




main.c



Share

Run

1 #include <stdio.h>

2 #include <stdint.h>

3

4 #define BLOCK_SIZE_64 8

5 #define BLOCK_SIZE_128 16

6 #define CONSTANT_64 0x1B

7 #define CONSTANT_128 0x87

8

9 void left_shift_and_xor(uint8_t *key, int block_size) {

10 uint8_t msb = key[0] & 0x80; // Check the most significant bit

11 for (int i = 0; i < block_size - 1; i++) {

12 key[i] = (key[i] << 1) | (key[i + 1] >> 7);

13 }

14 key[block_size - 1] <<= 1; // Shift the last byte

15

16 // If the MSB was set, XOR with the constant

17 if (msb) {

18 key[0] ^= (block_size == BLOCK_SIZE_64) ? CONSTANT_64 :

19 CONSTANT_128;

20 }

21 }

22 void generate_subkeys(uint8_t *key, uint8_t *subkey1, uint8_t

23 *subkey2, int block_size) {

Output

Clear

Subkey 1: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Subkey 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

=== Code Execution Successful ===