1. 保密通信的一般模型是什么，包括哪些组成?

2. 简述柯克霍夫准则。

3. 简述理论安全、计算安全和实际安全的内涵。

4. 有哪些密码攻击类型（或威胁模型)?

5. 简述凯撒密码、单表代换密码、维吉尼亚密码的加解密过程及存在的安全问题。

6. 简述一次一密的加解密过程，为什么一次一密是理论安全的，实际应用一次一密时存在什么问题。

7. 使用维吉尼亚密码加密消息 “explanation”，使用密钥 “leg”。

8. 仿射凯撒密码（简称为仿射密码）是凯撒密码的一种推广，定义如下：对每个明文字母 $p \in \{0, \ldots, 25\}$，用密文字母 $c \in \{0, \ldots, 25\}$ 代替，其中

$$c = E([a, b], p) \triangleq (ap + b) \bmod 26$$

对加密算法的基本要求是算法是单射的，即如果 $p \neq q$，则 $E(k, p) \neq E(k, q)$；否则就会因为很多明文映射到相同的密文而无法解密。仿射密码并不是对所有的 a 都是单射的，例如，当 $a = 2, b = 3$ 时，有 $E([a, b], 0) = E([a, b], 13) = 3$。

(a) 讨论仿射凯撒密码中参数 a, b 的取值范围。

(b) 有多少种仿射凯撒密码?

(c) 用仿射凯撒密码加密得到一份密文，统计密文中每个字母的频率得知频率最高的字母为 B，次高的字母为 U，请破译该密码。