CYBER SECURITY

2. forduló

Continental The Future in Motion

A kategória támogatója: Continental Automotive Hungary Kft.

Ismertető a feladathoz

Útmutató:

- A **radio button-os kérdésekre** egy helyes válasz van.
- **Ha lejár a feladatlap ideje, a rendszer AUTOMATIKUSAN** beküldi azt az addig megjelölt válaszokkal.
- Az **adatbekérős feladatokra NEM jár részpontszám**, csak a feleletválasztósakra.
- **Badge-ket** a 4.forduló után kapsz majd először.
- Az **adatbekérős kérdéseknél** igyekeztünk minden variációt megadni (kisbetű, nagybetű, szóköz), de ha mégis eltérést tapasztalsz a megoldásokban, kérjük, jelezd felénk!

+1: Azért szólunk, hogy senkit ne a végén érjen meglepetés: a játék nem tipp-mix és csapatkategória sincs! Természetesen akinek nem inge...

Jó versenyzést kívánunk!

A 2. fordulóban a bináris Cézár kódolást gyakorolhatod Cipher block chaining (CBC) módban.

Jó munkát a feladat megoldásához!

Felhasznált idő: 00:00/20:00 **Elért pontszám:** 0/12

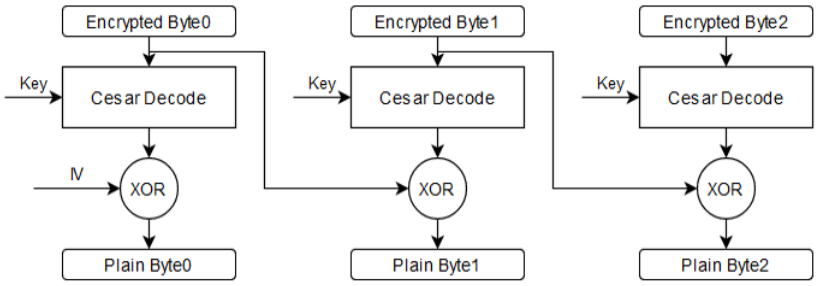
Indítás utáni csatolmányok

1. feladat 0/12 pont

A feladat a mellékelt encrypted.bin fájl dekódolása és a fájlban található utolsó szó (ASCII) meghatározása.

A fájl a Cipher Block Chainig (CBC) módszerrel lett kódolva bináris Cézár kódoló algoritmussal.

Cipher Block Chaining



Magyarázat

- Encrypted Byte#: a kódolt fájl soronkövetkező bájtja
- Key: kulcs a cézár dekódoláshoz (részletek lentebb)
- IV: inicializációs vektor a block chaining első lépéséhez
- XOR: bitenkénti kizáró vagy művelet (programkódban ^ jel)

Bináris Cézár kódolás

A cézár kódolás egy helyettesítő rejtjel, amely során az adott bájtot eltoljuk egy megadott **Key** értékkel pozitív irányba.

Amennyiben az eredmény meghaladná az egy bájton tárolható maximális értéket (255), úgy a skála elejére kerül az új érték (256 ->0, 257->1, stb...)

Mivel a megadott fájl kódolt állapotban van, így a cézár kódolást fordított módban kell használni, vagyis a **Key** értéket kivonni a kódolt bájtból, hogy megkapjuk az eredeti értéket. Értelemszerűen, ha 0-nál kisebb érték jönne ki, akkor a skála tetejéről kell lefelé mozogni (-1-> 255, -2->254)

Paraméterek

Key: 66 (0x42)

IV: 170 (0xAA)

Kérdés

Mi az utolsó szó az **encrypted.bin** fájl dekódolása után megkapott eredeti szövegben?

Válaszok

A helyes válasz:

turpis

turpis.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed bibendum finibus mauris eu volutpat. Proin et dui ut tortor turpis.

Magyarázat

Python mintakód a megoldásra:

```
key = 0x42
iv  = 0xAA

def cesarDecrypt(x):
    dec = x-key
    if dec < 0:
        dec = dec + 0x100
    return dec


data = bytearray()
with open("encrypted.bin", "rb") as f:
    byte = f.read(1)
    while byte:
        data.extend(byte)
        byte = f.read(1)

decData = bytearray()
for i in data:
    dec = cesarDecrypt(i)
    dec = dec ^ iv
    iv = i
    decData.append(dec)

with open("result.txt", "wb") as f:
    f.write(decData)
```

Megoldás:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed bibendum finibus mauris eu volutpat. Proin et dui ut tortor **turpis**.