INCS741-Assignment 2

ROW TRANSPOSITION CIPHER IMPLEMENTATION

Question 1:

Using any programming language of your choice, implement the Row Transposition Cipher encryption algorithm. [15 marks]

- **Specifications:**
    - The program should take two inputs 1) Message *M* 2) A word w of length *k.* The number of columns in the row transposition matrix will be k, and the columns in the matrix will be read in the alphabetical order of the letters in w. The program should then create the row transposition matrix and create the encrypted message C.
    - In coding the above, please note the following
        - Ignore spaces in the input text
        - You can write your code to be case insensitive – convert all input to lower case
        - In order to make decryption easy, pad any empty spaces in the last row of the row transposition matrix with the character X
        - Your final output should include M, w and C

Question 2:

What will be the decryption algorithm for a Row Transposition Cipher? Write down the pseudocode for the algorithm. [10 marks]

Question 3:

Using any programming language of your choice, implement the Row Transposition Cipher decryption algorithm [15 marks]

- **Specifications:**
    - The program should take two inputs 1) Encrypted Message ***C*** 2) The word **w** of length **k** that was used in encrypting the message. The program should then create the row transposition matrix and create the decrypted message **M**.
    - In coding the above, please note the following
        - You may or may not choose to remove any characters used for padding
        - Since spaces were removed from the plaintext before encryption they do not have to be reinserted after decryption
        - Your final output should include **C, w** and **M**

Question 4: (Encryption Test) [5 marks]

- Using a **w** value of ***NYITV***, use your code to encrypt the following text:
  "CRYPTOLOGY IS THE PRACTICE AND STUDY OF TECHNIQUES FOR SECURE COMMUNICATION IN THE PRESENCE OF THIRD PARTIES CALLED ADVERSARIES."
- Output your results

Question 5: (Decryption Test) [5 marks]

- Using a w value of *NYITV* use your code to decrypt the following text: “eroohalpsmeptroohalsefxphtnlefhhxtwstiiiieoecrastitosplmgeasentmitrasnefylypnhiasnetoiroitaetaxoeetonicrasetltesnicrfwmurnhrrhitrcrxhtpipsrmaimiitpiphlaleiucciptotpe”
- Output your results

Submission

- Submit the following documents separately in CANVAS by the deadline. **NO ZIPPED FILES ALLOWED**
    - All your code files
    - A detailed **README** file, which should explain how to run the code with sample input and output. If you are unfamiliar with READMEs you can find an introduction here https://www.makeareadme.com/ , here https://medium.com/@meakaakka/a-beginners-guide-to-writing-a-kickass-readme-7ac01da88ab3 and here https://www.youtube.com/watch?v=RZ5vduluea4. Note that the README file you submit for this project need not be complex, it only needs to at least explain how to compile the code and run the code with examples. **[5 marks]**
    - Your executable file and your **DOCKER** file. Please see the file **DOCKER INSTRUCTIONS** for information on how to create your Docker file.**[10 marks]**
    - A report (which should include your answer to the test results with screen shots)
- Note that your submission will be checked for plagiarism. All submissions with verified plagiarism cases will graded 0.