Question 4

Security Flaws

1. Limited Key Reuse: Reusing the same key for encrypting all blocks of data is not recommended, especially having a large number of blocks. A secure key management strategy should be considered for better security.

2. Patterns : Encrypting each block separately using the same key is known is not suitable for encrypting large amounts of data, as it does not provide semantic security. Identical plaintext blocks will result in identical ciphertext blocks, which can leak information about the plaintext.Further, the patterns in the plaintext could lead to patterns in the ciphertext, which can be exploited by attackers to gain information about the plaintext.