README.md

in-plain-sight

```
This level is simple: all you have to do is decrypt some HiddenCiphertext! To make it even easier, I'll gi\

You will need:

Algorithm: AES-256-CBC
Key: c086e08ad8ee0ebe7c2320099cfec9eea9a346a108570a4f6494cfe7c2a30ee1
IV: 0a0e176722a95a623f47fa17f02cc16a
```

While attempting another challenge on day two, I came across an interesting article that proved crucial to solving in-plain-sight:

Going the other way with padding oracles: Encrypting arbitrary data!

What is apparently plaintext, may in fact be the cipher text. And with a title 'in plain sight,' let's look for ciphertext candidates.

The 'HiddenCiphertext!' stuck out and I was guessing that it was the ciphertext. Since we need inputs to be multiples of 16, I omitted the exclamation point. Using Python, I converted the key and IV to bytes, and attempted to decrypt 'HiddenCiphertext':

```
>>> import binascii
>>> from Crypto.Cipher import AES
>>> k = binascii.unhexlify('c086e08ad8ee0ebe7c2320099cfec9eea9a346a108570a4f6494cfe7c2a30ee1')
>>> iv = binascii.unhexlify('0a0e176722a95a623f47fa17f02cc16a')
>>> c = 'HiddenCiphertext'
>>> aes = AES.new(k, AES.MODE_CBC, iv)
>>> aes.decrypt(c)
'FLAG:1d010f248d\x01'
```

Recon for the win; always do your homework.