## **Introduction**

The national security agency acquired a USB drive that contains an encrypted file and a web page, from a foreign secret spy, and there’s a secret intel hide inside it. From the interrogation, you know that you will need a \*Shift-CFB cipher and MD5 to find the first part of the secret intel, as well as a 5-character hint, from the encrypted file. The second part of the intel is hide in the web page. They want you to find out what is the secret intel the spy is trying to deliver.

*\*Shift-CFB cipher: In CFB mode, instead of AES, a simple shift cipher is used as the encryption method. The second input (apart from the key) for each round will be the last few bits (still deciding how many) from the cipher text you get from the last round.*

## **Directions for Solving the Challenge:**

The objective for this part is to decrypt the secret file to get the first part of the intel, as well as find the 5-character key. The first part of the intel, it is encrypted using a Shift-CFB cipher (Replacing the AES method in AES-CFB encryption with Shift cipher). You need to implement a CFB structure, along with a simple shift cipher, whose key will be the last few bits from the cipher text you get from the last round of the encryption. The key for the Shift-CFB cipher will be a MD5 hash digest of a 5-character long English word. You can use brute-force method to find the correct key, by applying all possible keys to the Shift-CFB cipher you developed.

For the second part of the intel, you will need the hint, which is the 5-character key you get from the last step. 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 code of the image.

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