**1.** Collect pairs of known plaintext and ciphertext: First, we need to obtain some known plaintext and its corresponding ciphertext. In 8-bit block encryption, since the block size is very small, there are theoretically only 256 possible inputs (2 to the 8th power), which means we can quickly map out all possible plaintext-to-ciphertext conversions.

Establish a mapping between plaintext and ciphertext: By looking at known pairs of plaintext and ciphertext, we can begin to build a mapping table. This mapping table includes all possible 8-bit combinations and their encrypted results. Since the block size is small, it is feasible to complete this mapping table.

Decryption process: Once we have the complete mapping table, decrypting the unknown ciphertext becomes very straightforward. Just split the ciphertext into 8-bit chunks and find the corresponding plaintext for each chunk.

**2.** **a:** Even if an eavesdropper cannot decrypt individual blocks, they can still learn something from this scheme. Especially if Alice sends a data table where each cell is exactly the size of a data block, then an eavesdropper can infer some pattern by observing the repetition of encrypted data blocks. For example, if two or more encrypted blocks are identical, this means that their plaintext is also identical. This exposes repeating patterns in the data, such as repeated values in a data table. Therefore, even without knowing the specific content, the eavesdropper can understand some structural information of the data.

**b:** Even worse, a malicious attacker can actually change the message Bob receives from Alice. This is achieved through a so-called replay attack. For example, an attacker could intercept encrypted data blocks and rearrange them, or send certain blocks repeatedly but not others. If an attacker knows the structure of the data being sent (as mentioned in part a), they can use this to change the meaning of the message, such as changing certain values in a table or the order of rows and columns. This attack is particularly dangerous because it changes the message content without decrypting the message.

**c:** In order to mitigate or prevent these types of attacks, the scheme can be modified by using a chain encryption mode such as CBC (Cipher Block Chaining) or GCM (Galois/Counter Mode). These modes mix the encryption result of the previous block with the plaintext of the current block in some way before encrypting each block of data. This ensures that even two identical plaintext blocks will be encrypted due to their different positions. into different ciphertext blocks. In addition, using a model such as GCM can also provide message integrity verification and authentication to prevent unauthorized changes. Through such measures, the security of communication can be significantly improved, preventing eavesdroppers from obtaining useful information and preventing malicious changes to messages.