CYBER SECURITY

3. forduló

A kategória támogatója: Continental

Ismertető a feladatlaphoz

Kérjük, hogy a feladatlap indítása előtt mindenképp olvasd el az alábbi útmutatót:

> Amennyiben olyan kategóriában játszol, ahol van csatolmány, de hibába ütközöl a letöltésnél, ott valószínűleg a vírusirtó korlátoz, annak ideiglenes kikapcsolása megoldhatja a problémát. (Körülbelül minden 3000. letöltésnél fordul ez elő.)

> Helyezéseket a 4. forduló után mutatunk, százalékos formában: adott kategóriában a TOP 20-40-60%-hoz tartozol.
>
> A feltűnően rövid idő alatt megoldott feladatlapok kizárást vonnak maguk után, bármilyen más gyanús esetben fenntartjuk a jogot a forduló érvénytelenítésére!

Jó versenyzést kívánunk!

Ezen a héten 2, kicsit pihentetőbb feladattal készültünk.

1. feladat 0 pont

Hány hibát találsz a következő kódrészletben? Szintaktikai és szemantikai hibák egyaránt előfordulhatnak.

```
#include <limits.h>
#include <string.h>

#define CMAC_LENGTH             0x10
#define MAX_NUMBER_OF_BLOCKS    0x400

typedef struct
{
    unsigned char * start_address;
    unsigned int    data_length;
    unsigned char   cmac[CMAC_LENGTH];
}DataBlock_Type

unsigned int VerifyCmacOnBlocks(DataBlock_Type blocks[], unsigned int num_blocks)
{
    unsigned int retval = 0;

    if(num_blocks > MAX_NUMBER_OF_BLOCKS)
    {
        retval = UINT_MAX;
    }
    else
    {
        unsigned char i;

        for(i=0; i<num_blocks; i++)
        {
            retval += VerifyCmac(&blocks[i]);
        }
    }
    return retval;
}

unsigned int VerifyCmac(DataBlock_Type *block)
{
    unsigned char calculated_cmac[CMAC_LENGTH];

    CalculateCmac(block.start_address, block.data_length, &calculated_cmac[0]);

    if(memcmp(calculated_cmac, blocks->cmac, CMAC_LENGTH) == 0)
    {
        return 0;
    }
    else
    {
        return 1;
    }
}
```

Válasz

- 3
- 4
- 5
- 6

2. feladat 10 pont

Adott 16 bájt adat: [0x58, 0x92, 0x93, 0x86, 0xCE, 0x1E, 0x30, 0x95, 0x81, 0xED, 0x22, 0x28, 0x87, 0x5F, 0xD2, 0xD8]

Adott egy 16 bájtos titkos kulcs: [0xD8, 0xDD, 0x3C, 0x68, 0x00, 0xB0, 0xAD, 0x19, 0xE8, 0x25, 0xF5, 0xBC, 0xA7, 0xBC, 0x0F, 0xDB]

Az adatot az AES128 algoritmus ECB (Electronic Code Block) módjával titkosítottuk. Mi lesz a 16 bájtos eredmény utolsó bájtja?

Válasz

- 0xAB
- 0xCD
- 0xEF
- 0xGH

Megoldások beküldése