CRYPTOGRAPHY
MASTER ON INFORMATICS SECURITY
2023-2024

PROJECT ASSIGNMENT
Option 1 – Proposal, Implementation, and Analysis of a New Cryptographic Algorithm

This is a practical assignment that can be done by groups of two students. The purpose is to propose, implement and analyse a new cryptographic algorithm. This should include:

- a detailed description/specification of the proposed encryption/decryption algorithm;
- a robustness analysis of the proposed encryption technique (strong and weak points), as well as a comparison with other cryptographic algorithms;
- an implementation of the proposed algorithm (this can be an Excel-based implementation or any sort of implementation in a programming language of your choice);
- Some examples of the use of the proposed algorithm, both for encrypt and decrypt operations.

The project encompasses two deliveries:

1. An **intermediate delivery**, which will be mainly focused on the specification/design of the proposed algorithm, although it may also comprise any initial robustness analysis and implementation. The students should hand in a single zip file with a report on the developed work, as well as any developed code. This phase will require an estimated effort of 20 hours and has a weight of 4/20 on the final course grade.
2. A **final delivery**, comprising a full specification/design, implementation, robustness analysis, and use examples. The students should hand in a single zip file with the final report on the developed work, as well as the developed code. This phase will require an estimated effort of 32 hours and has a weight of 6/20 on the final course grade.

Deadline: The intermediate delivery is scheduled for November 2nd, 2023, 23:59, using the Inforestudante platform. The final delivery is scheduled for December 31st, 2023, 23:59, using the Inforestudante platform. There is a delay credit of 20 days for the set of the two project assignment deliveries. The used delay in the first delivery will be deducted from the total 20-day credit, the remaining credit being available for the final delivery.

(see next page for Option 2)

CRYPTOGRAPHY
MASTER ON INFORMATICS SECURITY
2023-2024

PROJECT ASSIGNMENT
Option 2 – Blockchain Implementation

This is a practical assignment that can be done by groups of two students. The purpose is to explore existing Blockchain technologies/tools and their applications, using freely available tools that can be found on the Internet, to construct a simple, working blockchain. Alternatively, a new blockchain solution may be developed/implemented. The assignment should include:

- identification and description of the tool used or developed in the assignment;
- detailed description/specification of the selected use case;
- detailed description of the use case implementation;
- An analysis of the pros and cons of the used or developed blockchain tool.

The project encompasses two deliveries:

1. An **intermediate delivery**, which will be mainly focused on the specification/design of the used or developed blockchain tool and use case, although it may also comprise any initial analysis and implementation. The students should hand in a single zip file with a report on the developed work, as well as any developed code. This phase will require an estimated effort of 20 hours and has a weight of 4/20 on the final course grade.
2. A **final delivery**, comprising a full specification/design, implementation, analysis, and use examples. The students should hand in a single zip file with the final report on the developed work, as well as the developed code. This phase will require an estimated effort of 32 hours and has a weight of 6/20 on the final course grade.

Deadline: The intermediate delivery is scheduled for November 2nd, 2023, 23:59, using the Inforestudante platform. The final delivery is scheduled for December 31st, 2023, 23:59, using the Inforestudante platform. There is a delay credit of 20 days for the set of the two project assignment deliveries. The used delay in the first delivery will be deducted from the total 20-day credit, the remaining credit being available for the final delivery.