Question 1

A block cipher with an 8-bit block size is very easy to break with a known-plaintext attack (assuming each block is just encrypted independently with the same key). Describe how you would do so.

A known-plaintext attack on an 8-bit block cipher involves creating a complete mapping of all possible plaintext blocks to their corresponding ciphertext blocks. Since there are only 256 possible 8-bit blocks, it is practical to encrypt each one with the cipher under the known key and record the output. This results in a substitution table mapping every possible plaintext to a ciphertext. Once this table is constructed, any encrypted message can be decrypted by looking up each block of ciphertext in the table and replacing it with the corresponding plaintext.

Question 2 (10 points)

Assume you're sending a long message using a block cipher (like AES) with the following scheme: split the message into block-sized chunks, then encrypt each with the same key. Basically Alice sends Bob AES(m1, k), AES(m2, k), AES(m3, k), etc.

Part A (3 points): Even if they can't decrypt blocks, what information can an eavesdropper discern from this scheme? Hint: Imagine that Alice is sending a table of data where each cell is exactly one block of data.

Part B (4 points): Things are actually even worse! A malicious attacker can actually CHANGE the message that Bob receives from Alice (slightly). How? This is particularly bad if the attacker knows the structure of the data being sent (like in part A).

Part C (3 points): How could you modify the scheme to mitigate/prevent these types of attack?

Part A: An eavesdropper can discern patterns in the encrypted message. If the same block of plaintext is encrypted multiple times (such as repetitive data in a table where each cell is exactly one block), it will result in the same ciphertext block each time. Thus, an eavesdropper can identify repeating blocks and infer that the same plaintext block is being sent.

Part B: A malicious attacker can change the message by performing a bit-flipping attack on the ciphertext. By altering bits in the encrypted blocks, the attacker can cause predictable changes in the corresponding plaintext blocks, even without knowing the encryption key. If the structure of the data is known, they can potentially manipulate specific fields or entries within the table.

Part C: To mitigate these types of attacks, one could use an encryption mode that incorporates an initialization vector (IV) and chaining like Cipher Block Chaining (CBC) or Counter (CTR) mode, which ensure that the same plaintext block will encrypt to a different ciphertext block each time. Additionally, adding a message authentication code (MAC) or using an authenticated encryption mode like Galois/Counter Mode (GCM) can help to ensure the integrity and authenticity of the encrypted data, preventing an attacker from undetectably modifying the message.