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。

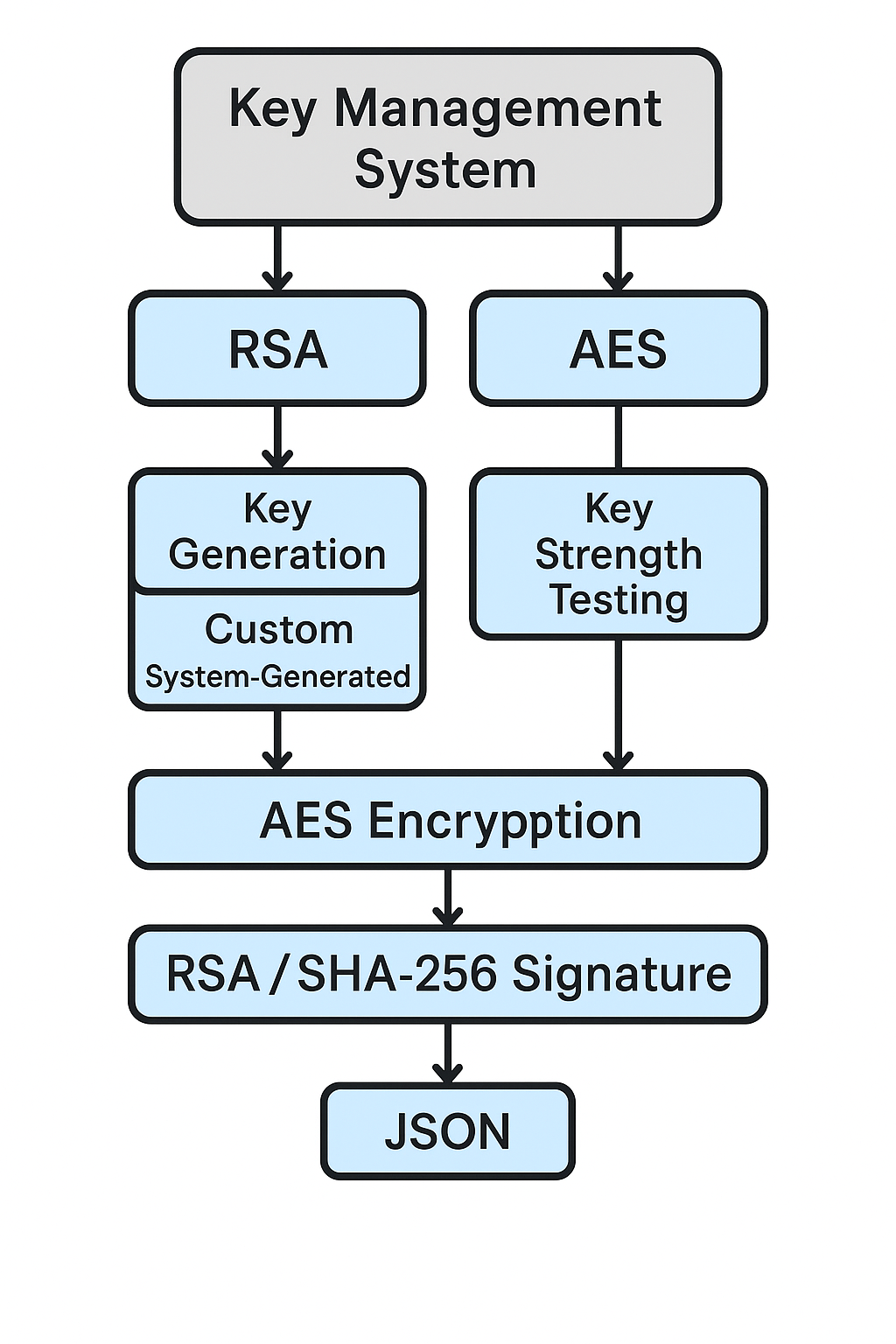
可以选择自定义设置密钥，也可以选择系统生成。

设计检测算法，对 RSA 密钥强度和 AES 密钥强度进行检验。

使用 AES 对密钥内容进行加密，对密钥使用 RSA 和 SHA256 进行数字签名。

最后以 json 文件格式储存。

1. **功能设计**

****

1. **系统特色及关键技术**

RSA（Rivest–Shamir–Adleman）是一种非对称加密。

公钥/私钥对：公钥用于加密。私钥用于解密，私钥还可用于数字签名，公钥用于验证签名。

RSA 基于两个大素数和 的乘积 ，安全性取决于因式分解的困难性。

加密： n，解密：。

安全性取决于密钥长度，常见长度为 2048 或 4096 位。主要用于小数据量加密（如密钥交换、签名验证），非对称加密速度慢。

AES（Advanced Encryption Standard）是一种对称加密。

使用同一密钥用于加密和解密，发送方和接收方需共享一个密钥。

加密 AES 将数据分成 128 位（16 字节）块进行处理。

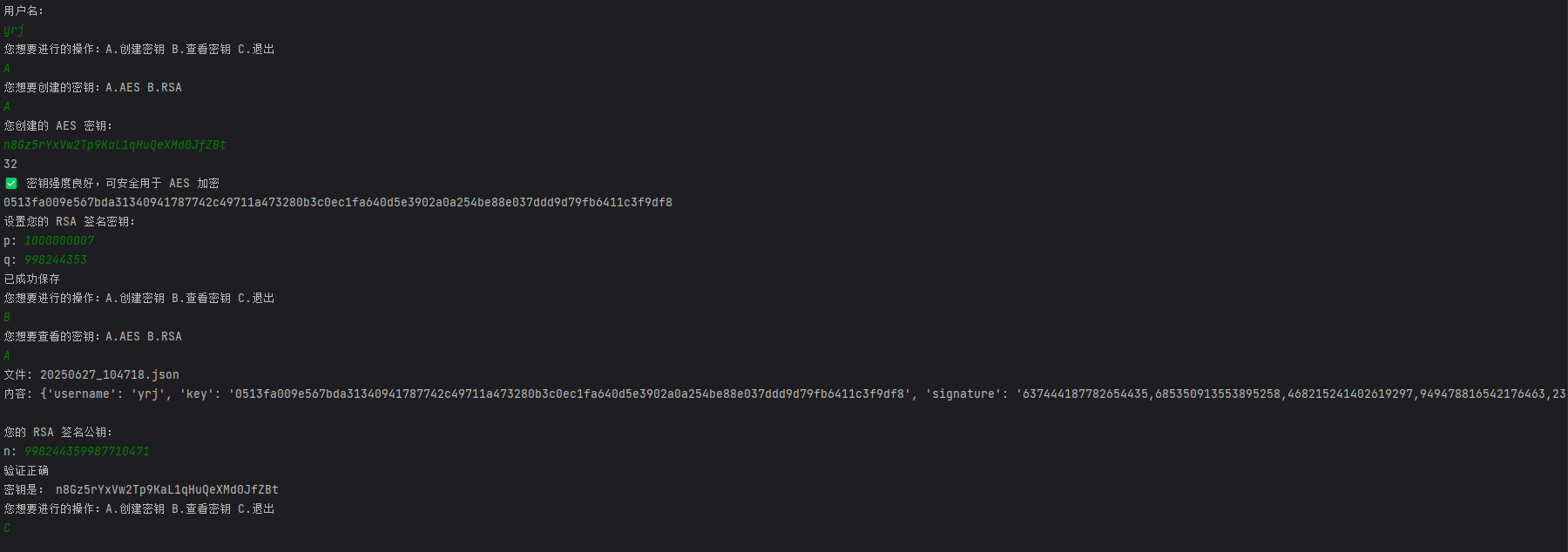
密钥长度支持 128、192 和 256 位密钥长度，密钥越长越安全。

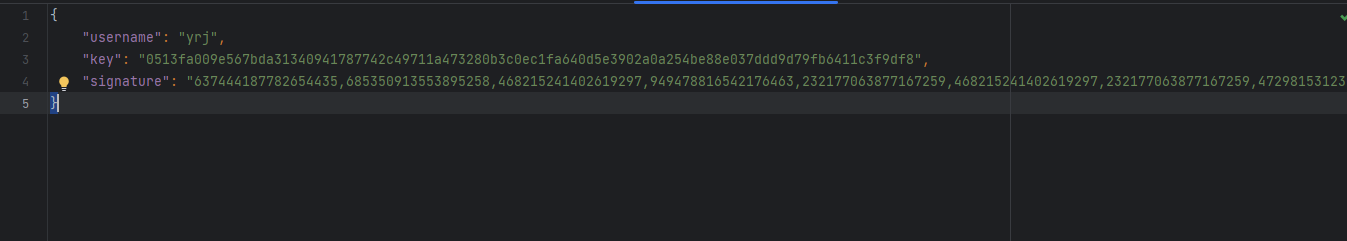
加密：每轮包括：字节替代（SubBytes）、行移位（ShiftRows）、列混合（MixColumns）、轮密钥加（AddRoundKey）。

高效快速，适合加密大量数据，广泛用于文件、数据库、网络通信。

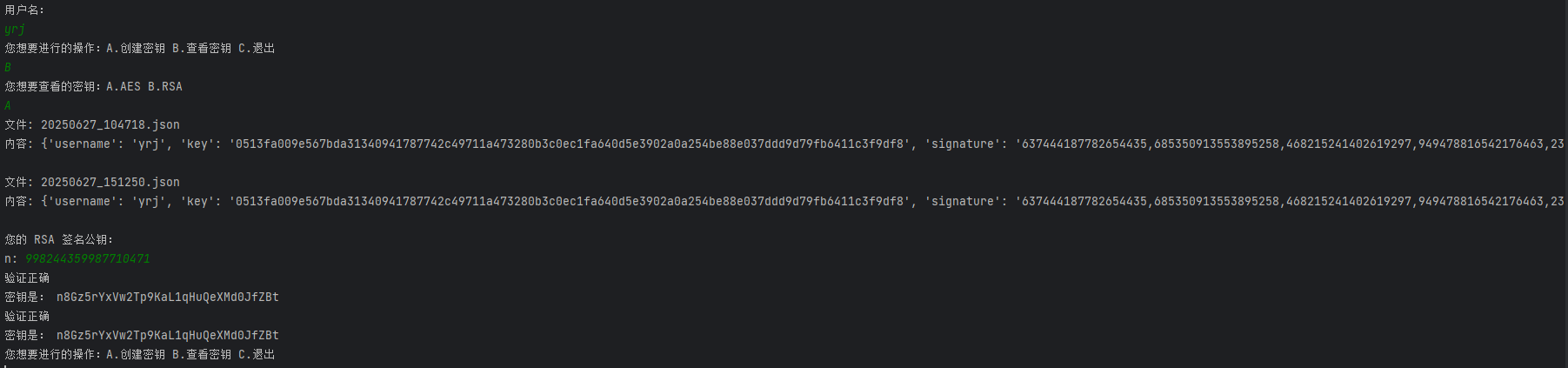
加密模式如 CBC、CFB、GCM 等，用于提高安全性和灵活性。

1. **测试**

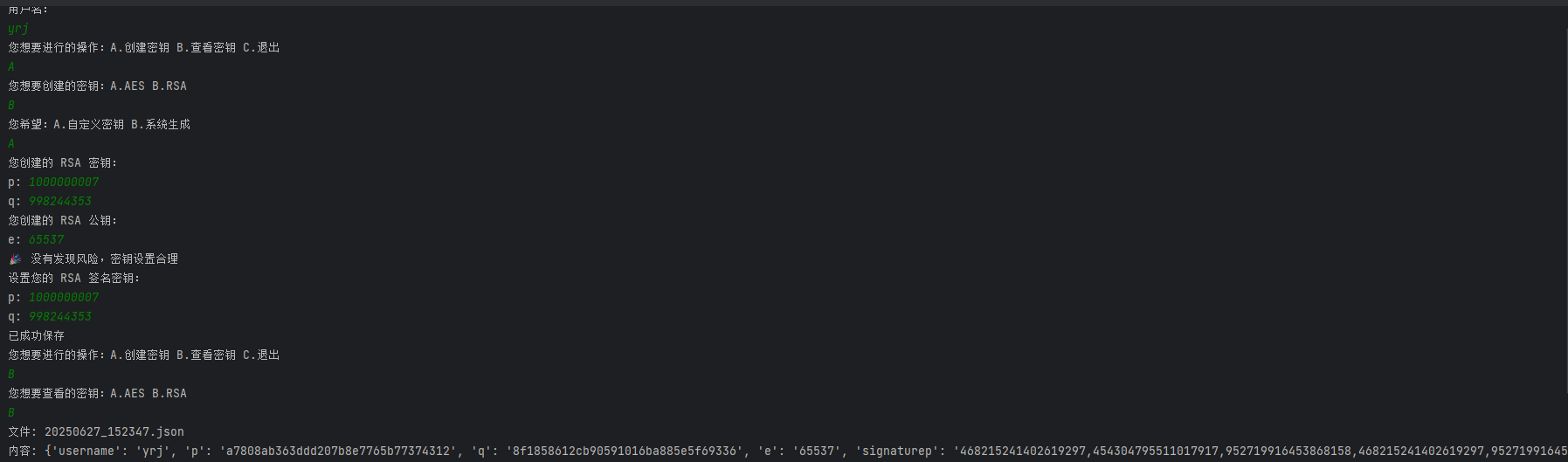
用户创建 AES 密钥：  


AES保存形式：  


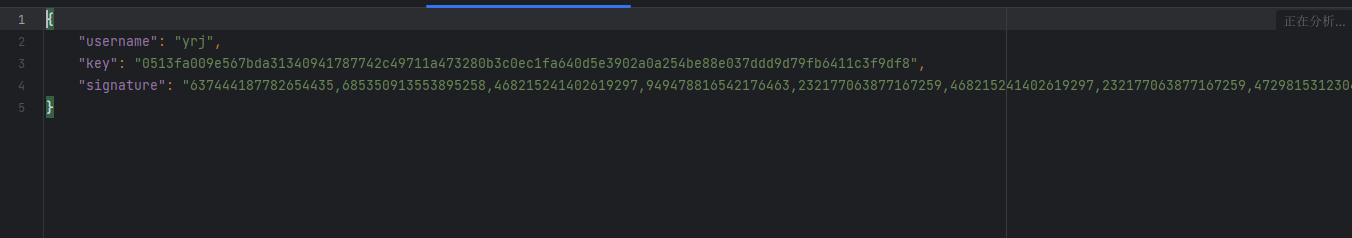
用户查看 AES 密钥：



用户创建 RSA 密钥



RSA密钥保存形式：



用户查看 RSA密钥：



1. **结论**

**心得：**

这是一次非常完整的密码学应用实践，在理论与实现之间建立了良好的桥梁。

提高了我对混合加密、数字签名、数据完整性验证等核心技术的理解。

这次实验不仅加深了我对加密算法和密钥管理体系的理解，也为将来开发更复杂的安全系统打下了坚实的基础。

**待改进：**

密钥保护：当前脚本中，AES 密钥和 RSA 私钥输入后直接存储到磁盘并可被任何人读取，建议用操作系统的密钥保险库（如 Windows DPAPI、Linux 的 libsecret）或硬件安全模块（HSM）。

异常与输入校验：大量 int(input())、文件 I/O 操作未做异常处理，生产环境易崩溃。

并发与锁：多用户或并发访问时对文件读写没有锁定，可能出错。

加密模式与填充：AES 编解码只做了“可逆编码”，并未指定加密模式（CBC、GCM 等）和随机 IV，安全性不完整。

用 RSA 的私钥指数直接“签名”，与标准的 PSS 签名／PKCS#1 v1.5 签名可能不兼容，建议使用成熟库（如 PyCryptodome）并选用安全的签名填充。

**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：**