Security Flaws in the Encryption Scheme

1. **Same Key for Every Block**: Using the same key to encrypt every block of the message means that if parts of the message are the same, their encrypted versions will also be the same. This makes it easier for attackers to guess the original content.
2. **Null Byte Padding Issues**: If the message has null bytes (zeros) in it, padding with null bytes can make decryption confusing or incorrect, as it's hard to tell what's part of the message and what's padding.
3. **Key is Too Small**: A 16-bit key is very short and easy for attackers to crack by trying all possible combinations (a brute-force attack).
4. **Simple Substitution**: If the encryption just substitutes parts of the message with other parts (like using a basic S-box), an attacker can use statistical patterns in the message to figure out what the original text was.
5. **Small Block Size**: Small block sizes can be a problem because attackers might be able to rearrange or swap blocks to change the message without breaking the encryption, which makes the scheme less secure.