## **第1章 概论习题答案**

**1. 试述密码学发展的四个阶段及其主要特征。**

**答：**

第一阶段，古代密码：远古一直到第一次世界大战；特征: 这一时期可看作科学密码学的前夜时期，这段时期的密码技术可以说是一种艺术。密码学专家通常凭直觉和信念来进行密码设计和分析，而不是推理证明，使用的密码体制为古典密码体制，主要原理是文字内容的代替、移位和隐藏等技巧。现在看来，古典密码体制大多数都比较简单而且容易破译。密码主要应用于军事、政治和外交，通信是由信使来传递的，加密的手段是使用手工。

第二阶段，机械密码：二次世界大战到1949年之前。特征：加密主要原理是字母的替换和移位，加密和解密的手段采用了机械和手工操作，破译则使用简单的词频分析，以及基于经验与想象的试探方法。

第三阶段，信息时代密码：1949年~1975年称为近代密码时期。特征：加密的对象既不是书写的文字，也不是有100多年历史的电报字码，而是电子形式的文件。人们可以将电子形式的文件转换成数字或数值符号，施以复杂的数学运算，达到数字符号的混淆、扩散和置换，实现加密、解密等各种控制的目的。传递信息的方法有无线通信、计算机网络等多种信息时代的传递方式。

第四阶段，现代密码：1976年至今称为现代密码学时期。特征：现代密码学的任务已经不局限于传统密码的保密通信，而是含义更广的信息安全，其中包括保密通信、数据加密、身份认证、数字签名、密钥协商、秘密分享等重要的功能。

**2. 什么是密码学？什么是密码编码学？什么是密码分析学？**

答：

密码学是研究密码与密码活动本质和规律，指导密码实践科学，主要探索密码编制、密码破译以及密码管理的一般规律。

密码编码学是指设计和研究密码通信系统，使其传递的信息具有很强的保密性和认证性的学科，是一门通过研究密码变化的客观规律，应用于编制密码以保守通信秘密的技术。

密码分析学是研究如何破解或者攻击受保护的信息的科学。指在没有加密密钥的情况下,攻击密文的过程。其目标就是要从密文得到明文或者由已知的条件得到密钥。

**3. 密码学的五元组是什么？它们分别有什么含义？**

答：

一个密码体制可以描述为一个五元组。

（1）是可能明文的有限集；

（2）是可能密文的有限集；

（3）是可能的密钥的有限集；

（4）是加密有限空间集合；

（5）是解密有限空间集合。

**4. 密码分析主要有哪些方式？各有何特点？**

答：根据密码分析者可能取得的分析资料的不同，密码分析可分为如下四类：

（1）唯密文攻击 (Ciphertext Only)：一种密码分析者只拥有密文进行密码攻击的方法；

（2）已知明文攻击（Known Plaintext）：一种利用大量互相对应的明文和密文进行分析的密码攻击方法；

（3）选择明文攻击（Chosen Plaintext）：一种选择特定明文和对应密文进行分析的密码攻击方法；

（4）选择密文攻击（Chosen Ciphertext）：一种选择特定密文和对应明文进行分析的密码攻击方法。

**5. 密码学的基本属性包含哪几方面？**

答：

信息的机密性、信息的真实性、数据的完整性和行为的不可否认性。

**6. 什么是对称密码体制和非对称密码体制？各有何优、缺点？**

答：在对称密码算法中，加解密使用相同的密钥；在非对称密码算法中，使用公钥进行加密，私钥进行解密。对称密码密码体制优点：加解密运行速度快、密钥相对较短、明密文长度相等、具有可靠的保密强度；不足：不便密钥交换和管理、密钥的分发需要安全通道、不能实现签名认证功能。非对称密码密码体制优点：密钥分发容易、便于密钥交换和管理、还可用于消息认证（数字签名）；不足：加解密运行速度缓慢、密钥长度过长、同时，其安全性所依赖的数学难题的复杂性一般都未能证明。