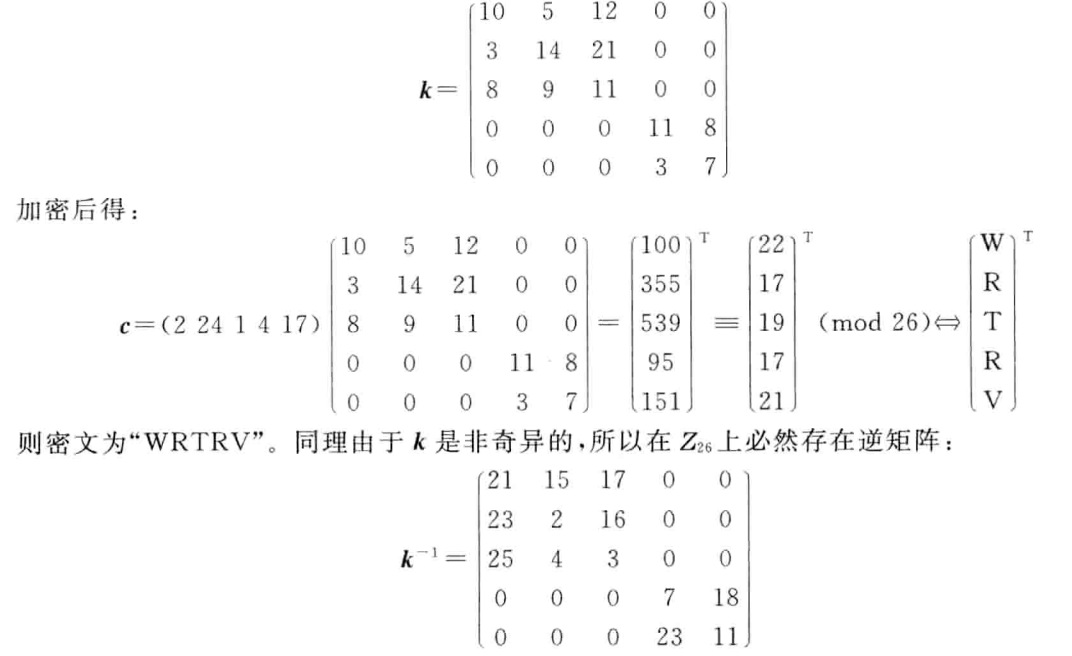
2021.03.11密码学第一次上机题目

题目：对于明文“In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes Currently the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control However if any server storing the data is compromised then the confidentiality of the data will be compromised In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption By using our techniques encrypted data can be kept confidential even if the storage server is untrusted moreover our methods are secure against collusion attacks”（忽略大小写及空格）。

完成（若分组长度不足请自行补足）：

a：选择分组n=7的周期置换（自定义置换），进行加解密；  
b：以P53页的K作为私钥，进行Hill算法加解密，并对明密文字符的频率分别做统计分析。

  
c：自己选择K1和K2，做仿射密码的加解密，并对明密文字符的频率分别做统计分析。

要求：1、可分组完成，每组成员不超过3人；

2、使用语言不限，不要调用现成的函数实现。

3、统计分析给出明文密文中的字符出现频率即可，无须完成唯密文攻击等。