Ciphertext CTF 2020

Cryptography & Steganography

AES_ECB

Description:

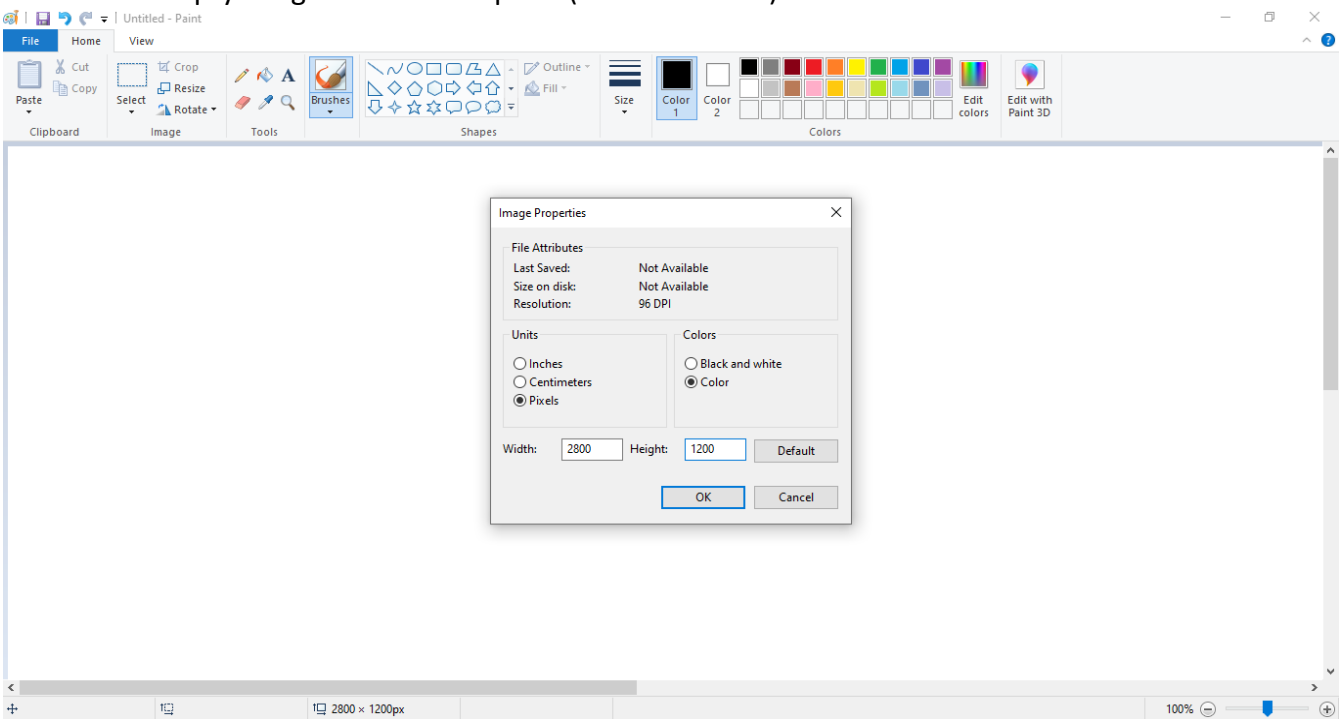
can you see what is on that encrypted picture?
image info before encryption: flag.bmp BMP3 2800x1200 2800x1200+0+0 8-bit sRGB 256c 3.20537MiB 0.020u.

Files:

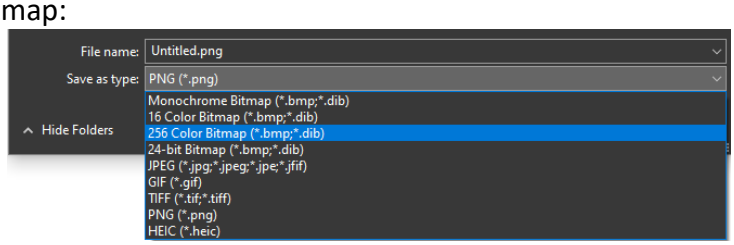
enc_flag Size: 3.283 MB MD5: 6c278cd20c7056e16139ad6e416dd172

Solution:

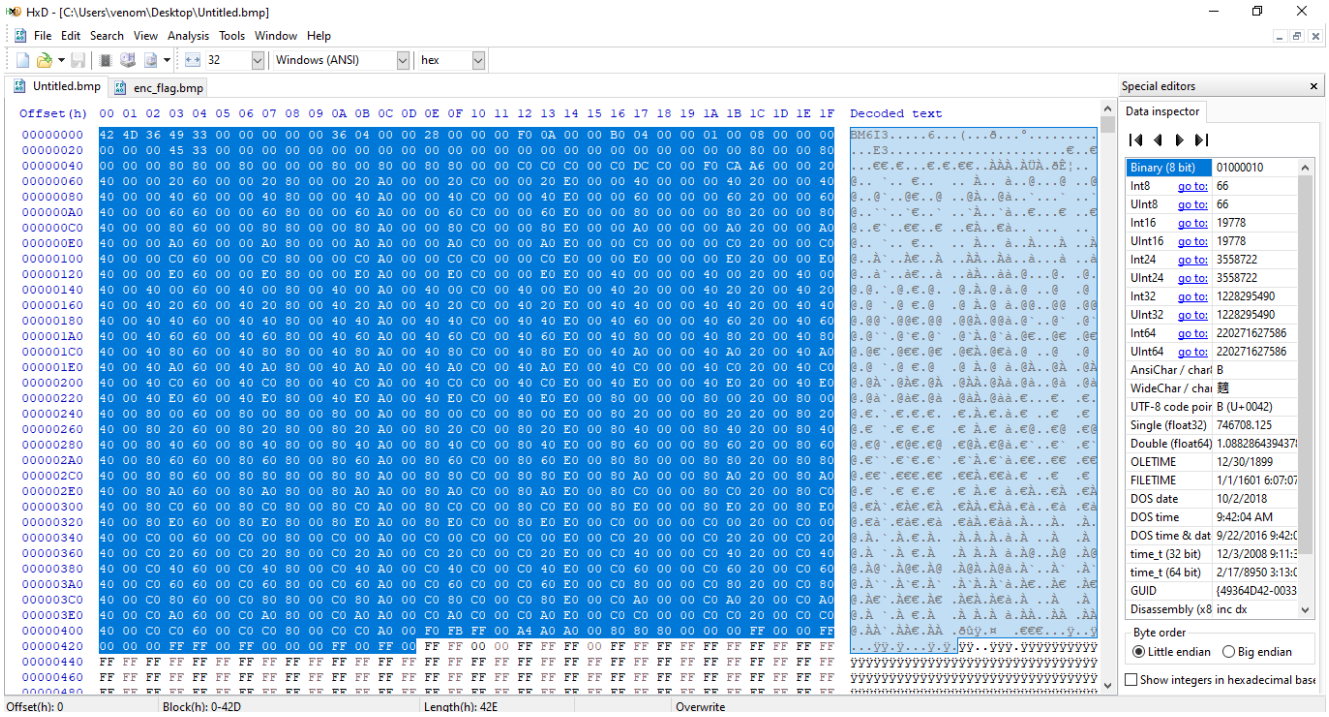
As the name of this challenge says, the picture is encrypted using AES ECB mode, the encrypted image has BMP format which stores pixel arrays as a block of 32-bit DWORDs, that describes the image pixel by pixel. So without the diffusion at encryption, the pattern will be still visible.
ECB lacks diffusion, that's why it is not recommended for large data, while AES provides block-level diffusion ECB doesn't provide data-level diffusion.
Enough theory for now, lets get to work, the solution is as simple as replacing the header of the encrypted image.
The easiest way for constructing a suitable header is to create an empty image with the same specifications provided in challenge description and copy its header and paste it instead of the encrypted header of our image.
Let's create an empty image in Microsoft paint (recommended):



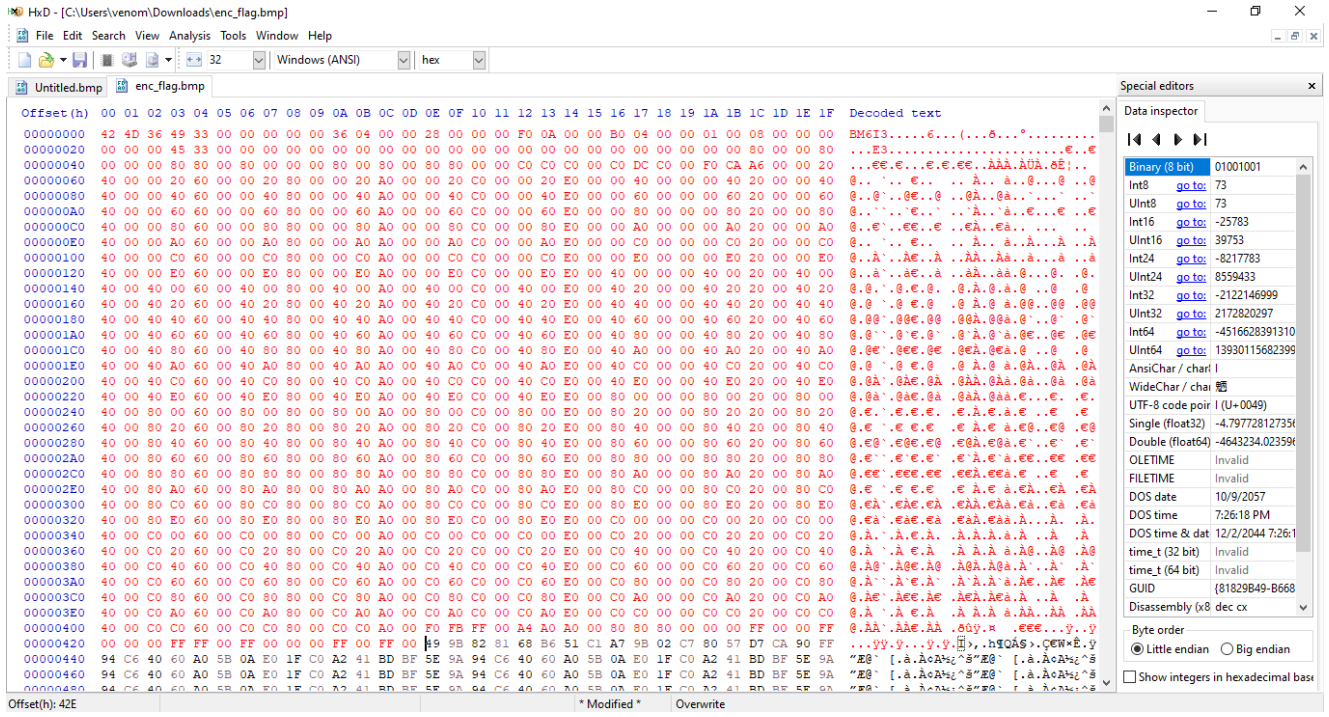
And save it as 256-color bitmap:



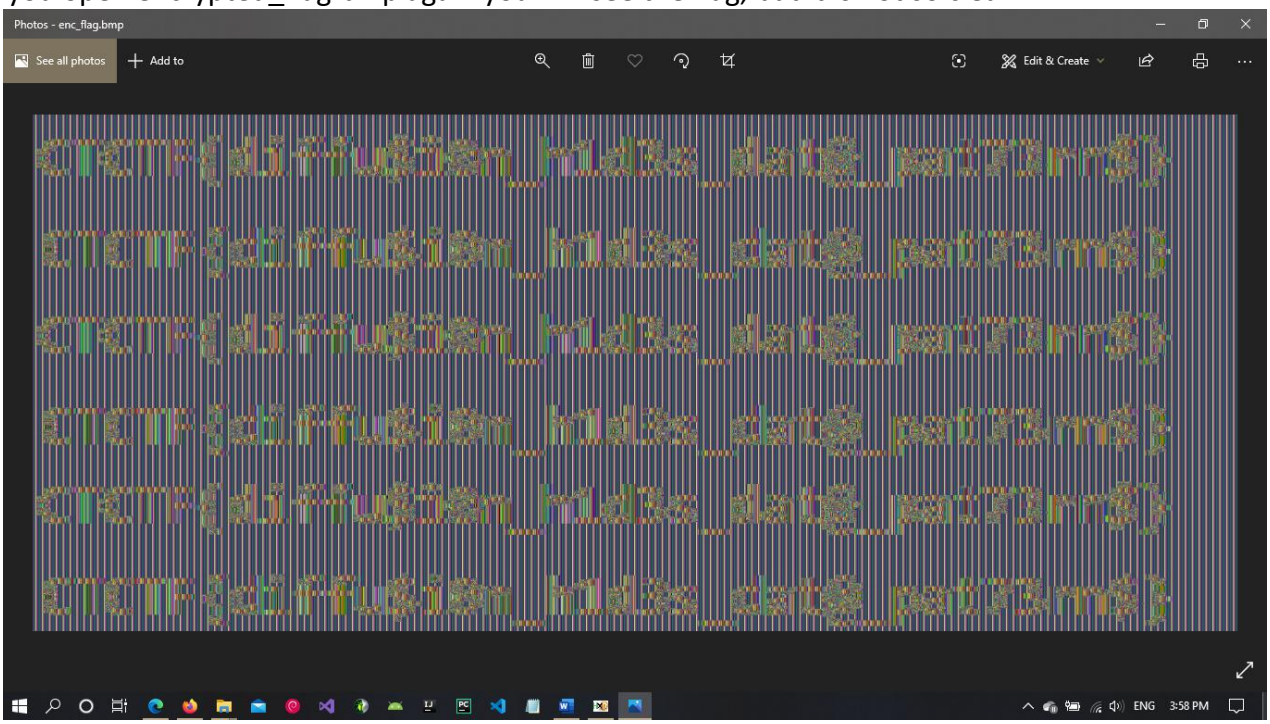
Now let's open both images in a hex editor and replace the header (I used HxD):
Let's take this whole part as a header, because the image we created has only white pixels which represented by FFFFFF, the part before F's start should be the header with all parameters
By the way even if we copied some of pixel data with the header that won't change it much.



Copy it and paste, then save:



Now if you open encrypted_flag.bmp again you will see the flag, but it is not so clear:



At this point, you can open it in [stegsolve] and figure it out.

If you still can't find it, then use [electroniccoloringbook] to get a perfectly clear image:

Run the following command, use more colors after c flag if needed:

$: python2 ElectronicColoringBook.py −S −f −c 32 enc_flag.bmp

```
root@VENOM3:/mnt/c/Users/venom/Desktop/CTCTF_writeups/crypto_and_stego/AES_ECB# python2 ElectronicColoringBook.py -S -f -c 32 enc_flag.bmp
94c64060a05b0ae01fc0a241bdbf5e9a     155456 #00 -> #FF #FF #FF
9d7e357f83ed637f0d861a2d515e82d3       9399 #97 -> #28 #73 #CC
ab05f59004be4e63a4470866199f23ed       1026 #22 -> #CC #A8 #28
7ceae49398da6f103b8d79847b63f062        738 #27 -> #CC #BB #28
890bb88d74b59e1b76f600af423c3ce7        615 #D7 -> #CC #28 #C3
87457941d30c231582adccfc94907adf        585 #AF -> #3A #28 #CC
c3d85ca3b5db17e916b8df6760073830        561 #36 -> #A2 #CC #28
980395dc71dc394f9685fa19b41969d2        558 #47 -> #61 #CC #28
b035cc72dc98795d5a36744eb4b6f587        534 #CD -> #AE #28 #CC
032b52c6afe5ba55cd6b27d7f97d3521        495 #8B -> #28 #A1 #CC
3846e22ea0b38e1940b53249a31f184e        483 #BD -> #70 #28 #CC
47eeb148def86ad7c06692e1bd5ccda4        477 #20 -> #CC #A0 #28
a56c0c1781764dacf1e518d81e187265        477 #AE -> #36 #28 #CC
1e098116802506695dab1ee171eba657        471 #CF -> #B6 #28 #CC
6c7a4a781841196753200d9922994955        459 #1B -> #CC #8D #28
55a7d053585b60bd0a3e593e4c4c4237        453 #BB -> #69 #28 #CC
13d675be08ad41c4ce3f8834a9c8b0c3        429 #56 -> #28 #CC #2A
fe26b7d9b11039918273841c88337544        426 #61 -> #28 #CC #54
d71400437b0f777b20b24c3a5422bf73        417 #D0 -> #BA #28 #CC
27b3aadb28f80fcec0583d7360d2b6b1        408 #87 -> #28 #B1 #CC
6367d469a39d3516c14087f73f50c84b        369 #0C -> #CC #53 #28
caa678a3516c95e0411e36ec5caa4823        363 #C0 -> #7C #28 #CC
1ac4dcc478b6edf54b52dd66f5aeefe7        360 #0D -> #CC #57 #28
8ad88cd062801c58d4e015aae11b7d03        357 #49 -> #59 #CC #28
50ca86d43e205f04a8f3d809171b479b        354 #5A -> #28 #CC #39
986213704e504ccc376f5cd53bf153b7        354 #42 -> #74 #CC #28
028a3d502436150d3d1d1823117230e1        345 #9F -> #28 #54 #CC
ae6cecaa9814778b1dca0f56a3cd0028        339 #EB -> #CC #28 #75
83a9f708767fe233d8a435041c8ee23e        339 #95 -> #28 #7B #CC
41052e7bc56d52afb8b8e90c8ecd389d        336 #B4 -> #4E #28 #CC
2b50bbbf327390da3ed4cdce8dcdf2f5        327 #30 -> #BA #CC #28
********************************      31758 #FF -> #00 #00 #00
Trying to guess ratio between 1:3 and 3:1 ...
Width: from 611 to 5499
Sampling: 1000
Progress: 700 800 900 1000 1100 1200 1300 1400 1500 1600 1700 1800 1900 2000 2100 2200 2300 2400 2500 2600 2700 2800 2900 3000 3100 3200 3300 3400 3500 3600 3700 3800 3
900 4000 4100 4200 4300 4400 4500 4600 4700 4800 4900 5000 5100 5200 5300 5400
Size:  (2800, 1200)
Saving output into enc_flag.bmp.b16_p1_c32_x2800_y1200.png
root@VENOM3:/mnt/c/Users/venom/Desktop/CTCTF_writeups/crypto_and_stego/AES_ECB#
```

As a result, we get the following image:

The flag is: CTCTF{diffu$i0n_h1d3s_dat@_pat73rn$}.