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.**

With a known-plaintext attack, the attacker has access to a message pair– the plaintext (input) and its corresponding ciphertext (output). If the message block is 8 bits, that means there are only 256 (2^8) unique message blocks that can be sent, thus there are 256 possible message pairs that cover the entire range of the plaintext inputs and their corresponding ciphertext outputs.

The attacker then only needs to collect 256 pairs to have the full message pair collection. This allows for an attacker to then create a table that directly maps the plaintext to ciphertext for the entire encryption operation. Now for any future messages, the attacker doesn't have to know the key–they can simply look the ciphertext up in their table to find its corresponding plaintext.

2. **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.**

    a. **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.**
    If the message has any repetition (which can happen with tabular message or pictures) and each message block is encoded with the same key then the repetition will show up inside the encrypted message. An eavesdropper can notice these repeats and figure out that certain blocks of message are identical without knowing the actual content. The easedroper could also figure out the type of communication based on the number to block ciphers–like if they know that a certain type of transaction or message has a fixed length.

    b. **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).**
    This can happen because the encryption of each block is independent of the other 2 blocks. The attacker can reorder the blocks of ciphertext without affecting their decryption and this reordering could change the message meaningfully. The attacker could replace one block of ciphertext with another. The attacker could duplicate blocks of ciphertext, thus the plaintext block will also be duplicated during decryption. This attack tactic can be used to make numbers bigger than

their true value or repeat specific actions for messages concerning operations or transactions.

c. **How could you modify the scheme to mitigate/prevent these types of attack?**
   Instead of encrypting each block independently with the same key we can bind the blocks together, so that changes to one block affect the decryption of the other 2 blocks and this can be done with cipher block chaining (Mode of Operation). CBC takes each plaintext block and XOR's it with the previous ciphertext block before being encrypted. An initialization vector is used for the first block since there is no previous block.

   This makes it so repeat plaintext blocks have different ciphertext blocks, and also prevents an attacker from being able to change parts of the message without detection.

3.