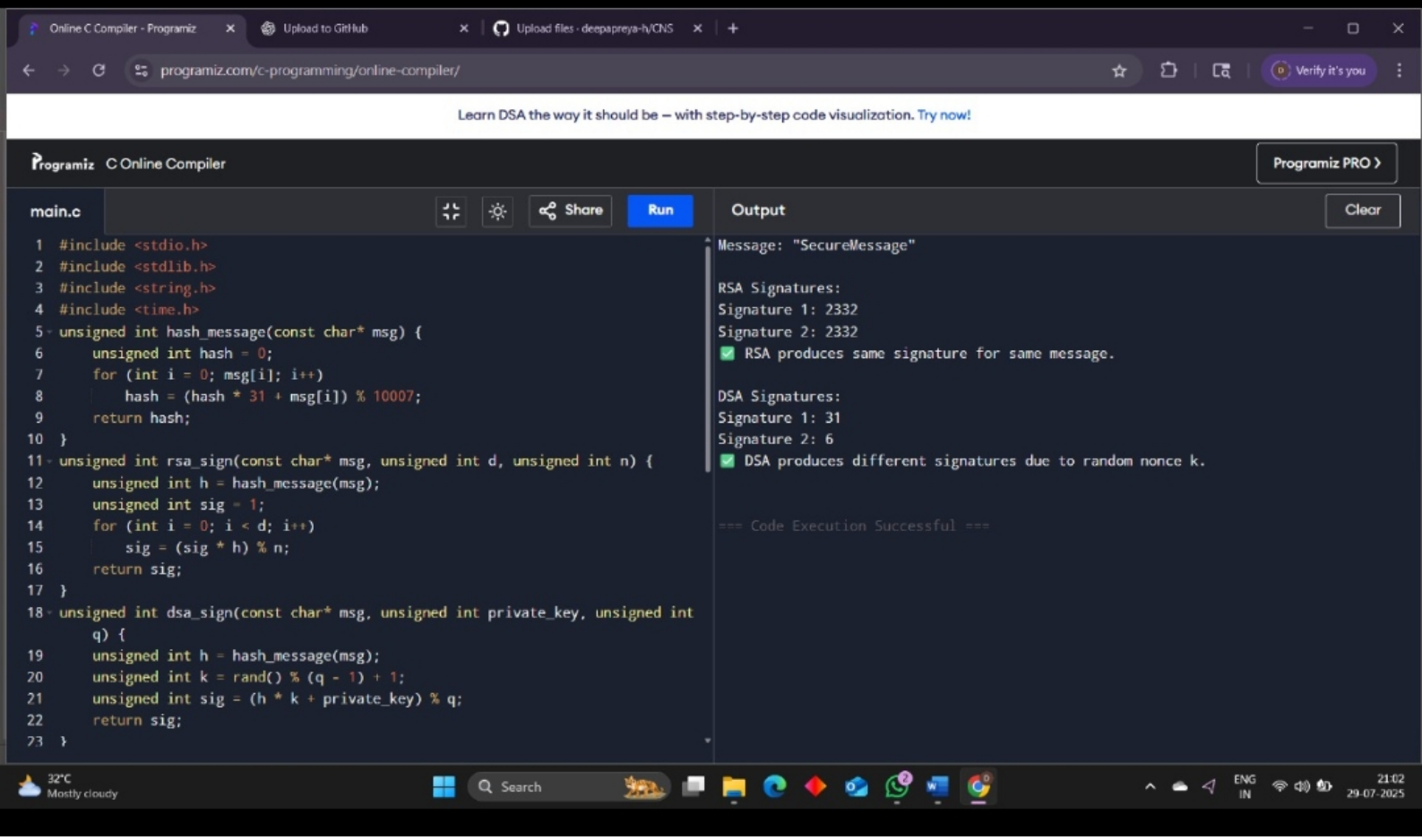
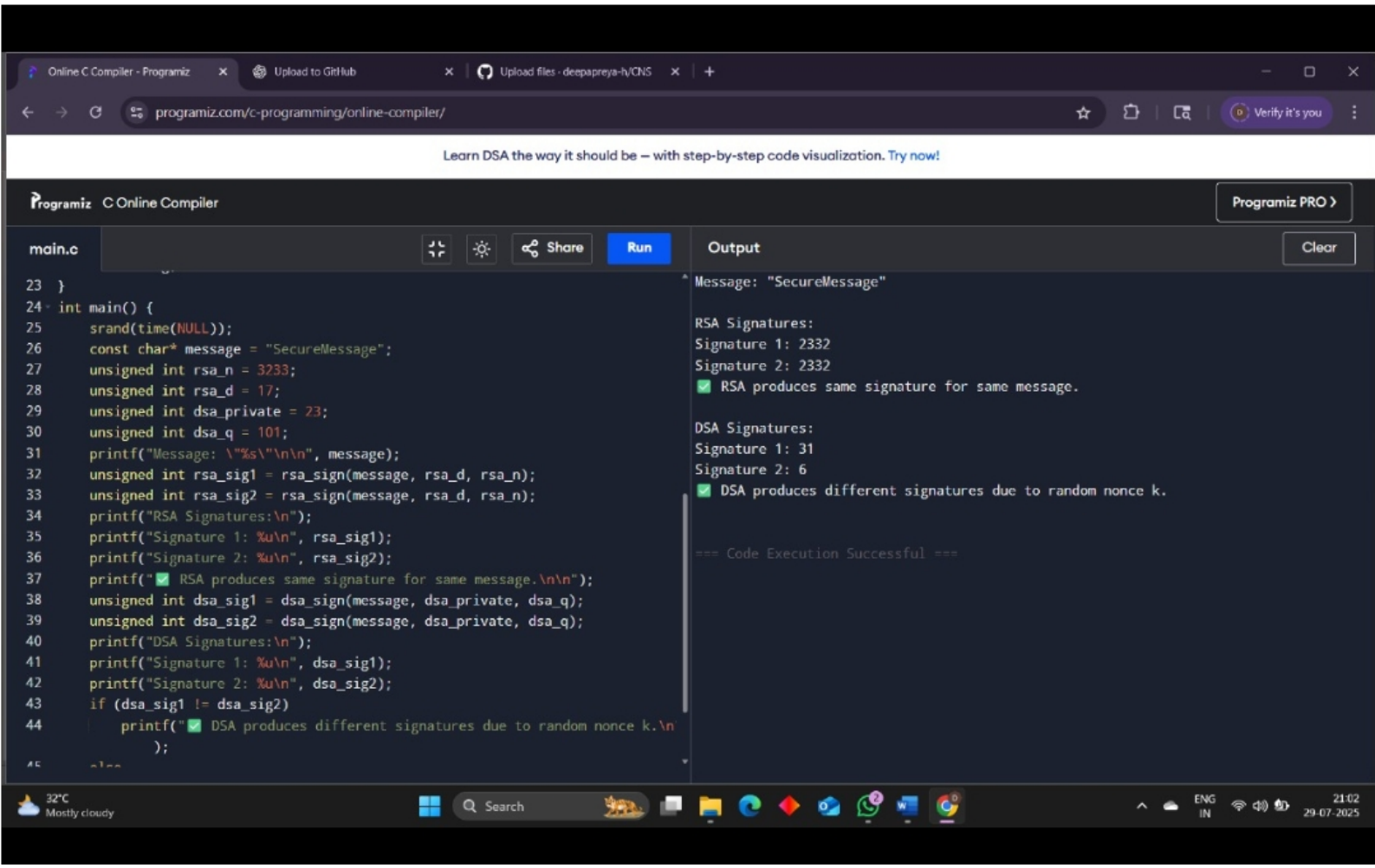
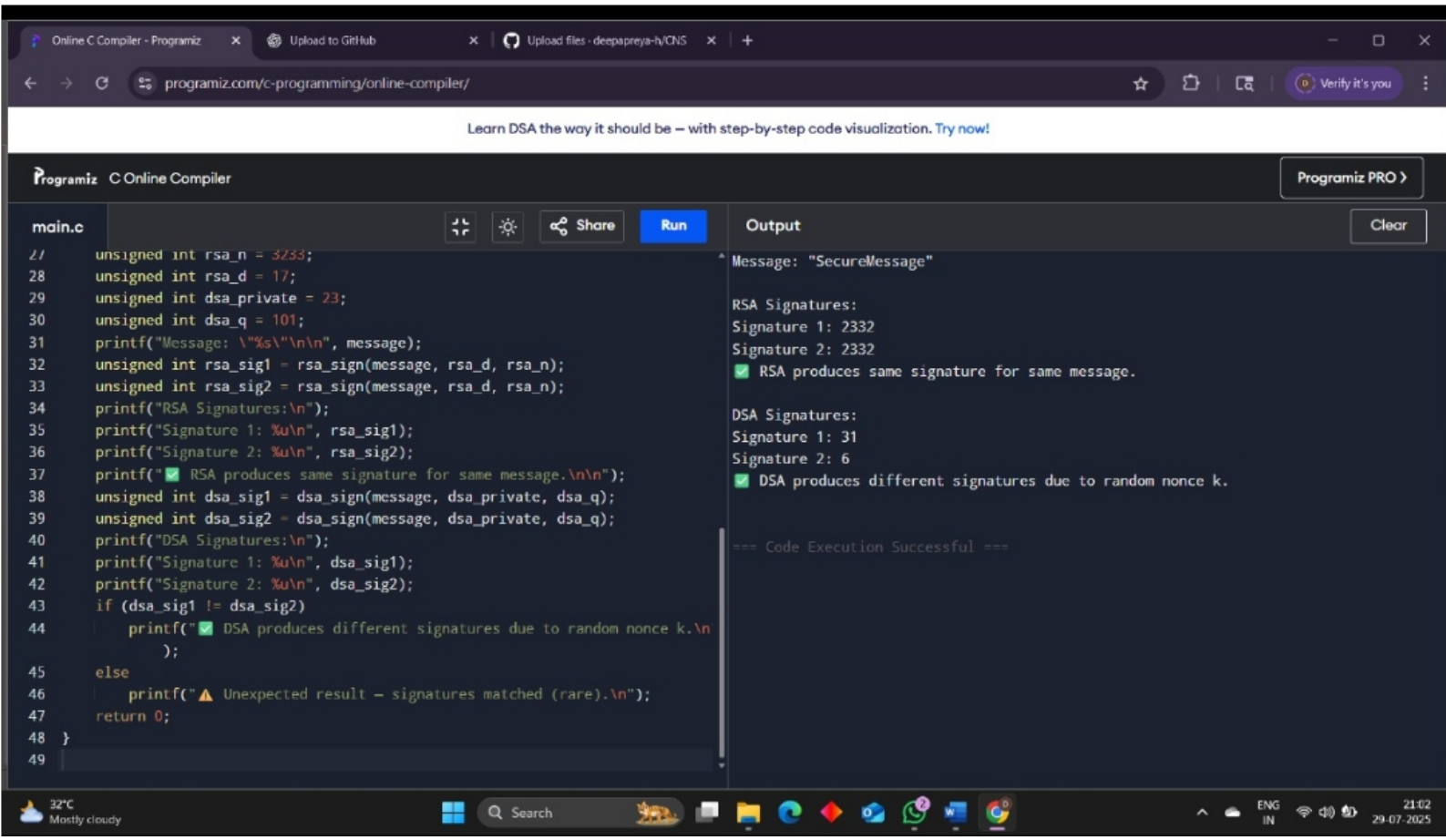

Online C Compiler - Programiz
Upload to GitHub
Upload files - deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>
unsigned int hash_message(const char* msg) {
unsigned int hash = 0;
for (int i = 0; msg[i]; i++)
hash = (hash * 31 + msg[i]) % 10007;
return hash;
}
unsigned int rsa_sign(const char* msg, unsigned int d, unsigned int n) {
unsigned int h = hash_message(msg);
unsigned int sig = 1;
for (int i = 0; i < d; i++)
sig = (sig * h) % n;
return sig;
}
unsigned int dsa_sign(const char* msg, unsigned int private_key, unsigned int q) {
unsigned int h = hash_message(msg);
unsigned int k = rand() % (q - 1) + 1;
unsigned int sig = (h * k + private_key) % q;
return sig;
}
Message: "SecureMessage"
RSA Signatures:
Signature 1: 2332
Signature 2: 2332
RSA produces same signature for same message.
DSA Signatures:
Signature 1: 31
Signature 2: 6
DSA produces different signatures due to random nonce k.
=== Code Execution Successful ===
32°C
Mostly cloudy
Search
ENG
IN
21:02
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
23 }
24 int main() {
25 srand(time(NULL));
26 const char* message = "SecureMessage";
27 unsigned int rsa_n = 3233;
28 unsigned int rsa_d = 17;
29 unsigned int dsa_private = 23;
30 unsigned int dsa_q = 101;
31 printf("Message: \"%s\"\n\n", message);
32 unsigned int rsa_sig1 = rsa_sign(message, rsa_d, rsa_n);
33 unsigned int rsa_sig2 = rsa_sign(message, rsa_d, rsa_n);
34 printf("RSA Signatures:\n");
35 printf("Signature 1: %u\n", rsa_sig1);
36 printf("Signature 2: %u\n", rsa_sig2);
37 printf("✅ RSA produces same signature for same message.\n\n");
38 unsigned int dsa_sig1 = dsa_sign(message, dsa_private, dsa_q);
39 unsigned int dsa_sig2 = dsa_sign(message, dsa_private, dsa_q);
40 printf("DSA Signatures:\n");
41 printf("Signature 1: %u\n", dsa_sig1);
42 printf("Signature 2: %u\n", dsa_sig2);
43 if (dsa_sig1 != dsa_sig2)
44 printf("✅ DSA produces different signatures due to random nonce k.\n
);
Message: "SecureMessage"
RSA Signatures:
Signature 1: 2332
Signature 2: 2332
✅ RSA produces same signature for same message.
DSA Signatures:
Signature 1: 31
Signature 2: 6
✅ DSA produces different signatures due to random nonce k.
=== Code Execution Successful ===
32°C
Mostly cloudy
Search
ENG
IN
21:02
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
unsigned int rsa_n = 3233;
unsigned int rsa_d = 17;
unsigned int dsa_private = 23;
unsigned int dsa_q = 101;
printf("Message: \"%s\"\n\n", message);
unsigned int rsa_sig1 = rsa_sign(message, rsa_d, rsa_n);
unsigned int rsa_sig2 = rsa_sign(message, rsa_d, rsa_n);
printf("RSA Signatures:\n");
printf("Signature 1: %u\n", rsa_sig1);
printf("Signature 2: %u\n", rsa_sig2);
printf("✅ RSA produces same signature for same message.\n\n");
unsigned int dsa_sig1 = dsa_sign(message, dsa_private, dsa_q);
unsigned int dsa_sig2 = dsa_sign(message, dsa_private, dsa_q);
printf("DSA Signatures:\n");
printf("Signature 1: %u\n", dsa_sig1);
printf("Signature 2: %u\n", dsa_sig2);
if (dsa_sig1 != dsa_sig2)
printf("✅ DSA produces different signatures due to random nonce k.\n
);
else
printf("⚠️ Unexpected result — signatures matched (rare).\n");
return 0;
}
Message: "SecureMessage"
RSA Signatures:
Signature 1: 2332
Signature 2: 2332
✅ RSA produces same signature for same message.
DSA Signatures:
Signature 1: 31
Signature 2: 6
✅ DSA produces different signatures due to random nonce k.
=== Code Execution Successful ===
32°C
Mostly cloudy
Search
ENG
IN
21:02
29-07-2025