Crypto Homework 1

Question 1:

- Look for most frequently recurring characters. Charts are easily available for English, and likely in other languages. From there you could also deduce words based on any provided punctuation. For every letter solved, words become more evident and from there context of other words.

Question 2:

A:

If it's using the same key for each block, patterns would begin to manifest quickly and could be decifiered. They could also recognize data that was the same, even though it'd gone through the encryption.

B:

If they figure out the key, or even parts of the key, the can begin to change data to mean different things when they intercept it, and then send that on to Bob.

C:

Assuming the keys can be transmitted securely, need to change the key each round (similar to AES).

Question 3:

See attached code

Question 4:

See attached code