信息安全课程设计报告

题 目： 密钥管理系统

专 业： 22智能科学与技术2

姓 名： 姚仁杰

学 号： 2022337621031

指导教师： 肖荣

2025年6月19日

**正文：**

1. **前言**

一个完善的密钥管理系统不仅仅是“生成”与“存储”密钥，更是在整个密钥生命周期中提供安全控制、合规审计、可扩展集成与高可用运维的能力。它是构建任何加密服务与保障数据安全的基石，对提升系统整体的安全性、可维护性与可信度都具有深远意义。

1. **系统分析**

分别选择了非对称加密算法 RSA 和对称加密算法 AES 进行密钥管理。

可以选择自定义设置密钥，也可以选择系统生成。

设计检测算法，对 RSA 密钥强度和 AES 密钥强度进行检验。

系统内部对密钥使用 RSA 进行数字签名，使用 SHA256 进行加密储存。

密钥以 .json 文件格式储存。

1. **功能设计**
2. **系统特色及关键技术**
3. **测试**
4. **结论**

**参考文献：**

[1] Rivest, R. L., Shamir, A., & Adleman, L.“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, *Communications of the ACM*, 1978, 21(2): 120–126.

[2] Daemen, J. & Rijmen, V. The Design of Rijndael: AES – The Advanced Encryption Standard Springer, 2002.

[3] 游新娥. RSA 算法中安全大素数生成方法及其改进. 《吉首大学学报(自然科学版)》, 2007, 28(5): 34–37.

**附录：**