密码学综合设计实验

实验1：多表代换密码

学号：031803134

姓名：郑晟

19年 09月 15日

1. 实验要求
2. 根据扩展欧几里得算法实现求乘法逆元模块
3. 设定分组长度为4, 输入加密密钥(A,B)和解密密钥A-1。
4. 验证密钥的正确性(即A A-1=E)
5. 实现多表代换加密解密，能够对输入的英文字符串进行加密解密。
6. 实验原理
7. 随机生成4x4的可逆矩阵A，确保A的行列式与模26互素，将该矩阵A作为密钥A。
8. 随机生成1x4的矩阵B，将该矩阵B作为密钥B。
9. 对明文按4位一组进行分组，对长度不为4的倍数的明文进行补位操作。
10. 通过Ci≡AMi+B(mod 26)进行加密变换得到密文。
11. 将密钥A作为矩阵A，求出矩阵A的逆矩阵。
12. 对密文按4位一组进行分组，对长度不为4的倍数的明文进行补位操作。
13. 通过Mi≡(Ci-B)(mod 26)进行解密变换得到明文。

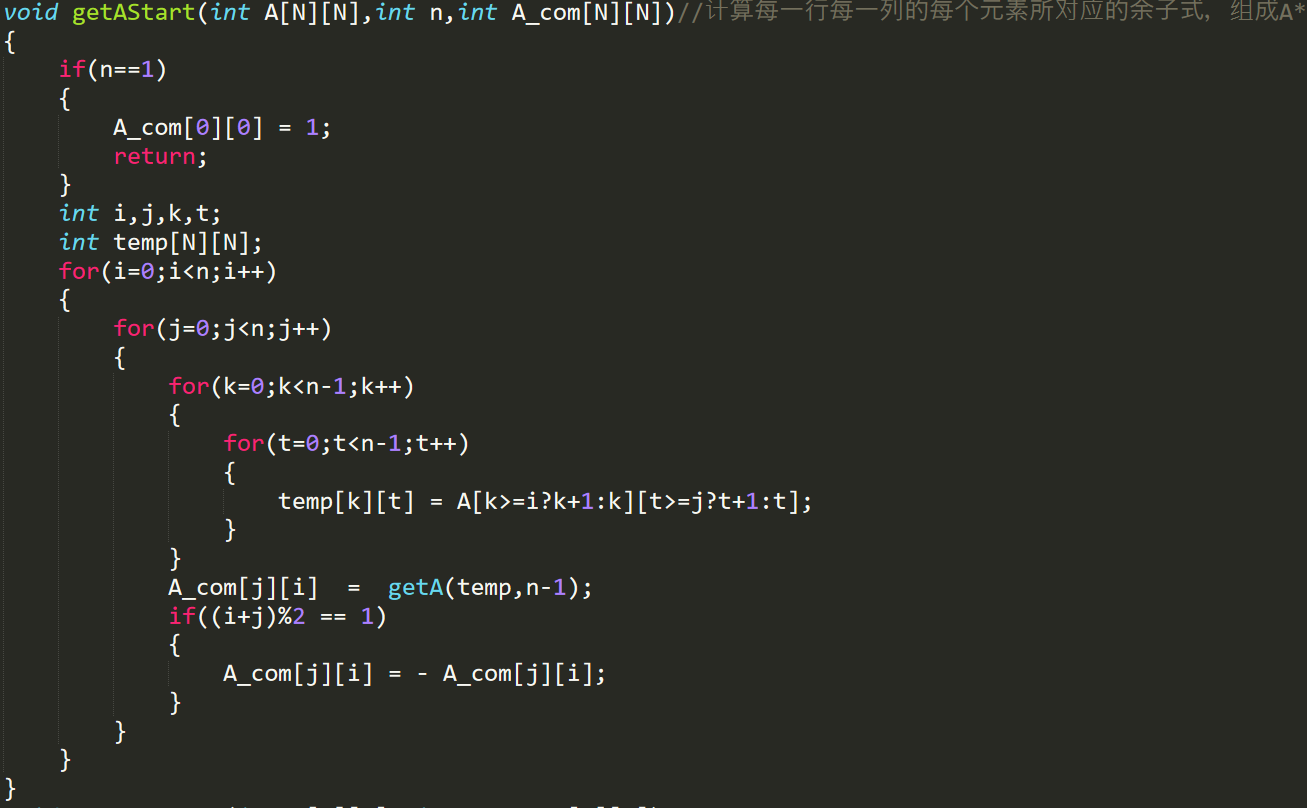


1. 软件系统设计

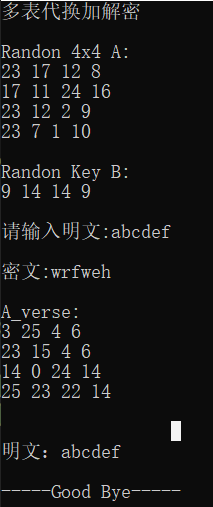
系统拥有两大功能模块，分别为加密模块和解密模块，包含一下函数：gcd函数，行列式计算函数，生成A矩阵函数，求逆函数，求伴随矩阵函数，求逆矩阵函数，生成B密钥函数。

1. 重要的实现细节

求伴随矩阵的函数中使用了三目运算符，提高算法简洁程度，使其逻辑清晰易懂。



1. 实现效果



1. 总结

多表代换密码

本系统实现4x4多表代换加解密，拥有分工明确的各个函数，程序简洁明了，不足的是未能成功实现对长度不是4的倍数的明文的处理。