# Project Guidelines

# Cryptography Course

## Guidelines for the Project

Note: One can follow these set of guidelines to complete the project.

**Guideline 0**: The project can consist 3-5 students. The full mark of the project is 20 Marks.

**Guideline 1**: Select a desired Cryptographic algorithm of your choice (not only which we studied, there are > 50 algorithms), as an underlying algorithm for your project. You can check the internet for the full list of Cryptographic algorithms.

**Guideline 2:** Properly write down (explain) the background (study) of the selected Cryptographic Algorithm of your choice.

**Guideline 3:** Provide an example where you Encrypt and Decrypt a message using the selected cryptographic algorithm.

**Guideline 4:** Write down the Advantages (pros) and the Disadvantages (cons) of the selected cryptographic algorithm.

**Guideline 5:** Carry out a thorough research on your selected cryptographic algorithm, discuss and analyze the security weaknesses and what are different kinds of modifications (mathematical and/or logical) one can carry out, to make the selected algorithm more secure.

**Guideline 6:** Draw a FLOWCHART which can help elaborate your selected Cryptographic Algorithm. This will be included in the report.

**Guideline 7:** Implement the selected cryptographic algorithm with any programming language. It should include a pair of programs to encrypt and decrypt text files using the selected cryptography algorithm by providing 5 examples (at minimum) [5 different PLAIN TEXTS to 5 different CIPHER TEXTS and vice versa].

**Guideline 8:** Written Report, you must turn in a short report that discusses your program, describes the design, and issues you encountered while working on it. Your report should cover the following:

- **Cover Page** (Module Name, Module Code, Title of the report, Student’s name, Semester, Submitted To, Submission Date, Word Count)
- **Table of Contents** (Structure of the report)
- **Table of Figures** (Lists the images within the report)
- **Abstract**
- **Introduction** (Introduction to the selected cryptographic algorithm, technical terminologies used, Aim and Objectives, report structure)
- **Background** (Main part of the report, must elaborate the contents here so as to create a solid foundation for the next sections of the report)
- **Development** (Must include and show the different steps involved in the development stage)
- **Testing** (Must demonstrate different test scenarios to validate the developed selected cryptographic algorithm)
- **Evaluation** (Advantages and disadvantages of the developed selected cryptographic algorithm, application areas can also be discussed)
- **Conclusion**
- **References**

## Guideline 9: Timeline

| | |
|---|---|
| ▪ Group Formulation and Algorithm Selection | 21/04/2024 |
| ▪ Presentation and Discussion | 13/05/2024 |

## Guideline 10: Conflict

- No group select the same algorithm, if two groups select the same algorithm, they will penalized for a 25% deduction of the project mark.