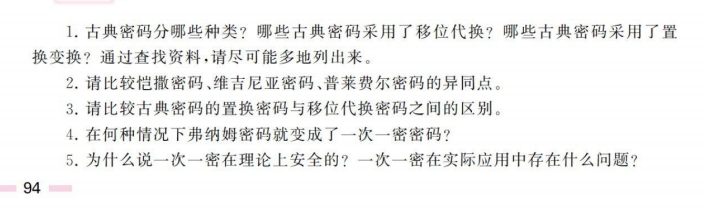
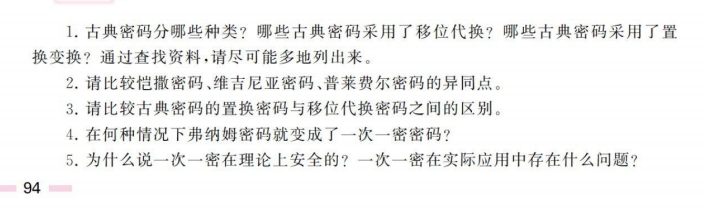
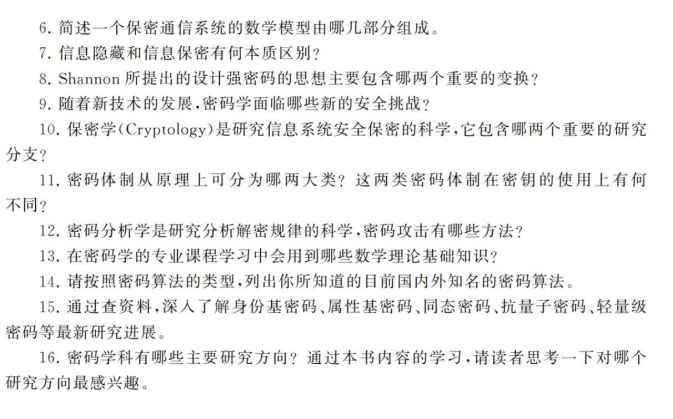
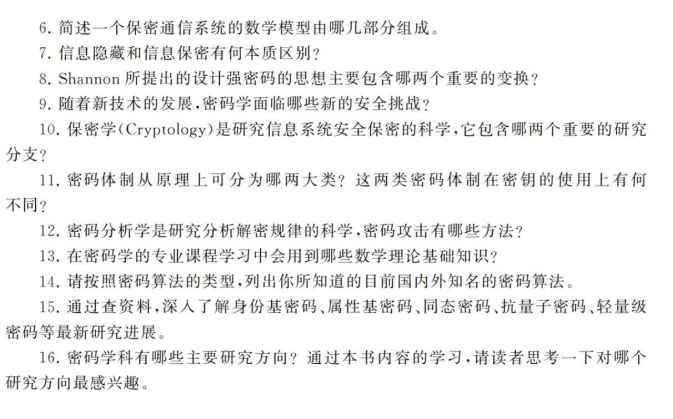
第二章







1. 凯撒密码，维吉尼亚密码和普莱费尔密码的异同点：

都是古典密码中的采用位移代换的密码类型，不改变明文顺序，改变明文字母；

不同点在于代换方式不同，凯撒密码采用单表代换；维吉尼亚密码采用多表代换；普莱费尔采用的是多字母代换。

1. 古典密码的置换密码和移位代换密码之间的区别：

置换密码不改变明文字母，改变明文顺序

5、若密钥都是真随机数，那么产生的密文流也是真随机数。

问题：

1.产生大规模的随机密钥有困难

2.密钥的分配和保护存在困难

8.shannon所提出的设计强密码的思想包含

扩散和混淆。

11、密码体制从原理上分为单钥密码体制和双钥密码体制

--单钥密码体制（加密密钥和解密密钥相同）、双钥密码体制（加密和解密分开）

12、密码攻击方法：穷举攻击法、数学攻击法、物理攻击。.