

HOMEWORK 10

Submission deadline: 5 Dec 2019, 20:00.

QUESTION 1

The aim of this exercise is to implement the suggestion made by Gregory in class. You are asked to amend the program for the caesar cipher seen in class, in such a way that the ascii values are not used. You should cover both encryption and decryption.

QUESTION 2

Amend the Vigenere cipher program seen in class to include white spaces and punctuation signs. You should cover both encryption and decryption.

1. QUESTION 3

Using your answer to question 2, decrypt the following message “LM LETB ZT UHC-NXOGS, KNLE IKNNT”. All we know is that it was encrypted using the Vigenere cipher method. You may use a dictionary attack for that (see files in attachment). Which key was used to do the encryption? Explain what you had to do to have the small program running.