Text Encryption and Decryption using Cryptography Algorithms

April 22, 2025

1 Background

Cryptography is a critical field in both theoretical and applied mathematics, particularly in the realm of secure communications. The RSA [RSA78] and ElGamal [Gam84] encryption algorithms are two prominent public-key cryptosystems that have been widely adopted for their robust security properties. RSA, named after its inventors Rivest, Shamir, and Adleman, leverages the difficulty of factoring large numbers to provide secure encryption and decryption. ElGamal, on the other hand, is based on the discrete logarithm problem and offers a different approach to achieving secure communication. Both algorithms are essential for understanding modern cryptographic practices and are widely used in various applications, from secure web transactions to encrypted messaging.

2 Objective

The objective of this project is to provide a comprehensive understanding of the RSA and ElGamal encryption algorithms through practical implementation and analysis. You will implement both algorithms in Python, focusing on key generation, encryption, and decryption processes. You will also analyze the security and performance characteristics of each algorithm, comparing their strengths and weaknesses. By the end of the project, students should be able to apply these algorithms to encrypt and decrypt messages and understand their theoretical foundations as well as practical applications in securing digital communications.

3 Task Description

Each group will implement a modular encryption/decryption system for textual messages:

- Implement the **RSA** algorithm with the key generation, encryption, and decryption functions.
- Implement the **ElGamal** algorithm with the key generation, encryption, and decryption functions.
- Test the implementation with the encryption/decryption of short and long **"textual"** messages.
- Analyze the performance and security level of **RSA** and **ElGamal**.

Students are encouraged to experiment with different parameters (e.g., sizes of prime numbers, public exponent, etc) and analyze their impact on performance. Beyond the required cryptography methods, students are also welcome to explore more recent or advanced cryptography techniques or propose and prototype novel approaches. Innovation and thoughtful system design will be taken into account in the grading rubric, particularly under the criterion of "Application and Innovation."

4 Tools

You may use any standard Python packages (but not existing RSA or ElGamal libraries) for implementation.

使用密码学算法进行文本加密和解密

2025 年 4 月 22 日

1 背景

密码学是理论数学和应用数学中的一个关键领域，尤其是在安全通信领域。RSA 和 ElGamal 加密算法是两种著名的公钥密码系统，因其强大的安全性而被广泛采用。RSA 算法以它的发明者 Rivest 、Shamir 和 Adleman 的名字命名，利用大数分解的困难性来提供安全的加密和解密。另一方面，ElGamal 算法基于离散对数问题，提供了一种不同的安全通信实现方法。这两种算法对于理解现代密码学实践至关重要，并且在各种应用中得到了广泛的使用，从安全的网络交易到加密消息。

2 目标

本项目的目标是通过对 RSA 和 ElGamal 加密算法的实践实现和分析，提供一个全面的了解。你将使用 Python 实现这两个算法，重点关注密钥生成、加密和解密过程。你还将分析每个算法的安全性和性能特征，比较它们的优缺点。到项目结束时，学生应该能够应用这些算法来加密和解密消息，并理解它们的理论基础以及在实际数字通信安全中的应用。

3 任务描述

Each group wil我实现了一个模块化的加密 / 解密系统 or textual messages:

- 实现 RSA 算法，包括密钥生成、加密和解密功能。
- 实现 **ElGamal** 算法，包括密钥生成、加密和解密函数。
- 使用短和长 " **文本** " 消息的加密 / 解密来测试实现 .

分析 **RSA** 和 **ElGamal** 的性能和安全级别。

学生被鼓励尝试不同的参数（例如，素数的尺寸、公钥指数等）并分析它们对性能的影响。除了必需的加密方法之外，学生还可以探索更近期的或高级的加密技术，或者提出并原型化新的方法。创新和深思熟虑的系统设计将在评分标准中考虑，尤其是在 " 应用与创新 " 这一标准下。

4 个工具

您可以使用任何标准的 Python 包（但不是现有的 RSA 或 ElGamal 库）进行实现。

5 Team Organization

- Each team should consist of **4 students**.
- Team members are encouraged to divide responsibilities (e.g., basic functions, evaluation, and drafting report) and all members should participate in the algorithm implementation.
- Teams are free to organize themselves, but must submit one final project as a group.

6 Deliverables

Each group is required to submit the following components:

- **Code**: A well-organized Python project with modular structure, inline documentation, and clear instructions for installation and execution (e.g., via `README.md` or Jupyter notebooks).
- **Report**: A concise report (3–5 pages) summarizing the project. The report should include the following sections:
  - **Motivation**: Why shortest path finding matters and what this project aims to solve.
  - **Related Work**: Brief summary of the used technology.
  - **System Design**: Description of the architecture, modules, and key design choices.
  - **Method Comparison**: Analysis of the two approaches in terms of performance and their security levels.
  - **Experimental Setup and Results**: Analyzed results, and visualizations.
  - **Conclusion and Future Work**: Summary and potential directions for improvement.
- **Presentation**: Each group will attend a short (8-minute) presentation session with TAs and lecturers to demonstrate their system, findings, and answer questions. Presentation quality will also be considered in grading.

References

[Gam84] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1984.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

5 团队组织

每个团队应包括 **4 名学生**。

鼓励团队成员分担责任（例如，基本功能、评估和起草报告）并且所有成员都应参与算法实现。

团队可以自由组织，但必须以团队形式提交一个最终项目。

6 可交付成果

每个小组必须提交以下组件：

- **代码**：一个结构良好、模块化、具有内联文档和清晰的安装和执行说明（例如通过 README.md 或 Jupyter 笔记本）的 Python 项目。
- **报告**：一份简洁的报告（ 3-5 页），总结项目。报告应包括以下部分：
  - **动机**：为什么最短路径查找很重要以及本项目旨在解决的问题。– **相关工作**：对所使用技术的简要总结。– **系统设计**：对架构、模块和关键设计选择的描述。– **方法比较**：从性能和安全性水平分析两种方法。– **实验设置和结果**：分析结果和可视化。– **结论和未来工作**：总结和潜在改进方向。
- **演示**：每个小组将参加一个简短的（ 8 分钟）演示环节，与助教和讲师一起展示他们的系统、发现并回答问题。演示质量也将作为评分标准之一。

参考文献

[塔赫尔 · 埃尔 · 加马尔。基于离散对数的一个公钥密码系统和签名方案。在 G. R. 布莱克利和戴维 · 乔姆编辑的《密码学进展，CRYPTO '84 会议论文集》，美国加利福尼亚州圣巴巴拉，1984 年 8 月 19-22 日，Lecture Notes in Computer Science 系列，第 196 卷，第 10-18 页。Springer，1984。

[RSA78] 罗纳德 ·L· 里弗斯特、阿迪 · 沙米尔和伦纳德 ·M· 阿德尔曼。一种获取数字签名和公钥密码系统的方法。通讯协会计算机杂志，第 21 卷第 2 期：120–126，1978 年。