



信息加密系统测试报告

学 院： 数学与计算机学院

姓 名： 谢焕豪 许洛熙 彭锦锋

关超华 邓佳诚 李佳伦

展浩铭

科任老师： 蔡浩

课 程： 软件工程

报告时间： 2025年1月1日

信息加密系统测试报告

1. 测试目的

本次测试旨在验证信息加密系统的功能性、安全性、性能和用户体验，确保其在本地环境下能够正确、稳定地运行，满足加密和解密的需求，并在高负载下保持良好的性能和低资源消耗。

1. 测试环境

* 硬件环境:

处理器: Intel Core i7-10750H

内存: 32GB DDR4

存储: 1TB SSD

操作系统: Windows 11 x64

* 软件环境:

编程语言: GDScript

测试工具: Python自定义脚本、系统监控工具Task Manager

* 信息加密算法:

Caesar密码

Transposition密码

Vigenere密码

RSA加密

* 系统特点:

本地运行，无需网络连接，所有加密和解密操作均在本地机器上进行。

1. 测试内容
   1. 功能性测试

* ****加密与解密测试:****

输入数据：文本

对比原始数据与解密后的数据是否一致。

确保不同的数据输入能够正确加密并且可以准确解密。

* ****算法支持:****

测试四种加密算法（Caesar密码、Transposition密码、Vigenere密码、RSA加密）是否能正常工作，确保在使用不同的加密算法时，数据能够按预期进行处理。

* ****加密性能:****

测试每种加密方法的处理速度，尤其是对大数据量的加解密速度，确保系统能够处理常见的使用场景。

* 1. 安全性测试
* ****攻击模拟:****

对Caesar密码、Transposition密码和Vigenere密码进行暴力破解测试，评估其安全性。特别是对于Caesar密码和Transposition密码，其密钥空间相对较小，需要重点测试破解的难度。

* ****密钥强度测试:****

对每种加密方法使用不同密钥长度进行测试，验证系统是否能有效抵抗密码破解攻击。重点测试RSA加密的强度，确保其能提供足够的安全性。

* 异常输入处理****:****

测试系统如何处理无效数据、格式错误或恶意输入，确保系统能够抵御简单的输入攻击，避免信息泄露或程序崩溃。

* 1. 性能测试
* **加密/解密性能:**

测试不同数据量（如1MB, 10MB, 100MB）的加解密时间，评估其在生产环境中的表现。

* **系统资源消耗:**

使用系统监控工具（如Task Manager）监控加解密过程中的CPU、内存和磁盘使用情况，评估系统在高负载下的资源消耗。

* **负载均衡测试:**

模拟多个并发用户进行加解密操作，测量在高负载情况下的性能表现。

* 1. 用户体验测试
* **操作简便性:**

测试用户界面的友好程度和加密解密操作的简便性。

检查文档和帮助系统，确保用户能够理解并顺利完成加密过程。

* **错误信息反馈:**

确保系统在用户操作错误时能够提供明确且有用的错误提示。

1. 测试结果
   1. 功能性测试

* **加密与解密验证**:

所有加密算法（Caesar、Transposition、Vigenere和RSA）能够成功加密并解密数据。对比原始数据与解密数据，完全一致，说明加解密过程正确无误。

对于文本的加密测试，所有算法均表现良好。

* **算法支持**:

Caesar密码：可以成功加密和解密，适用于简单的文本加密。

Transposition密码：通过字符位置交换加密，解密效果良好，适用于小文件和中等复杂度的加密。

Vigenere密码：适用于较长的文本数据，通过关键字加密，提供较强的安全性，解密结果准确。

RSA加密：适用于加密密钥和小数据文件，虽然加密解密速度相对较慢，但能够成功实现加解密操作。

* **密钥管理**:

密钥生成、存储和替换的测试结果符合预期。RSA密钥能够正确生成和保护，其他对称密钥（Caesar、Transposition、Vigenere）也能按照规定存储并使用。

* **加密性能**:

Caesar密码和Transposition密码的加解密速度较快，适合短小文本的加密。

Vigenere密码在处理中等大小文本时性能良好。

RSA加密虽然能成功处理小文件，但加解密速度较慢，特别是处理大文件时，性能瓶颈较为明显。

* 1. 安全性测试
* **暴力破解测试**:

Caesar密码：密钥空间仅有26个，暴力破解非常容易，因此安全性较低。

Transposition密码：密钥空间较大，但仍然能够通过暴力破解进行破解。

Vigenere密码：对于短密钥，暴力破解较为容易，但长密钥则大幅提高破解难度，安全性较高。

RSA加密：RSA的密钥强度足够，暴力破解几乎不可能，符合当前安全标准。

* **密钥强度**:

Caesar密码：密钥强度极低，不适合用于实际应用。

Transposition密码：密钥强度相对较低，需要进一步提升复杂度。

Vigenere密码：密钥长度越长，破解难度越大，适合中等安全需求。

RSA加密：RSA的密钥足够强大，可以抵御当前的密码学攻击。

* **异常输入处理**:

系统能够处理所有输入异常，如格式错误、输入过长等，并提供清晰的错误信息，防止潜在的攻击。

* 1. 性能测试
* **加密/解密速度**:

Caesar密码和Transposition密码的加解密速度非常快，适合处理小型数据。

Vigenere密码的加解密速度适中，适合处理中型文本。

RSA加密对于大数据的加密解密较为缓慢，特别是对100MB以上的数据进行加密时，解密速度较慢。

* **系统资源消耗**:

Caesar密码和Transposition密码的资源消耗较低，几乎不会影响系统性能。

Vigenere密码和RSA加密在大文件加解密时消耗较高的CPU资源，特别是在RSA加密时，系统CPU使用率较高。

* **并发性能**:

系统在高并发的加解密请求下能够保持稳定运行，但随着RSA加密并发数增加，性能有所下降。

* 1. 用户体验测试
* **操作简便性**:

系统界面友好，用户可以轻松进行加解密操作，尤其是对于Caesar和Vigenere密码，界面简洁明了。

RSA加密部分稍显复杂，适合有强烈保密需求的用户。

* **错误信息反馈**:

当上传同名文本时，最新的文本会掩盖老的文本，但是用户界面依旧会显示老文本。当删除任意同名文本时，其他文本的内容会同步消失，仅显示“信息”二字。

电脑萤幕的截图

描述已自动生成

1. 打开Caesar演示，内容正常

电脑萤幕的截图

描述已自动生成

1. 打开同名文件，应该显示“这是一个测试内容1”

电脑萤幕的截图

描述已自动生成

1. 删除任意同名文件
2. 结论

本次测试表明，信息加密系统能够有效地支持四种加密算法（Caesar、Transposition、Vigenere和RSA）。系统在加解密准确性、安全性、性能和用户体验等方面表现良好。对于短文本和中等数据量的加解密，Caesar、Transposition和Vigenere密码提供了足够的安全性和较好的性能。对于需要高安全性的应用。