Defense Project:
Project Implementation Guidelines-IS493

2nd **Semester 2024-2025 | IS493 - Instructor: Dr. Abdulaziz Alajaji**

Organization

In this component of the course, students will be organized into groups, at least (2), or MAXIMUM 3 students per group, to deliver this implementation task. Each group will be given about ten minutes to present and discuss their work with the rest of the class. In addition, the group will submit a **project report** with a **demo** showing their project description, source code, and sample execution results.

Timeframe

- **The final deadline for submitting project reports and a demo video is** *March 13th 2025*. The presentations will be held on *May 5th 2025*.
- Each group is required to send their name, student IDs, and topic of choice as soon as possible, not exceeding Feb 12th. The order of presentations will be randomly determined.

Project implementation

Each participant in the group is required to implement one of the following:

1) RSA
2) Hill Cipher
3) Keyword columnar ciphers
4) Product ciphers like Feistel cipher or DES
5) Any cryptosystem of your choice, or other defensive coding measures such as OWASP safe coding practices (**subject to approval**).

The program must allow the user to enter some of the crypto parameters (e.g., in the case of RSA: p, q, e or d, etc., and perform input validation). It must also show **both encryption and decryption processes.** It should be programed **using Python** and **have a graphical interface (GUI)**. During the presentation, the group will demonstrate the program execution to class.

IMPORTANT: e.g. If you are a group of THREE: your application should implement THREE different elements from the list above.

Project report

- Length: 5-7 pages, including code (you will use a template for that).
- Evaluation will consider structure of the report, quality of code, and writing skills.

Project presentation

- Presentation must be self-contained as much as possible, i.e., includes contribution and challenges.
- Length: 7-8 minutes for presentation, plus 2-3 minutes Q&A session.

- Evaluation will consider structure of the presentation, quality of contents, and presentation skills.
- Be prepared for questions about the source code and the understanding of the cipher logic.
- You need to show results for both crypto directions: encryption and decryption processes.
- Evaluation mark is not necessary to be the same for all students in the same group.
- If for any reason any of your group members is not present, make sure you attend and perform the presentation.