The encryption scheme used in section B of the assignment has some security flaws stated below:

- The encryption key used is only 16 bits. Such a key might be highly susceptible if an attacker uses the brute force approach.

- Same key is used to encrypt each block of data, which makes the blocks of data independent of each other. In such a case, an attacker can resort to educated guessing to find out what the cipher says without decrypting it. For example, if somehow the attacker finds out that ciphertext1 means Hello, the attacker can take a guess that ciphertext2 will either mean World or There etc.

- The block size being limited is another security flaw. The block size is only 16 bits long, this makes only 2^16=65536 possible block values for each block. Using the brute force algorithm, an attacker can find out what the cipher means.

- The padding used in the encryption process is not random. Using null bytes (00 hex) to perform padding creates a deterministic environment for the attacker. The lack of unpredictability raises a security threat because an attacker might be able to analyze the patterns in the cipher.