Description(Visible to students)

You work for a secret intelligence agency. One of your undercover agent managed to steal an important intel from “Enemy of the State Corporation”. You know that they use a new encryption scheme with Shift CPB Cipher (contains md5). Unfortunately, the specification of the cipher was incomplete because he didn’t have top level clearance. The director wants you to crack the encrypted file and get the intel.
Hint: think about the input and output length

Directions for Solving the Challenge (Visible instructors only)

The objective for this part is to decrypt the secret file to get the first part of the intel, as well as find the 3-character key. The first part of the intel is encrypted using a Shift-CFB cipher (*You can find the details about this cipher in Top Secret Revealed.jpg*). You need to implement a CFB structure, along with a full range Ascii shift cipher. The correct key for the Shift-CFB cipher will be a MD5 hash digest of a 3-character long lower case English word. You can use brute-force method to find the correct key “ITA” , by applying all possible keys to the Shift-CFB cipher you developed.

For the second part of the intel, you will need the hints, which are the 3-character key you get from the last step and the plain text that you have decrypted. The plaintext will contain the first part of the flag and a website address. The key will be an English word, more specifically, a country name. Then you need to locate the image that contains the flag of that country on the web page given and download it. The second part of the intel is hide in the source code of the image.

Finally, the flag will be the result of concatenating two secret intel.

Flag: kopictf{I4am9Hao9zhang-ha0-w1sh-y0u-A-900d-day}