MIDTERM ESSAY

Applied Probability and Statistics for IT

Requirements

1/ Encryption using **Monoalphabetic Substitution Cipher**.

a/ Study and write a document about this algorithm.

b/ Write a demo program using Python.

2/ Decryption using **Frequency Analysis**.

a/ Study and write a document about this algorithm.

b/ Write a demo program using Python.

Regulations

Students need to submit a document file and a sourcecode file.

- The document file is in Word format (.doc/docx), named by your StudentID, eg. 52000000.docx, using our faculty's format, from 15 to 25 pages. English is required for high-quality 100% English classes only. The structure of this document should be:
  - Chapter 1: Introduction
    - Concepts about encryption and decryption; symmetric and asymmetric cryptosystem…
  - Chapter 2: Monoalphabetic Substitution Cipher
    - State the problem, constrains/conditions (if any), method/algorithm,
    - Examples,
    - Your comment, analysis, evaluation…
  - Chapter 3: Frequency Analysis
    - State the problem, constrains/conditions (if any), method/algorithm,
    - Examples,
    - Your comment, analysis, evaluation…
  - Chapter 4: Experiments
    - DO NOT just copy your code in this chapter.
    - Instruction for building and running your sourcecode. Screencaptures of your experimental results.
    - The language used in plaintext is English only.
    - Experiment with different lengths of text: 50 words, 100 words, 1000 words, 5000 words...
  - References
    - Using the faculty's format.
- The Python sourcecode file is named by your StudentID, eg. 52000000.py.
  - Encryption function.

- Decryption function.
- You can use libraries for supportive functions only.

Format violations will cost from 10% to 50% of your total scores.

You should solve and submit this report to your theory Google classroom within 14 days, from the beginning of April 4th 2022 to the end of April 17th 2022. Late submissions are not accepted. Submissions via email are not accepted.

This is an individual final report. Any case of plagiarism will get 0.

Rubric

Criteria	**Scale**	**1**	**2**	**3**	**Self-evalutaion**	**Reason**
	Score /10	**0 score**	**1/2 score**	**Full score**		
Chapter 1	0.5	Do nothing or wrongly.	Not enough details.	Detailed explanation.		
Chapter 2	2	Do nothing or wrongly.	Not enough details, no example, no comment.	Detailed explanation, good examples and comments.		
Chapter 3	2	Do nothing or wrongly.	Not enough details, no example, no comment.	Detailed explanation, good examples and comments.		
Question 4	1	Do nothing or wrongly.	Not enough details.	Detailed explanation.		
References	0.5	No reference.	Wrong format.	Right format.		
Encryption function	2	Error.	Correct but bad performance.	Correct and good performance.		
Decryption function	2	Error.	Correct but bad performance.	Correct and good performance.		
Total	10			Result	0	