Crypto Homework 1: Blocks and Streams

Question 1:

An 8 bit block size is tiny, particularly with the assumption that each of these blocks is encrypted independently with the same key, there are only 256 options (2 ^ 8) for any given block. If this is a known-plaintext attack, we know pairs of the cipher text and the plain text for a given message(i.e we know the word “attack” in plain text and we know its corresponding cipher text). In general, If the message is larger than 256 characters, we will have repeated cipher text as we have surpassed the number of possible unique values. Additionally if there are repeated input values of plain text, we will get the same ciphertext for those.
In ECB if we know the ciphertext for a given plaintext, we know the key and can compute the rest of the plaintext from the cipher text
For cipher block chaining, if we know at least 2 consecutive plaintext/ciphertext combos, we can easily deduce the key by xor-ing the previous ciphertext with the next plaintext, whatever we get will reveal the key as it will be the difference between the plaintext and ciphertext for that block

Question 2:

a. They would be able to see the number of blocks being sent, the general message length and I guess who the messages is being sent from and to
b. If you noticed the pattern of things being sent, you could intercept and send a different block than the expected one (i.e. flip sending the 2nd and 3rd block so the 3rd is sent before the 2nd one). Or copy and send duplicate blocks.You can’t modify individual bits because this causes an avalanche effect in that specific block and Bob will know the block has been modified
c. Send a hashed authentication code with each block to verify things are in the correct order that can be verified on both sides. :)

Question 3: when a single bit is flipped it causes a cascading effect (avalanche effect) that causes the decryption of the message to fail. This protects against bit flipping attacks as we can easily tell the encrypted message has been modified