**Crypto Homework 1: Blocks and Streams**

## Question 1

We can approach this by decoding the words which are common and known, like and, I, a, etc. Once we are able to crack those, we can identify the key or the cipher used for the encryption. We can follow the same key for the other letters.

## Question 2

1. Even if the eavesdropper cannot discern the message, he/she will have a good idea about what could be the size of each message block. Based on this information, one could determine the size of the substitution table (the range of values the substitution table could have).
2. If the attacker knows the structure of the data being sent, they could manipulate the message by changing the value of each block with a range that lies between the size of the substitution table.
3. We can prevent this attack by using varying-size substitution table sets where each table should be of a different size. Or we can have data blocks of different or large sizes and create substitution tables of sizes that can accommodate the data size. This will make it difficult for the attacker to predict the data size and what the manipulated value could be.