Symetrické šifry 2 crypto

Challenge status: Available
Challenge flags: 4

232

Ponořte se do další úlohy symetrické kryptografie a prozkoumejte detaily funkce F ve Feistelově šifře, která je klíčovou součástí algoritmu DES. Postupně si vyzkoušíte všechny čtyři části funkce, přesněji expanzi, mixování klíče, substituci pomocí S-boxů a permutaci.

Theory Flags Handbook Solves

Assignment

Představte si, že jste malý skřítek, který provádí šifrování dat v DESu ve funkci F. Funkce F se skládá ze čtyř kroků a na vstup přišla tato data

```
01101000 01100001 01111000 01100001
```

Kromě prvního úkolu použijete ve všech dalších výsledek z předchozího úkolu.

> *Například v úkolu č. 2 použijete výsledek z úkolu č. 1. Samozřejmě použijete pouze binární data, ne celou vlajku.*

Task 01

Expanze

Vaším úkolem je provést expanzi dat z úvodu úlohy na 48 bitů. Odpověď odevzdejte ve formátu `haxagon{binarnicislo}`.

> *Například, kdyby výsledkem bylo číslo `10101110 10101110 00011110 10110011 10101110 10101110`, tak odpověď bude `haxagon{101011101010111000011110101100111010111010101110}`.*

▶ Nápověda

Answer +15

Your answer

Submit

999 Total attempts

Task 02

Mixování klíče

Teď je na řadě další krok funkce F. Mixování klíče. Výsledek předchozího úkolu "mixněte" se sub klíčem: `10101101011011100110101110001000001111010101111O` .

Odpověď formátujte stejně, jako v předchozím úkolu.

Answer +5

Your answer

Submit

999 Total attempts

Task 03

Substituce

Jak už asi tušíte, tak dalším úkolem je substituce pomocí S-boxů. Proveďte substituci výsledku předchozího úkolu.

Odpověď odevzdejte ve formátu `haxagon{binarnicislo}` .

> *Například, kdyby výsledkem bylo číslo `1010 1110 1010 1110 0001 1110 1011 0011` , tak odpověď bude `haxagon{10101110101011100001111010110011}` .*

Answer +10

Your answer

Submit

999 Total attempts

Task 04

Permutace

Na závěr výsledek předchozího úkolu permutujte.

> *Nespleťte si IP s P.*

Odpověď formátujte stejně, jako v předchozím úkolu.

Answer **+15**

Your answer

Submit

999 Total attempts