**Essay**

***Discrete Structures***

# Objective

The objective of this assignment is to understand and implement RSA cryptosystem using modular arithmetic.

The assignment will be assessed based on the completeness of the research, correctness of the Python code, accuracy of the calculated results, and quality of the report written.

Students will be expected to demonstrate their understanding of RSA cryptosystem, and its mathematic foundations; their ability to write efficient code; and their skill in analyzing and reporting on data.

# Tasks

## 1. Finding an Inverse Modulo *n*

* Conduct research on Finding an Inverse Modulo *n* using the extended Euclidean algorithm. Give your own examples.
* Implement a Python program to find an Inverse Modulo *n* using the extended Euclidean algorithm. Related libraries are NOT allowed.
* Test the implemented program using sample data and verify the results. Capture your screen results and explain them in your report document.

## 2. RSA cryptosystem

* Conduct research on RSA cryptosystem. Understand the mathematical concepts behind the RSA cryptosystem, including prime number generation, modular arithmetic, extended Euclidean algorithm, prime factorization, etc. Give your own examples.
* Implement a Python program to encrypt and decrypt a message with the RSA cryptosystem. Cryptography libraries are allowed.
* Test the implemented RSA cryptosystem using sample messages and verify the results. Capture your screen results and explain them in your report document.
* Analyze the efficiency and security of the implemented RSA cryptosystem.
* Discuss the potential security threats and limitations of the RSA cryptosystem.
* Conclude with recommendations for improving the RSA cryptosystem implementation.

# Submission

Students need to submit a compressed file named with your Student ID, 52100000.zip/rar, including this structure:

* The document file is in Word format (.doc/docx), named by your Student ID, eg. 52100000.docx, using our faculty’s format, from 15 to 25 pages. English is required for high-quality classes. The structure of this document should be:
  + Chapter 1: Finding an Inverse Modulo *n*
  + Chapter 2: RSA cryptosystem
  + References: Using the faculty’s format.
  + Self- evaluation based on the given rubric.
* The Python source code files are named by your Student ID and Task Number, eg. 52100000\_1.py.

# Regulations

You should solve and submit this report to your theory ELIT classroom within 15 days, from the beginning of March 30th 2023 to the end of April 13th 2023. Late submissions are not accepted. Submissions via email are not accepted.

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

Students need to solve all the problems and submit a zip/rar file named by their Student ID, using the given structure. English is required for high-quality classes. Format violations will cost from 10% to 50% of your total scores.

# Rubric

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | | **Scale** | **0 score** | **1/2 score** | **Full score** | **Self-evaluation** | **Reason** |  |
| Task 1 | Theorical research | 1 | Do nothing or wrongly | Not enough  details, no  example, no  comment | Correct calculations, detailed explanations |  |  |  |
| Implementation | 2 | Error | Correct but  bad  performance | Correct and  good  performance |  |  |  |
| Test | 1 | No test | Test without verification | Test and verification |  |  |  |
|  |
| Task 2 | Theorical research | 2 | Do nothing or wrongly | Not enough  details, no  example, no  comment | Correct calculations, detailed explanations |  |  |  |
| Implementation | 1 | Error | Correct but  bad  performance | Correct and  good  performance |  |  |  |
| Test | 1 | No test | Test without verification | Test and verification |  |  |  |
|  |
| Analysis | 0.5 | Do nothing or wrongly | Not enough  details, no  example, no  comment | Correct, detailed explanations |  |  |  |
| Discussion | 0.5 | Do nothing or wrongly | Not enough  details, no  example, no  comment | Correct, detailed explanations |  |  |  |
| Recommendation | 0.5 | Do nothing or wrongly | Not enough  details, no  example, no  comment | Correct, detailed explanations |  |  |  |
| Reference | | 0.5 | No  reference | Wrong  format | Right format |  |  |  |
| **Total** | | 10 | Result | | | 0 |  |  |