Crypto Homework 1: Blocks and Streams

Question 1 -

An 8-bit block size means that each character is translated to exactly one other character. There isn't any mixing of values between adjacent characters in the ciphertext and so that makes making some guesses about the nature of the plaintext much easier. For instance, you might assume that the most frequent character you see (and you know that character will be the result of a 1-to-1 swap) is a space character and other most frequent characters might be vowels. You still will have to make a brute force attack, but there are a lot of hints that an 8-bit block size provides for the attacker.

Question 2 -

A) The size is certainly available to the attacker and some level of structure can probably be determined as well. Unless the block size is very large it's likely that it will produce some duplicates and any duplicate might give the attacker some idea of the format and maybe, eventually, the content of the message. For instance, if each row in an encrypted datasheet is a long and then two ints they it's likely that over time the attacker might be able to guess that information.

B) There is nothing to stop the attacker from either scrambling the order of packets or adding nonsense packets of their own, too. At the best this might be inconvenient for the receiver to make sense of and at worse might invalidate the data completely. Also, If the attacker is able to deduce something about the structure of the message it's possible that they could even add in an appropriately sized data structure that might not be immediately obvious as garbage, as well.

C) Increasing the size of the block cipher never hurts (thought it does get more expensive to encode and decode) and would make it harder for an attacker to get a good idea of the message's structure. Including some metadata with the block messages might be helpful, too. Listing the location of the block in the overall message as part of the ciphertext would prevent block scrambling and block addition.