Devin Sevy

Question 1

Since the block is only 8 decoded bits, the block of data lies within a 256 possible answers. If the 1 byte was not correct, simply XOR the previous block and continue checking. You would only have to set one round of checks.

Question2

a. Makes it easier to decrypt the keystream. Since Alice is sending the same size blocks, the key can be derived from this size. When XORing the previous bits, the attacker knows the exact size to use on the next bits coming across.

b. Since the blocks are the same size, they contain the same key when decrypting the message on Bob's end. When the stream is set in the same size blocks, the order does not matter as Bob is decrypting the message. The attacker can change the order or delete blocks, and at Bob's end, he would not know the difference.

c. Cypher Block Chaining, Alice can send the same blocks but before encrypting a block, XOR it with the cyphertext of the previous block. It will make it less susceptible to rearrangement, but can be susceptible to bit flipping.