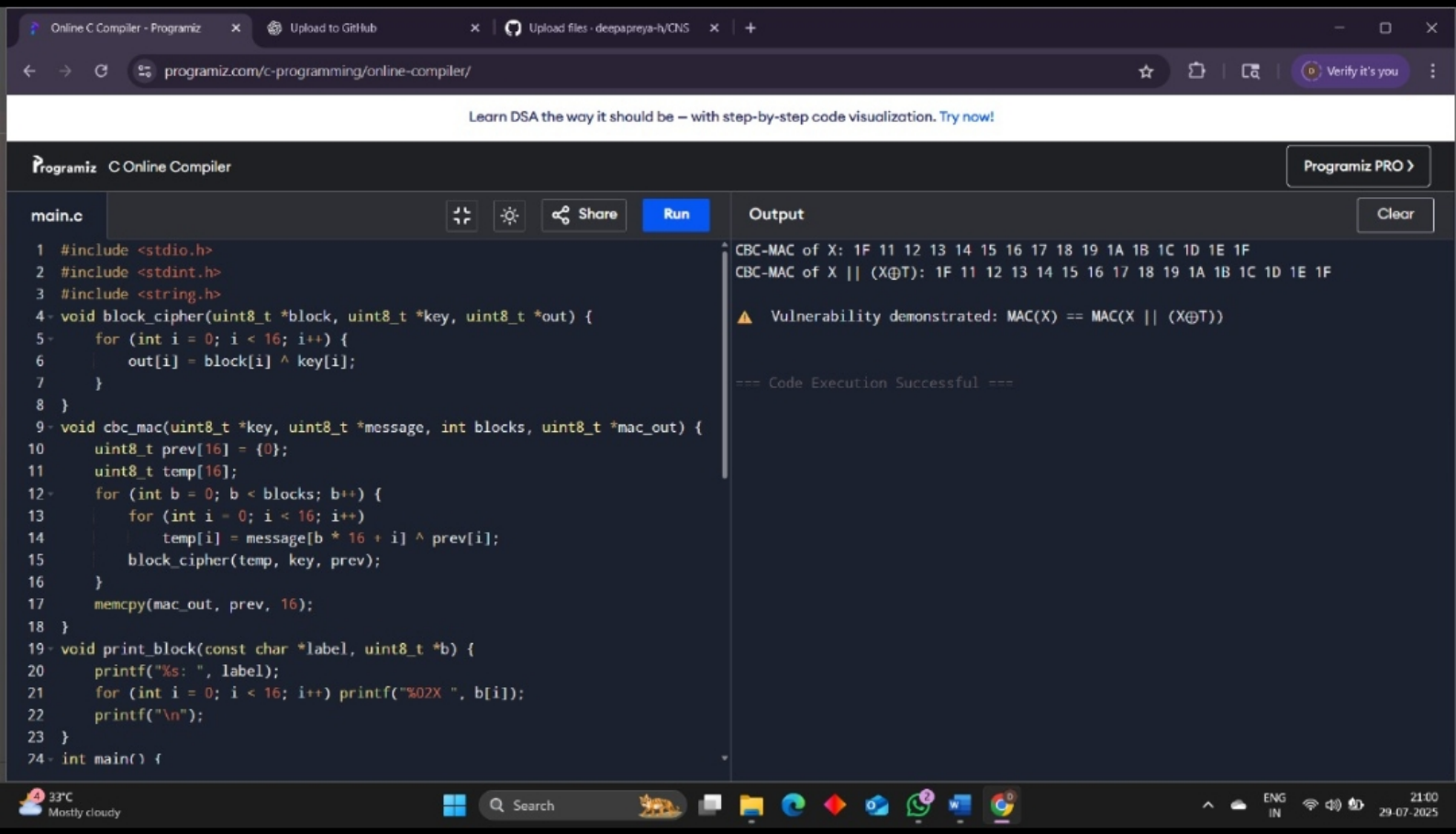
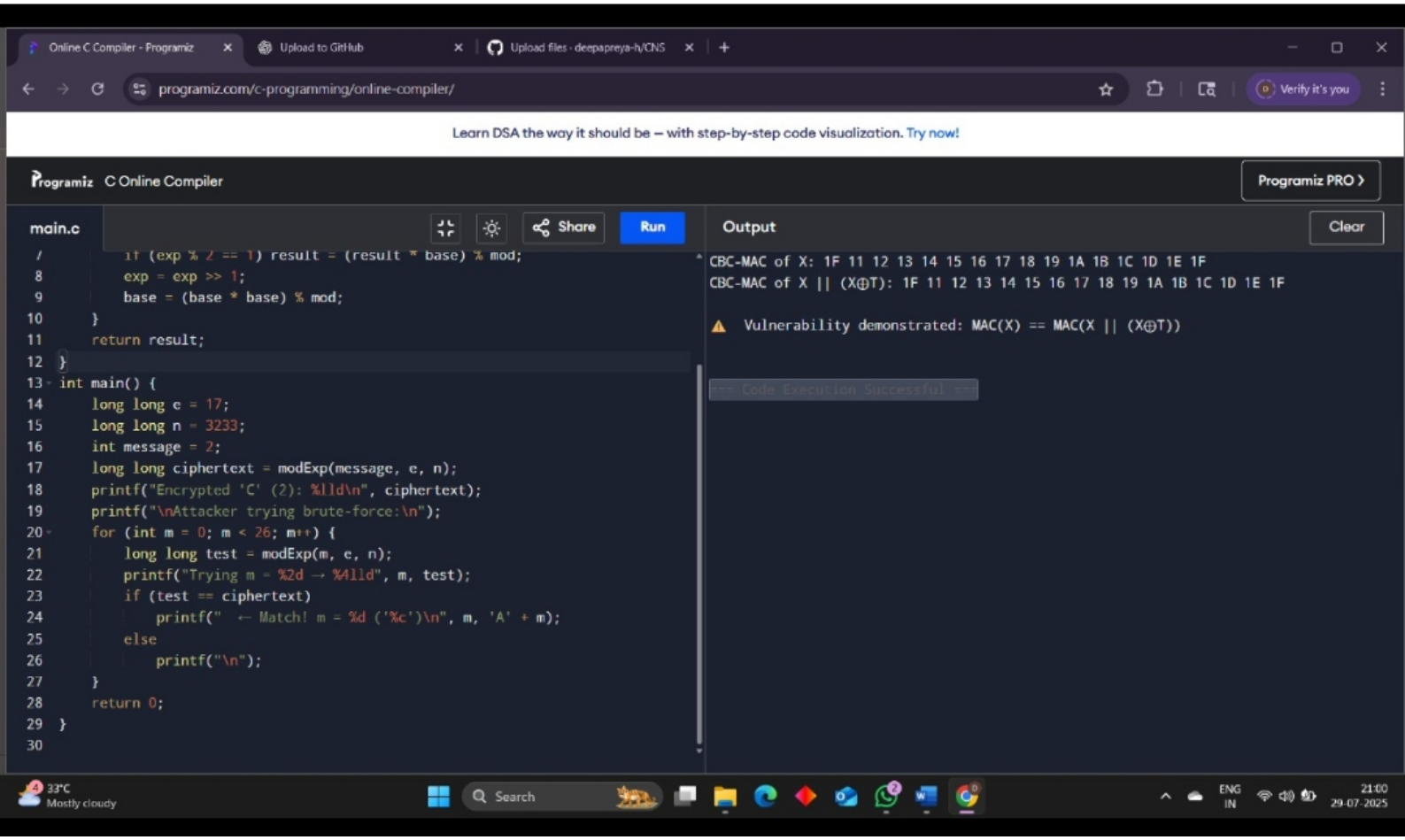

Online C Compiler - Programiz
Upload to GitHub
Upload files · deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <stdint.h>
#include <string.h>
void block_cipher(uint8_t *block, uint8_t *key, uint8_t *out) {
for (int i = 0; i < 16; i++) {
out[i] = block[i] ^ key[i];
}
}
void cbc_mac(uint8_t *key, uint8_t *message, int blocks, uint8_t *mac_out) {
uint8_t prev[16] = {0};
uint8_t temp[16];
for (int b = 0; b < blocks; b++) {
for (int i = 0; i < 16; i++)
temp[i] = message[b * 16 + i] ^ prev[i];
block_cipher(temp, key, prev);
}
memcpy(mac_out, prev, 16);
}
void print_block(const char *label, uint8_t *b) {
printf("%s: ", label);
for (int i = 0; i < 16; i++) printf("%02X ", b[i]);
printf("\n");
}
int main() {
CBC-MAC of X: 1F 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
CBC-MAC of X || (X⊕T): 1F 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
Vulnerability demonstrated: MAC(X) == MAC(X || (X⊕T))
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
21:00
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
if (exp % 2 == 1) result = (result * base) % mod;
exp = exp >> 1;
base = (base * base) % mod;
}
return result;
}
int main() {
long long e = 17;
long long n = 3233;
int message = 2;
long long ciphertext = modExp(message, e, n);
printf("Encrypted 'C' (2): %lld\n", ciphertext);
printf("\nAttacker trying brute-force:\n");
for (int m = 0; m < 26; m++) {
long long test = modExp(m, e, n);
printf("Trying m = %2d → %4lld", m, test);
if (test == ciphertext)
printf(" ← Match! m = %d ('%c')\n", m, 'A' + m);
else
printf("\n");
}
return 0;
}
CBC-MAC of X: 1F 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
CBC-MAC of X || (X⊕T): 1F 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
Vulnerability demonstrated: MAC(X) == MAC(X || (X⊕T))
33°C
Mostly cloudy
Search
ENG
IN
21:00
29-07-2025