

Challenge: Gonna Lift Em All

Challenge Description :

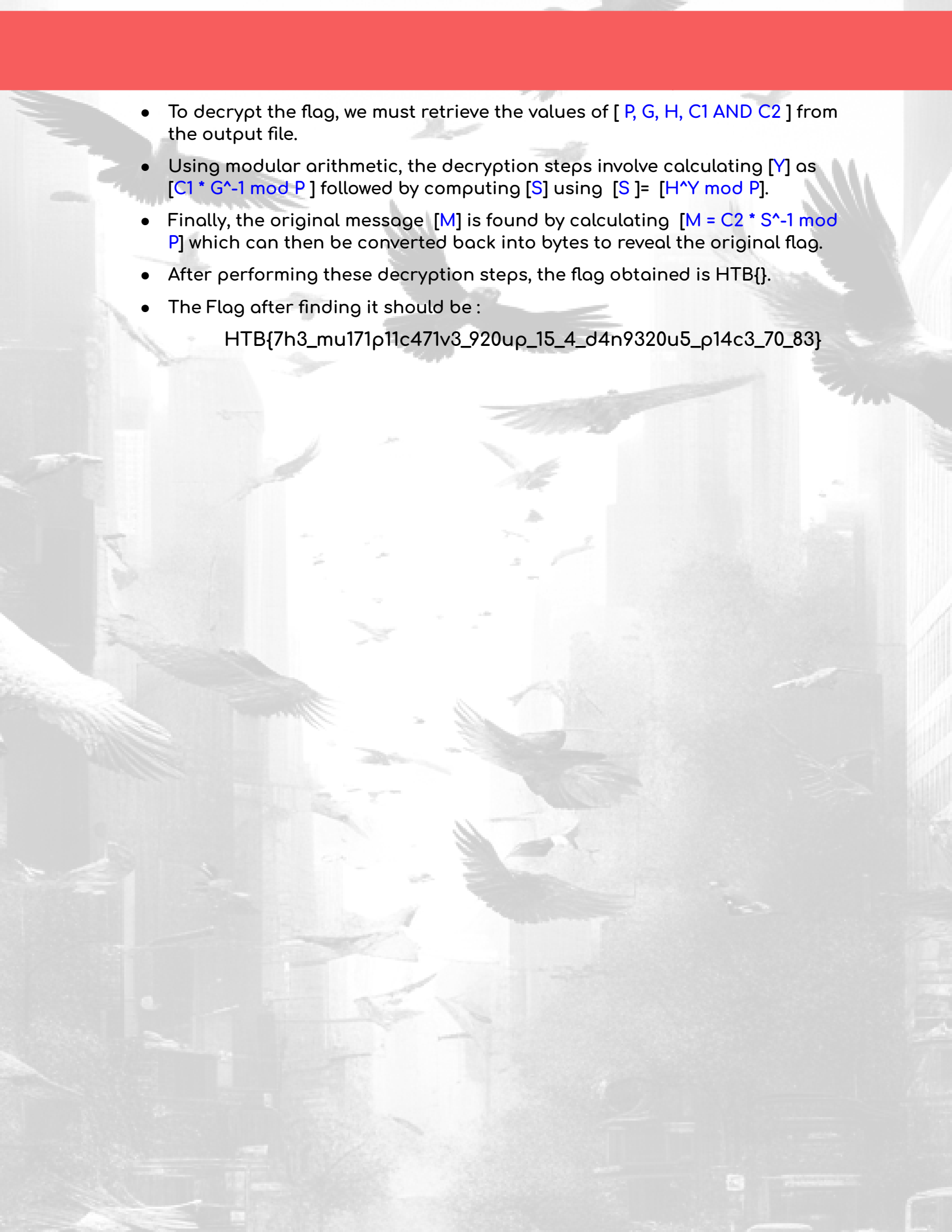
Quick, theres a new custom Pokemon in the bush called The Custom Pokemon. Can you find out what its weakness is and capture it?

Context :

- You are given a .EML file, a weird plain text format for emails, basically just analyze it, open the file up and get both base64 encoded strings. From there analyze the code you are given and find the flag.

Flag :

- First Install the files and install the files. You can open it with a notepad or any basic text editor.
- The Python script encrypts a flag using mathematical operations based on modular arithmetic. The encryption process begins with the `gen_params()` function, which generates key parameters:
 - A large prime number p ,
 - A random integer g between 2 and $p-2$,
 - A random integer x within the same range,
 - And h , computed as $g^x \bmod p$.
- These parameters are essential for the algorithm.
- The encryption occurs in the `encrypt(pubkey)` function. Here, the flag is converted into a large integer $[M]$.
- A random integer $[Y]$ is then chosen, and the value of $[S]$ is calculated using the formula $[S = H^Y \bmod p]$.
- The ciphertext consists of two parts: $[C1]$ which is calculated as $[G^Y \bmod p]$ and $[C2]$, computed as $[(M * S) \bmod P]$. These values form the encrypted representation of the flag.
- In the `main()` function, the code generates the necessary parameters and writes the values of $[P, G, H, C1 \text{ AND } C2]$ to a file named `data.txt`, which is the output of the encryption process.

- 
- To decrypt the flag, we must retrieve the values of [P , G , H , $C1$ AND $C2$] from the output file.
 - Using modular arithmetic, the decryption steps involve calculating [Y] as [$C1 * G^{-1} \bmod P$] followed by computing [S] using [S] = [$H^Y \bmod P$].
 - Finally, the original message [M] is found by calculating [$M = C2 * S^{-1} \bmod P$] which can then be converted back into bytes to reveal the original flag.
 - After performing these decryption steps, the flag obtained is HTB{ }.
 - The Flag after finding it should be :

HTB{7h3_mu171p11c471v3_920up_15_4_d4n9320u5_p14c3_70_83}