

[Pragyan CTF] Evil Corp

Standard

Description:

fsociety has launched another attack at Evil Corp. However, Evil Corp has decided to encrypt the .dat file with a CBC cipher.

Reports reveal that it is not AES and the key is relatively simple, but the IV might be long. And remember, fsociety and evilcorp are closely linked.

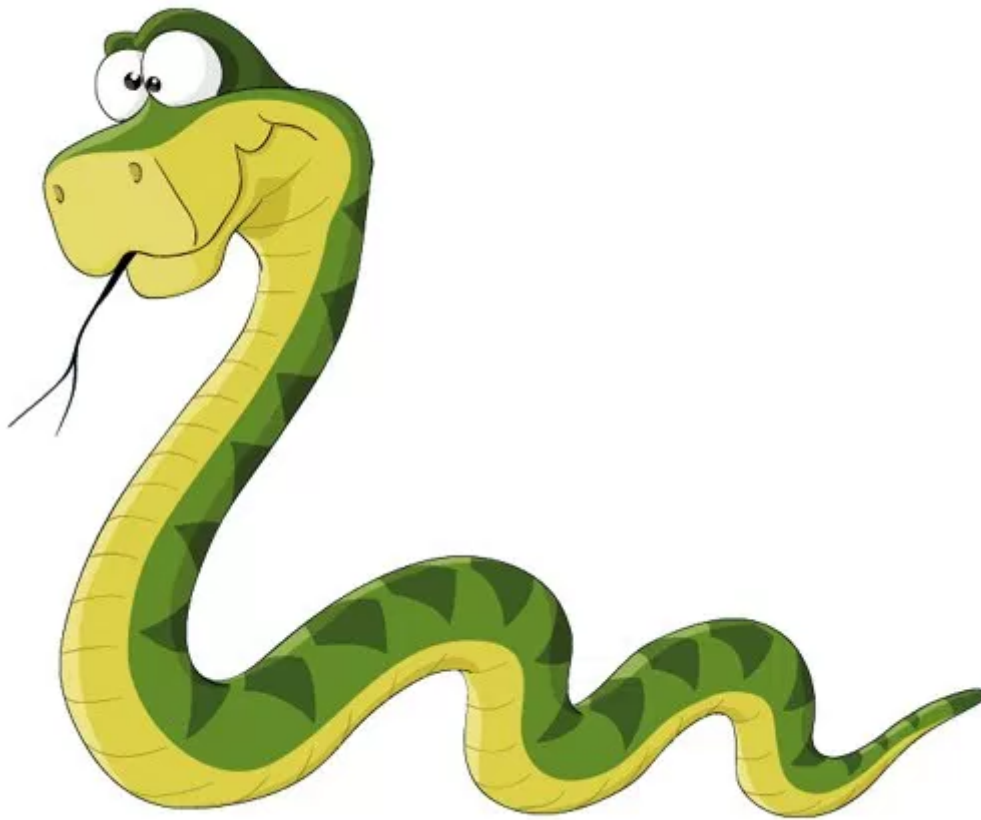
Hint! Snakes serve the fsociety. Hmmm.

Hint! fsociety and evilcorp are too close, even 16 characters long together. Damn

[fsociety_new.dat](#)

This challenge was tricky for lot of people, the riddle was hiding in the questions itself. The challenge doesn't require high skills, just understanding the meaning behind the words and hints.

From the question we know it's a CBC cipher, but which? I got it just after the first hint was released, something to do with **snakes**. hmm... Serpent! Serpent is another term for Snake, and there's Serpent-CBC cipher.



What about the IV? We know several things about the IV:

1. The length of Serpent-CBC IV must be 32 bytes,
2. Most of the Serpent decrypters are taking the IV as hex sequence
3. in the question: “but the IV might be long”
4. in the Hint: “even 16 characters long together...fsociety and evilcorp are closely linked”.

So, this made me believe that the IV is “fsocietyevilcorp” because

`len(hex("fsocietyevilcorp"))==32.`

So we now know the algorithm and the IV, what is the Key? The question says “the key is relatively simple”. So I tried [online](#) with some simple and “obvious” keys until I recognize a valid header of file and found that the key was “*fsociety*”.

Input type: File

File: Browse

Function: SERPENT

Mode: CBC (cipher block chaining)

Key:
(plain)

☒ Plaintext ☐ Hex

Init. vector:

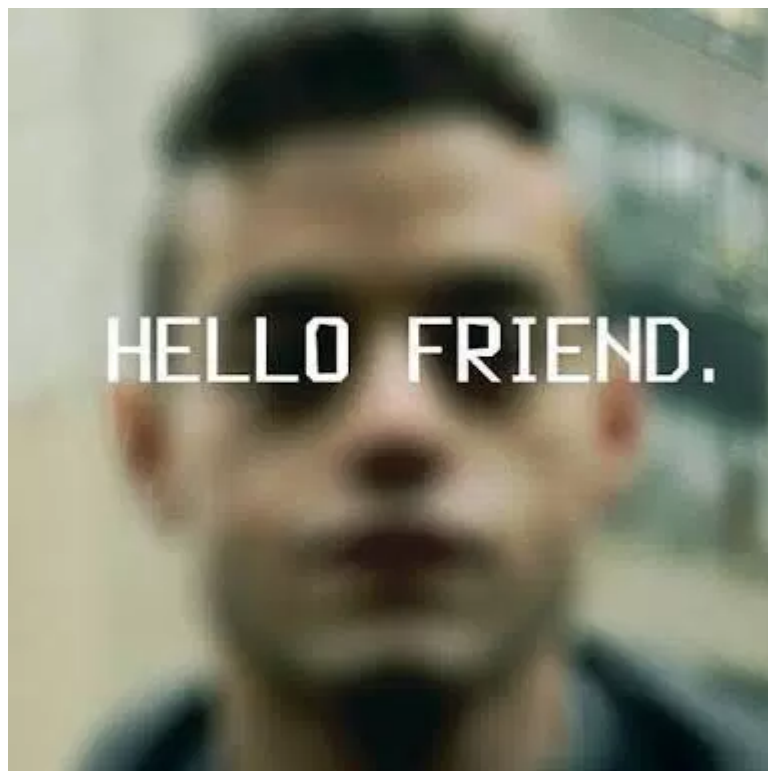
> Encrypt! > Decrypt! ▶ 🔗



Displayed output of your task is restricted to the first 16 kB of data. You can get the full result using the [Download as a binary file link](#).

00000000	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01	ÿ 0 ÿ à . . J F I F
00000010	00 01 00 00 ff e2 02 a0 49 43 43 5f 50 52 4f 46 ÿ à . I C C _ P R O F
00000020	49 4c 45 00 01 01 00 00 02 90 6c 63 6d 73 04 30	I L E l c m s . 0
00000030	00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 df	. . m n t r R G B X Y Z . ß
00000040	00 09 00 08 00 15 00 28 00 07 61 63 73 70 41 50 (. . a c s p A P
00000050	50 4c 00 00 00 00 00 00 00 00 00 00 00 00 00	P L
00000060	00 00 00 00 00 00 00 00 00 00 00 00 f6 d6 00 01 ö Ö . .
00000070	00 00 00 00 d3 2d 6c 63 6d 73 00 00 00 00 00 00 Ö - l c m s

We got a leet JPEG image with the flag:



The flag
was `pragyanctf{hellofriend}`

Viewed using [Just Read](#)