Programiz
C Online
Compiler

Programiz
PRO ›

main.c

Run

Output

Clear

```c
#include <stdio.h>
#include <stdint.h>

#define BLOCK_SIZE 8

// Permutation tables
int P10[] = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6};
int P8[] = {6, 3, 7, 4, 8, 5, 10, 9};
int IP[] = {2, 6, 3, 1, 4, 8, 5, 7};
int IP_INV[] = {4, 1, 3, 5, 7, 2, 8, 6};
int EP[] = {4, 1, 2, 3, 2, 3, 4, 1};
int P4[] = {2, 4, 3, 1};

int S0[4][4] = {
    {1, 0, 3, 2},
    {3, 2, 1, 0},
    {0, 2, 1, 3},
    {3, 1, 3, 2}
```

```
Plaintext : 00000001000000100000100
Encrypted : 00000001000000100000100
Decrypted : 00000001000000100000100


=== Code Execution Successful ===
```

Programiz
C Online
Compiler

Programiz
PRO ›

main.c

Run

Output

Clear

```
        // 00000001 00000010 00000100
    uint8_t ciphertext[3];
    uint8_t decrypted[3];

    // Encrypt
    ctr_mode(plaintext, ciphertext, 3, counter,
        k1, k2);
    // Decrypt (same as encrypt in CTR)
    ctr_mode(ciphertext, decrypted, 3, counter,
        k1, k2);

    print_bin("Plaintext ", plaintext, 3);
    print_bin("Encrypted ", ciphertext, 3); //
        Should be: 00111000 01001111 00110010
    print_bin("Decrypted ", decrypted, 3);

    return 0;
}
```

```
Plaintext : 000000010000001000000100
Encrypted : 000000010000001000000100
Decrypted : 000000010000001000000100


=== Code Execution Successful ===
```