Introduction to Data and Cyber-Security (DCS3101) - Assignment 1

Kiran Raja (kiran.raja@usn.no)

September 15, 2019

Universitetet
i Sørøst-Norge

1 Organization and Information

1. This is the first assignment of the total 4 assignments for this course.

2. The assignment contributes to 10% of the final grade and is mandatory to pass this assignment to qualify for the final exam.

3. Group work is tolerated but submissions are individual.

4. Each submission will be graded independently.

5. Use figures when needed to answer the questions.

6. *Deadline for submission of assignment is 29 Sep, 2019.*

7. The extra credit point (Q4) can be used carried to assignments 2, 3, 4 in case you obtain lower points.

8. Assignments to be submitted via Canvas.

2 Assignment

Q1 Consider Alice wants to send the message "Introduction to Data and Cyber-Security (DCS3100)" to Bob. Illustrate the concepts of CIA within the communication between Alice and Bob.

[2 Point]

Q2 Consider the sentence: "The quick brown fox jumps over the lazy dog." Write a script/program to encrypt this using Vigenere Ciphering.

- Illustrate the concepts of Vigenere Ciphering. [2 Point]
- Single key: "Lemon" [2 Point]
- Two keys: key-1: "Green" and key-2: "Watermelon". [2 Point]

*Note: The answer will be tested by giving a random string to verify the correctness of the script/program.

Q3 Illustrate the concepts of "Confusion" and "Diffusion" in information security.   [2 Point]

Q4 Extra credit point - Create a program for ENIGMA-I Encryption and Decryption.   [3 Points]