## **Introduction**

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

*\*Simplified-AES-CFB cipher: In CFB mode, instead of AES, a simplified AES is used as the encryption method. You can refer to the attached pdf for more details.*

## **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 is encrypted using a SAES-CFB cipher (Replacing the AES method in AES-CFB encryption with a simplified version). You need to implement a CFB structure, along with a simplified AES cipher. The correct key for the SAES-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 SAES-CFB cipher you developed.

For the second part of the intel, you will need the hints, which are the 5-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 code of the image.

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

e.g., ‘kopiCTF{<first + second>}’.