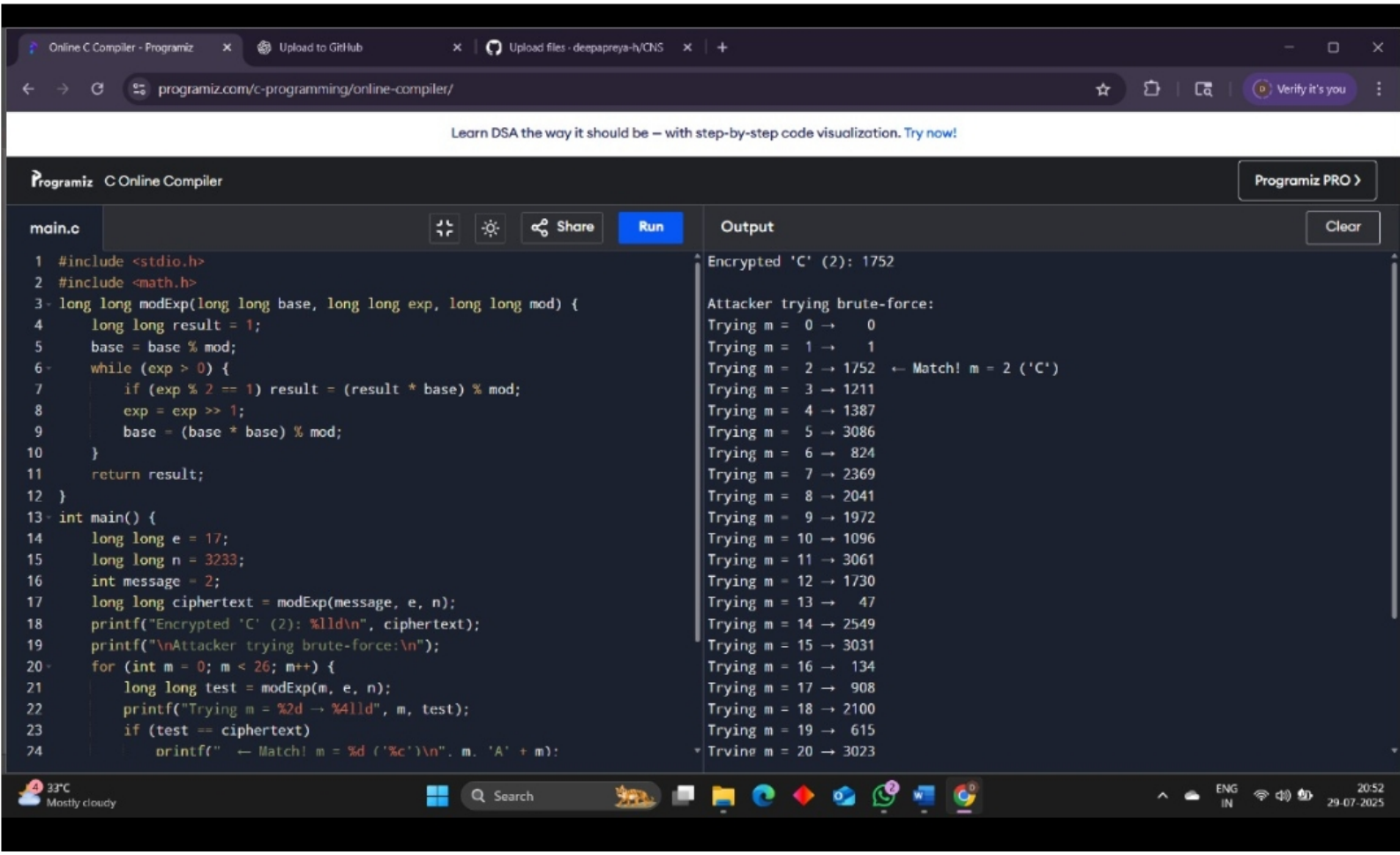
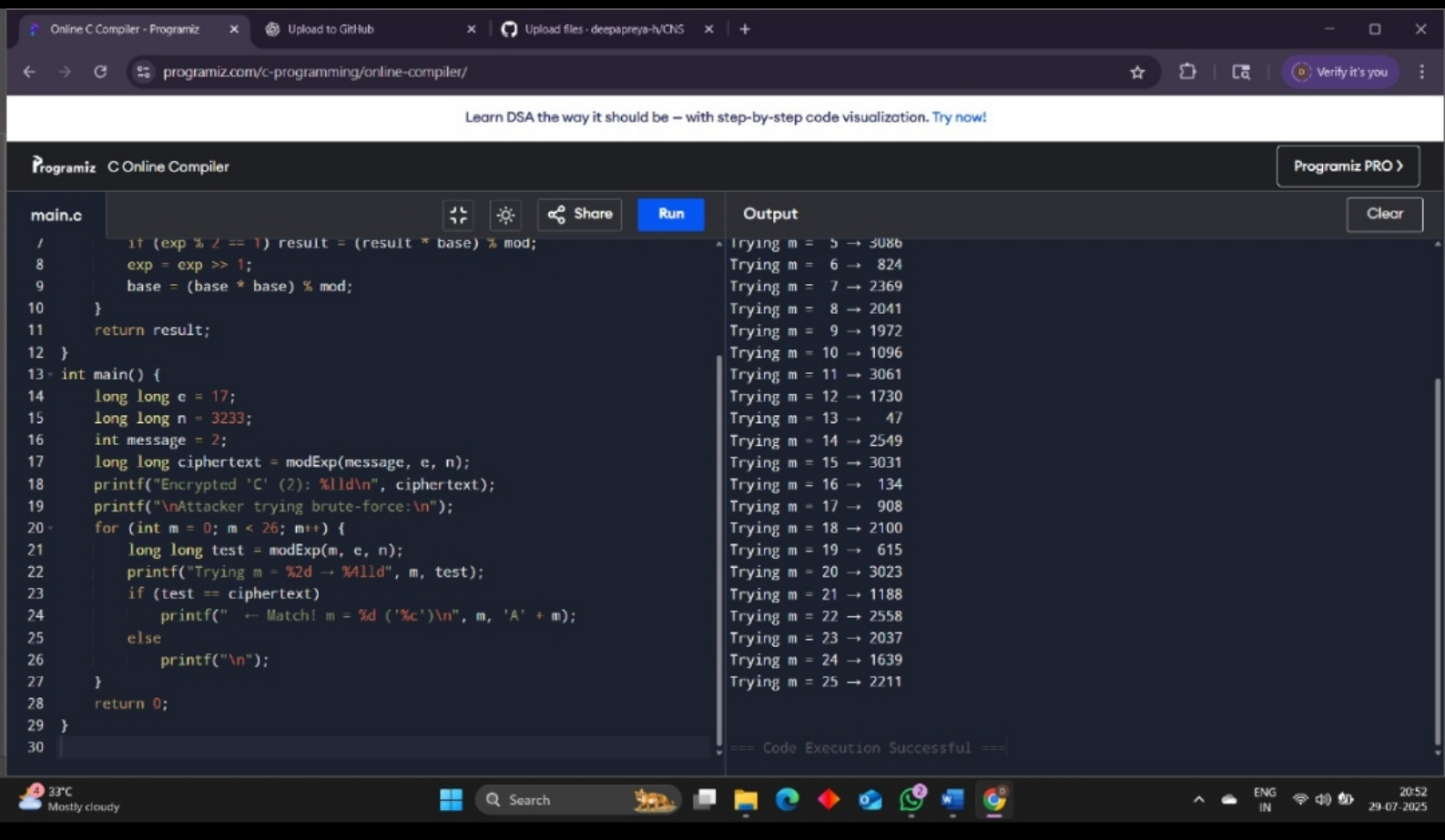

Online C Compiler - Programiz
Upload to GitHub
Upload files · deepapreya-h/CNS
programiz.com/c-programming/online-compiler/
Verify it's you
Learn DSA the way it should be — with step-by-step code visualization. Try now!
Programiz C Online Compiler
Programiz PRO
main.c
Share
Run
Output
Clear
#include <stdio.h>
#include <math.h>
long long modExp(long long base, long long exp, long long mod) {
long long result = 1;
base = base % mod;
while (exp > 0) {
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);
Encrypted 'C' (2): 1752
Attacker trying brute-force:
Trying m = 0 → 0
Trying m = 1 → 1
Trying m = 2 → 1752 ← Match! m = 2 ('C')
Trying m = 3 → 1211
Trying m = 4 → 1387
Trying m = 5 → 3086
Trying m = 6 → 824
Trying m = 7 → 2369
Trying m = 8 → 2041
Trying m = 9 → 1972
Trying m = 10 → 1096
Trying m = 11 → 3061
Trying m = 12 → 1730
Trying m = 13 → 47
Trying m = 14 → 2549
Trying m = 15 → 3031
Trying m = 16 → 134
Trying m = 17 → 908
Trying m = 18 → 2100
Trying m = 19 → 615
Trying m = 20 → 3023
33°C
Mostly cloudy
Search
ENG
IN
20:52
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;
}
Trying m = 5 → 3086
Trying m = 6 → 824
Trying m = 7 → 2369
Trying m = 8 → 2041
Trying m = 9 → 1972
Trying m = 10 → 1096
Trying m = 11 → 3061
Trying m = 12 → 1730
Trying m = 13 → 47
Trying m = 14 → 2549
Trying m = 15 → 3031
Trying m = 16 → 134
Trying m = 17 → 908
Trying m = 18 → 2100
Trying m = 19 → 615
Trying m = 20 → 3023
Trying m = 21 → 1188
Trying m = 22 → 2558
Trying m = 23 → 2037
Trying m = 24 → 1639
Trying m = 25 → 2211
=== Code Execution Successful ===
33°C
Mostly cloudy
Search
ENG
IN
20:52
29-07-2025