Crypto CTF

Problem 1

- I started with reading all letters then used the English letters frequency analysis study from Wikipedia in this link https://en.wikipedia.org/wiki/Letter_frequency and then generate a dictionary
- After that I examined the decrypted text there’s some words that was about to be correct then I tried to fix these words by changing the dictionary letters until I got an understandable words
- The flag is : `SOME_TEXT`

Problem 2

- After Analyzing the packet using packet viewer which we used here https://apackets.com/
- We examine that there’s a familiar pattern of flags found in the response example of the GET done by ip and port 192.168.38.104:64093
- we found this Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}
- we examine that the word cvpbPGS can reach to picoCTF as the absolute difference between 2 words is 13
- So after decryption we found that : **The flag is picoCTF{p33kab00_1_s33_u_deadbeef}**
- Note :- we also applied the decryption algorithm on what inside {} and we didn’t apply anything to numbers

Problem 3

- I started by reading the 2 images
- I examined that the summation of most of the 2 images is 255 in all channels which form white color
- So what about adding all pixels RGB channel together (R channel 1 + R channel 2, G channel 1 + G channel 2, etc …)
- The flag : `picoCTF`
- The message : `d72ea4af`

Problem 4

- Firstly I shifted all words by 1 bit shift
- Then I followed the hint when in doubt shift
- The flag is : `fastctf`
- The message :-

`Hello and welcome in file00 Forensic challenge. This is just filler text to make it longer.`

`fastctf{a-bit-tricky}`

Problem 5

- It can be solved by using grep command or simply opening the text in notepad
- The flag is : `picoCTF`
- The message is : `grep_is_good_to_find_things_dba08a45`

Problem 6

Algorithm (I depended on the encryption algorithm)

1. Applying the inverse Caesar shift algorithm
2. applying decode base 16 which is getting each pair of characters in the string and take difference of it and 97 which is order of ‘a’ then shifting and adding them to form the ascii code

3. You then got the plain text

In this problem I got the key trying different letters form (a - z) depending on hint that key is single letter

- The flag is : `SOME_TEXT`
- The message : `The enemies are making a move. We need to act fast.`

Problem 7

- We tried many steganography decoding mechanisms like examining histograms, LSB for each pixel, etc…… but in vain so we detect another steganography algorithm but Unfortunately it requires key we found that the project statement about this CTF has strange word case as HIDING is Uppercase without any punctuation reason for that so why not trying this as key
- We used this key and image as inputs to this website https://futureboy.us/stegano/decinput.html it outputs this message
- The message :- `Hello, the flag is CMPN{Spring2024}`
- The flag is : `CMPN`
- The message is : `Spring2024`

Problem 8

This is Morse Code Audio

- The message: THE RUSSIAN TERRORISTS ARE THE ONES WHO STARTED THIS, THEY ARE THE KEY. PLEASE Y MUST EXTRACT ME