## Problem 5.1.

Within this homework, we consider that the Vigenère cipher is designed for 26 characters, where each letter is assigned its position in the alphabet: $A \to 0, B \to 1, \ldots, Z \to 25$. The encryption is done by adding the (repeated) key with the plaintext and then taking modulo 26. Assume that you have intercepted the following ciphertext which was encrypted either using monoalphabetic substitution or using the Vigenère cipher:
`EBGRYCXGBGHITURSYNEAVCGBGRYV`
Also, you have managed to find out 4 letters of the plaintext message:
`T****************U**I**I***`

1. Can you tell if the message was encrypted with the Vigenère cipher or by means of monoalphabetic substitution?
2. Using the previous question, can you find the key and the plaintext?
   Hint: the key and plaintext consist of English words.

## Problem 5.2.

Let $n$ be a positive integer, and $M$ a uniformly distributed message of length $2n$ over the alphabet $\mathcal{A} = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$. Given a key $K$, let $V_K(M)$ be the Vigenère encryption of $M$ with key $K$.

1. You have a key $K$ of length $n$, uniformly distributed in $\mathcal{A}^n$.
   (a) Does the encryption $V_K(M)$ provide perfect secrecy?
   (b) Is your answer to the previous question still true if $M$ is not uniformly distributed?
   (c) Is there any way to encrypt $M$ with a key of length $n$ taken from $\mathcal{A}^n$ that provides perfect secrecy?
2. You have two keys $K_1$ and $K_2$ each of length $n$ chosen uniformly and independently in $\mathcal{A}^n$.
   (a) Does the double encryption $V_{K_2}(V_{K_1}(M))$ provide perfect secrecy?
   (b) Let $K_1||K_2$ denote the concatenation of the two keys. Does $V_{K_1||K_2}(M)$ provide perfect secrecy? Does the answer require $M$ to be uniformly distributed in $\mathcal{A}^{2n}$?
3. Now fix $n = 4$. A crime lord learned about the betrayal of three of his men, Matt, Axel and Kyle. He decides that some will be killed, and some will simply be sent a warning, by receiving the kiss of death (as a caution). He sends the orders to his hitman: messages of the form $M = A||B$ where $A \in \{\mathtt{kiss}, \mathtt{kill}\}$ and $B \in \{\mathtt{matt}, \mathtt{axel}, \mathtt{kyle}\}$.
   (a) Suppose the messages are encrypted as $V_K(M)$ for keys $K$ of length 4 (different for each message). Decrypt the two ciphertexts
   $$C_1 = \mathtt{iolgielz}, \text{ and } C_2 = \mathtt{gikdiale}.$$
   (b) Suppose the key $K$ is of length 8, but the same is used to encrypt all the messages. You intercept
   $$C_1 = \mathtt{xwcxlzkj}, \text{ and } C_2 = \mathtt{xwjenbsy}.$$
   Who will the hitman kill, and who will receive a warning?