Practical Cryptography

Assignment 1

Runjie Zhang

Problem 4:

To use a single key that is at least as long as the message, it will be impossible for adversaries to analyze the key length theoretically. Because, the reason we can analyze the key length of Vigenere cipher is the length of key is much shorter than the length of message in most of the scenario. The key then has to be used repeatedly. Therefore, the letters which have the same intervals of the key length will be encrypted by the same letter. We can then guess the key length by using index of coincidence and finally recovered the key based on the key length using frequency analysis. On the other hand, if the key length is at least as long as the length of message, we can apply the method, index of coincidence, to guess the key length since the key is not used repeatedly. Therefore, much safer in this case.

In the case which the length of message is not too long, we can use the key which length is at least as long as the message to ensure it. Because it is more practical to do it in short message than a long one.