Use of Same Key for Encryption and Decryption:

- **Drawback:** AES uses the same key for both encryption and decryption, which is known as symmetric encryption. If an attacker gains access to the key, they can decrypt all encrypted data. Therefore, protecting the secrecy of the key is crucial.

Same Key Used for All Blocks - Preservation of Pattern:

- **Drawback:** AES operates on fixed-size blocks of data (128 bits or 16 bytes for AES-128). When encrypting multiple blocks of the same data, the same key is used for each block. This can potentially lead to patterns in the ciphertext if the plaintext blocks are the same

Usage of Null Padding is Insecure:

- **Drawback:** Null padding (adding null bytes to the end of plaintext to make it a multiple of the block size) can be insecure in some cases. Null bytes can be easily removed from the end of ciphertext, and the padding scheme doesn't provide integrity protection.