**Essay**

***Discrete Structures***

# Objective/ Khách quan

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.

Mục tiêu của nhiệm vụ này là hiểu và triển khai hệ thống mật mã RSA bằng cách sử dụng số học mô-đun.

Bài tập sẽ được đánh giá dựa trên tính đầy đủ của nghiên cứu, tính chính xác của mã Python, độ chính xác của kết quả tính toán và chất lượng của báo cáo được viết.

Học sinh sẽ được yêu cầu thể hiện sự hiểu biết của mình về hệ thống mật mã RSA và nền tảng toán học của nó; khả năng viết mã hiệu quả của họ; và kỹ năng của họ trong việc phân tích và báo cáo về dữ liệu.

# Tasks

## 1. Finding an Inverse Modulo *n/*1. Tìm một Modulo nghịch đảo 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.
* Tiến hành nghiên cứu Tìm một Modulo n nghịch đảo bằng thuật toán Euclide mở rộng. Đưa ra ví dụ của riêng bạn.Thực hiện một chương trình Python để tìm Modulo n nghịch đảo bằng cách sử dụng thuật toán Euclide mở rộng. Thư viện liên quan KHÔNG được phép.
* Kiểm tra chương trình đã triển khai bằng cách sử dụng dữ liệu mẫu và xác minh kết quả. Chụp kết quả màn hình của bạn và giải thích chúng trong tài liệu báo cáo của bạn.

## 2. RSA cryptosystem/ Hệ thống mật mã RSA

* 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.
* Tiến hành nghiên cứu về hệ thống mật mã RSA. Hiểu các khái niệm toán học đằng sau hệ thống mật mã RSA, bao gồm tạo số nguyên tố, số học mô-đun, thuật toán Euclide mở rộng, phân tích thừa số nguyên tố, v.v. Hãy đưa ra các ví dụ của riêng bạn.
* Triển khai chương trình Python để mã hóa và giải mã tin nhắn bằng hệ thống mật mã RSA. Thư viện mật mã được cho phép.
* Kiểm tra hệ thống mật mã RSA đã triển khai bằng các thông báo mẫu và xác minh kết quả. Chụp kết quả màn hình của bạn và giải thích chúng trong tài liệu báo cáo của bạn.
* Phân tích hiệu quả và tính bảo mật của hệ thống mật mã RSA đã triển khai.
* Thảo luận về các mối đe dọa bảo mật tiềm ẩn và những hạn chế của hệ thống mật mã RSA.
* Kết luận với các khuyến nghị để cải thiện việc triển khai hệ thống mật mã RSA

# 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 |  |  |