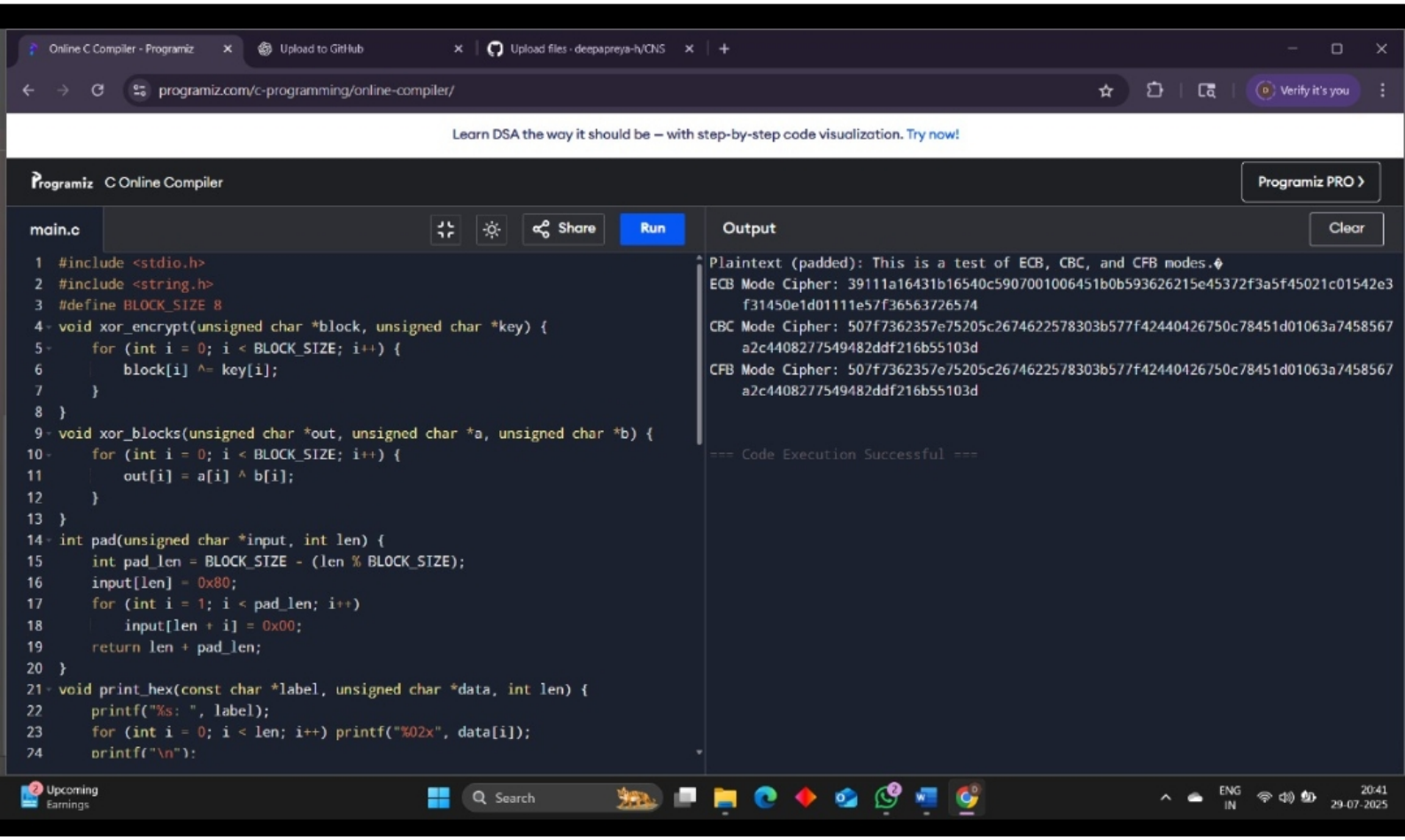
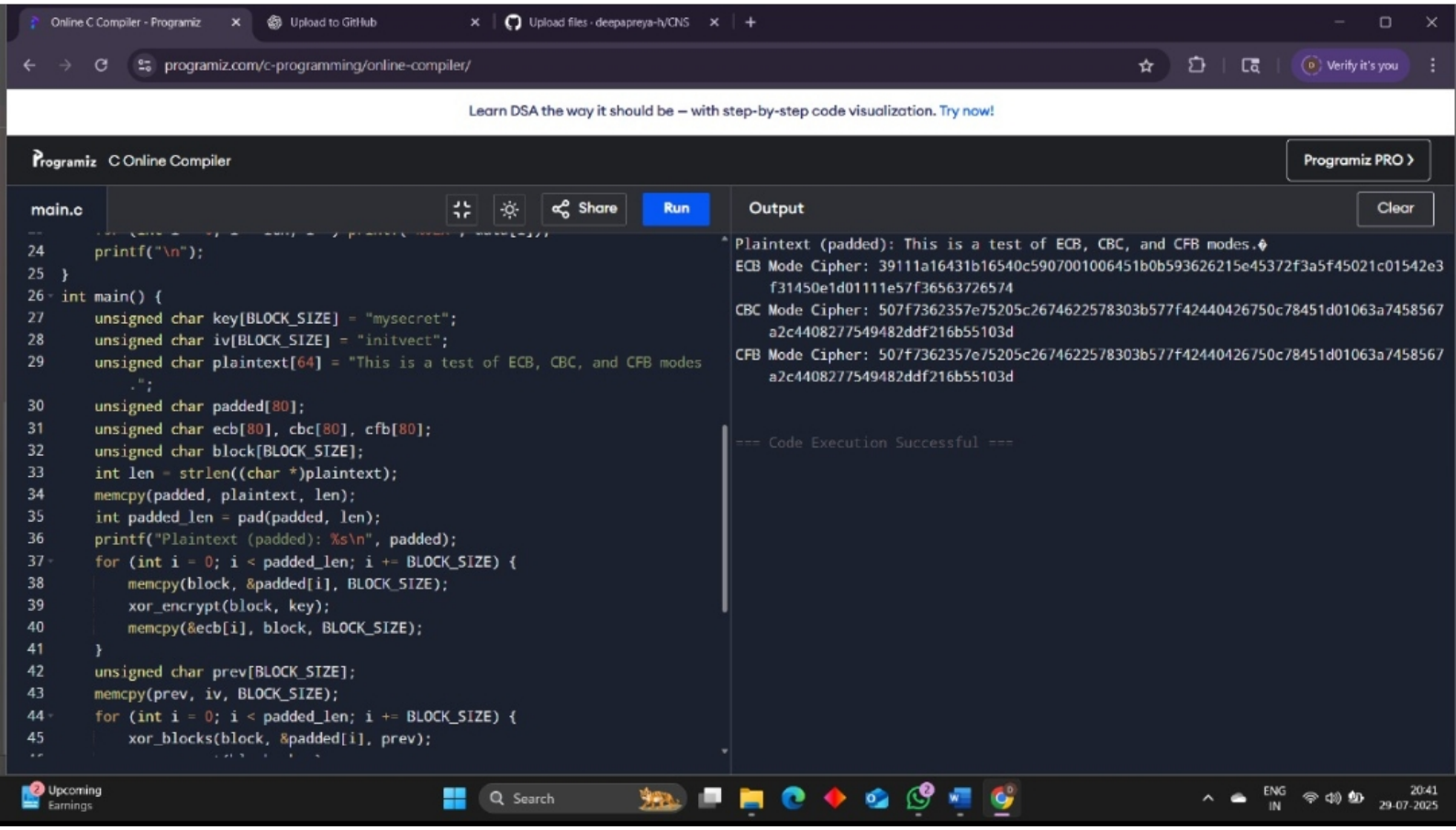
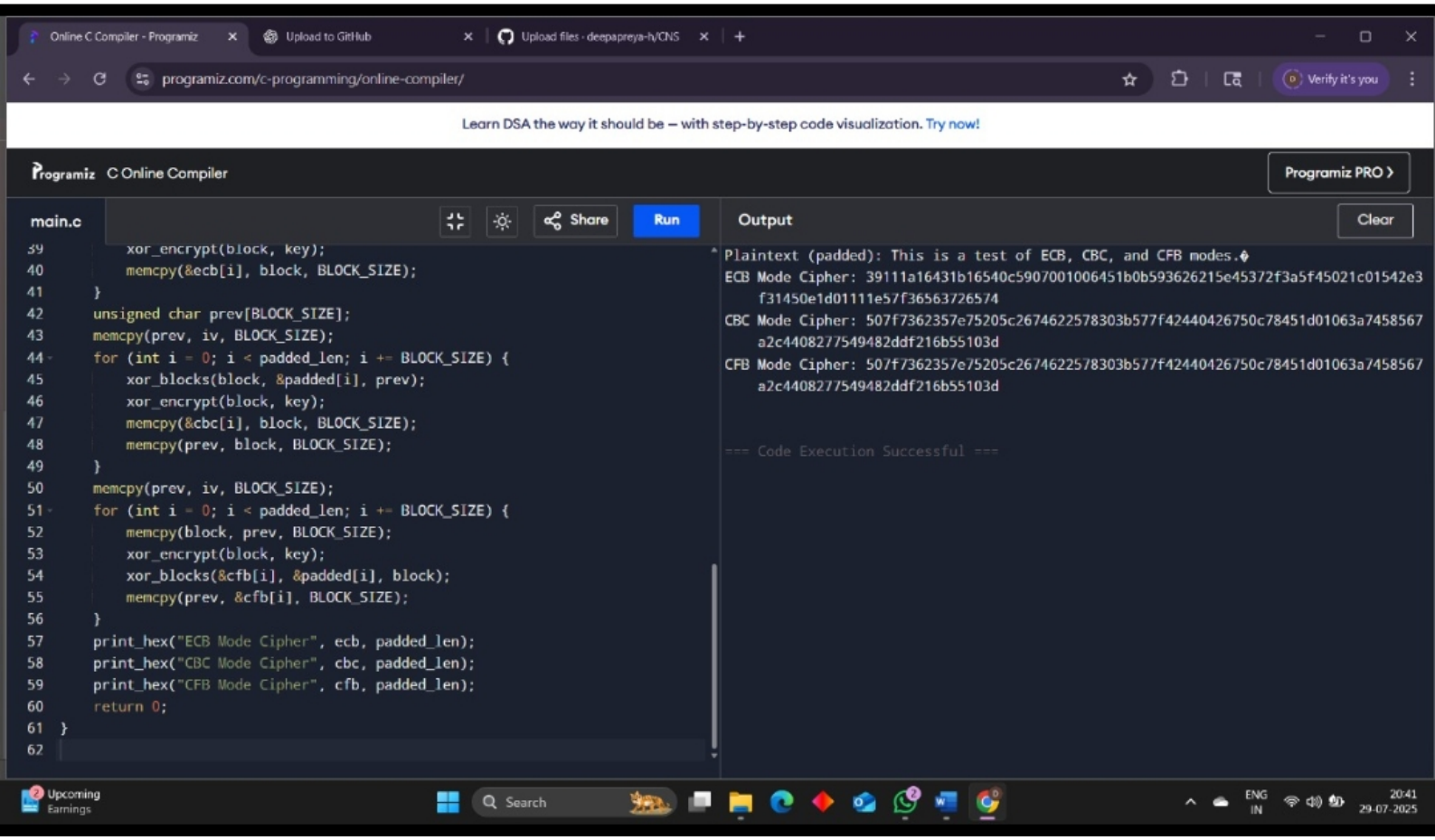

Online C Compiler - Programiz
Upload to GitHub
Upload files - deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <string.h>
#define BLOCK_SIZE 8
void xor_encrypt(unsigned char *block, unsigned char *key) {
for (int i = 0; i < BLOCK_SIZE; i++) {
block[i] ^= key[i];
}
}
void xor_blocks(unsigned char *out, unsigned char *a, unsigned char *b) {
for (int i = 0; i < BLOCK_SIZE; i++) {
out[i] = a[i] ^ b[i];
}
}
int pad(unsigned char *input, int len) {
int pad_len = BLOCK_SIZE - (len % BLOCK_SIZE);
input[len] = 0x80;
for (int i = 1; i < pad_len; i++)
input[len + i] = 0x00;
return len + pad_len;
}
void print_hex(const char *label, unsigned char *data, int len) {
printf("%s: ", label);
for (int i = 0; i < len; i++) printf("%02x", data[i]);
printf("\n");
Plaintext (padded): This is a test of ECB, CBC, and CFB modes.
ECB Mode Cipher: 39111a16431b16540c5907001006451b0b593626215e45372f3a5f45021c01542e3
f31450e1d01111e57f36563726574
CBC Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567
a2c4408277549482ddf216b55103d
CFB Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567
a2c4408277549482ddf216b55103d
=== Code Execution Successful ===
Upcoming Earnings
Search
ENG IN
20:41
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
printf("\n");
}
int main() {
unsigned char key[BLOCK_SIZE] = "mysecret";
unsigned char iv[BLOCK_SIZE] = "initvect";
unsigned char plaintext[64] = "This is a test of ECB, CBC, and CFB modes.";
unsigned char padded[80];
unsigned char ecb[80], cbc[80], cfb[80];
unsigned char block[BLOCK_SIZE];
int len = strlen((char *)plaintext);
memcpy(padded, plaintext, len);
int padded_len = pad(padded, len);
printf("Plaintext (padded): %s\n", padded);
for (int i = 0; i < padded_len; i += BLOCK_SIZE) {
memcpy(block, &padded[i], BLOCK_SIZE);
xor_encrypt(block, key);
memcpy(&ecb[i], block, BLOCK_SIZE);
}
unsigned char prev[BLOCK_SIZE];
memcpy(prev, iv, BLOCK_SIZE);
for (int i = 0; i < padded_len; i += BLOCK_SIZE) {
xor_blocks(block, &padded[i], prev);
Plaintext (padded): This is a test of ECB, CBC, and CFB modes.
ECB Mode Cipher: 39111a16431b16540c5907001006451b0b593626215e45372f3a5f45021c01542e3f31450e1d01111e57f36563726574
CBC Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567a2c4408277549482ddf216b55103d
CFB Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567a2c4408277549482ddf216b55103d
=== Code Execution Successful ===
Upcoming Earnings
Search
ENG IN
20:41
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
xor_encrypt(block, key);
memcpy(&ecb[i], block, BLOCK_SIZE);
}
unsigned char prev[BLOCK_SIZE];
memcpy(prev, iv, BLOCK_SIZE);
for (int i = 0; i < padded_len; i += BLOCK_SIZE) {
xor_blocks(block, &padded[i], prev);
xor_encrypt(block, key);
memcpy(&cbc[i], block, BLOCK_SIZE);
memcpy(prev, block, BLOCK_SIZE);
}
memcpy(prev, iv, BLOCK_SIZE);
for (int i = 0; i < padded_len; i += BLOCK_SIZE) {
memcpy(block, prev, BLOCK_SIZE);
xor_encrypt(block, key);
xor_blocks(&cfb[i], &padded[i], block);
memcpy(prev, &cfb[i], BLOCK_SIZE);
}
print_hex("ECB Mode Cipher", ecb, padded_len);
print_hex("CBC Mode Cipher", cbc, padded_len);
print_hex("CFB Mode Cipher", cfb, padded_len);
return 0;
}
Plaintext (padded): This is a test of ECB, CBC, and CFB modes.
ECB Mode Cipher: 39111a16431b16540c5907001006451b0b593626215e45372f3a5f45021c01542e3f31450e1d01111e57f36563726574
CBC Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567a2c4408277549482ddf216b55103d
CFB Mode Cipher: 507f7362357e75205c2674622578303b577f42440426750c78451d01063a7458567a2c4408277549482ddf216b55103d
--- Code Execution Successful ---
Upcoming Earnings
Search
ENG IN
20:41 29-07-2025