Challenge: Perfect Synchronization

Challenge Description :

The final stage of your initialization sequence is mastering cutting-edge technology tools that can be life-changing. One of these tools is quipqiup, an automated tool for frequency analysis and breaking substitution ciphers. This is the ultimate challenge, simulating the use of AES encryption to protect a message. Can you break it?

Context :

- You have a Python script that encrypts a secret message (the flag) using AES encryption in ECB mode. The message consists of uppercase letters, underscores, curly braces, and spaces. The output of the flag is called Output.txt

Flag :

- This one is pretty straightforward.
- The encryption process uses AES in ECB mode to encrypt each character of a message, which consists of only uppercase letters, underscores, curly brackets, and spaces—up to 30 unique characters in total. This means there are at most 30 unique ciphertext blocks.
- To decode the message, we analyze the ciphertext frequency. Unique ciphertexts, which appear only once, help us identify specific characters like: { a}/{ b}/{ c}. We create a mapping from ciphertexts to characters, allowing us to easily decrypt the message.
- By checking the ciphertexts against this mapping, we can reconstruct the original message, filling in gaps with educated guesses based on context and frequency.

The Flag is : HTB{SIMPLE_SUBSTITUTION_CIPHER}