# 《应用密码学》试题

## 一、简单题（40 分）

**1. 简述密码学发展的三个阶段及其主要特点。**

答题要点：密码学的发展大致经历了三个阶段：

（1）古代加密方法。特点：作为密码学发展的起始阶段，所用方法简单，体现了后来发展起来的密码学的若干要素，但只能限制在一定范围内使用。主要基于手工的方式实现。

（2）古典密码。特点：加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法更复杂，但其变化量仍然 比较小。转轮机的出现是这一阶段的重要标志，传统密码学有了很大的进展，利用机械转轮可以开发出极其复杂的加密系统，缺点是密码周期有限、制造费用高等。

（3）近代密码。特点：这一阶段密码技术开始形成一门科学，利用电子计算机可以设计出 更为复杂的密码系统，密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密 码算法和各种攻击方法。另外，密码使用的范围也在不断扩张，而且出现了以 DES 为代表的 对称密码体制和 RSA 为代表的非对称密码体制，制定了许多通用的加密标准，促进网络和 技术的发展。

**2. 密码学的五元组是什么？它们分别有什么含义？**

答：密码学的五元组是指：{明文、密文、密钥、加密算法、解密算法}。

明文：是作为加密输入的原始信息，即消息的原始形式，通常用 $m$ 或表示。

密文：是明文经加密变换后的结果，即消息被加密处理后的形式，通常用 $c$ 表示。

密钥：是参与密码变换的参数，通常用 $k$ 表示。

加密算法：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程，通常用表示，即 $c = E_k\left(p\right)$。

解密算法：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程，通常用 $D$ 表示，即 $p = D_k\left(c\right)$。

**3. 从运行条件和安全条件两个方面比较常规密码体制和公开密钥密码体制并列举典型的**

| 分类 | 常规密码体制 | 公开密钥密码体制 |
|---|---|---|
| 运行条件 | 加密和解密使用同一个密钥和同一个算法。 | 用同一个算法进行加密和解密，而密钥有一对，其中一个用于加密，另一个用于解密。 |
| | 发送方和接收方必须共享密钥和算法。 | 发送方和接收方每个使用一对相互匹配、而又彼此互异的密钥中的一个。 |
| 安全条件 | 密钥必须保密。 | 密钥对中的私钥必须保密。 |
| | 如果不掌握其他信息，要想解密报文是不可能或至少是不现实的。 | 如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的。 |
| | 知道所用的算法加上密文的样本必须不足以确定密钥。 | 知道所用的算法、公钥和密文的样本必须不足以确定私钥。 |

**4. 解释群、交换群、有限群、有限群的阶、循环群、生成元、域、有限域、不可约多项式并举例说明。**

答：群由一个非空集合$G$组成，在集合$G$中定义了一个二元运算符“$\cdot$”，满足：

(1) 封闭性：对任意的$a,b\in G$，有：$a\cdot b\in G$；

(2) 结合律：对任何的$a,b,c\in G$，有：$a\cdot b\cdot c=(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

(3) 单位元：存在一个元素$1\in G$（称为单位元），对任意元素，有：$a\cdot 1=1\cdot a=a$；

(4) 逆元：对任意$a\in G$，存在一个元素$a^{-1}\in G$（称为逆元），使得：$a\cdot a^{-1}=a^{-1}\cdot a=1$。

如果一个群满足交换律，则称其为交换群。

如果一个群的元素是有限的，则称该群为有限群。

有限群的阶就是群中元素的个数。

如果群中每一个元素都是某一个元素$a\in G$的幂$a^k\in G$（$k$为整数），则称该群是循环群。

在循环群中，认为元素$a$生成了群$G$，或$a$是群$G$的生成元。

域是由一个非空集合$F$组成，在集合$F$中定义了两个二元运算符：“+”(加法)和“$\cdot$”(乘法)，并满足：

(1) $F$关于加法“+”是一个交换群；其单位元为“0”，$a$的逆元为$-a$。

(2) $F$关于乘法“$\cdot$”是一个交换群；其单位元为“1”，$a$的逆元为$a^{-1}$。

(3)(分配律)对任何的$a,b,c\in F$，有：$a\cdot(b+c)=(b+c)\cdot a=a\cdot b+a\cdot c$；

(4)(无零因子)对任意的$a,b\in F$，如果$a\cdot b=0$，则$a=0$或$b=0$。

如果域$F$只包含有限个元素，则称其为有限域。

不可约多项式是指不能再分解为两个次数低于该多项式最高次的多项之积的多项式。

**5. 画出分组密码算法的原理框图，并解释其基本工作原理。**

答：

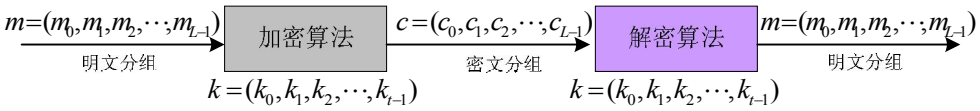


图5-1 分组密码原理框图

分组密码处理的单位是一组明文，即将明文消息编码后的数字序列$m_0,m_1,m_2,\cdots,m_i$划分成长为$L$位的组$m=(m_0,m_1,m_2,\cdots,m_{L-1})$，各个长为$L$的分组分别在密钥$k=(k_0,k_1,k_2,\cdots,k_{t-1})$（密钥长为$t$）的控制下变换成与明文组等长的一组密文输出数字序列$c=(c_0,c_1,c_2,\cdots,c_{L-1})$。$L$通常为64或128。解密过程是加密的逆过程。

**二、（15 分）求解：** $\begin{cases} x \equiv 2(\mathrm{mod}\,3) \\ x \equiv 1(\mathrm{mod}\,5) \\ x \equiv 1(\mathrm{mod}\,7) \end{cases}$

解： M = 3×5×7 = 105; M/3 = 35; M/5 = 21; M/7 = 15。

$35b_1 = 1 \pmod 3$

$21b_2 = 1 \pmod 5$

$15b_3 = 1 \pmod 7$

因此有： $b_1 = 2$; $b_2 = 1$; $b_3 = 1$。

则：$x = 2\times2\times35 + 1\times1\times21 + 1\times1\times15 = 176 \pmod{105} = 71$

**三、（15 分）用 Hill 密码加密明文“pay more money”，密钥是：** $k = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

解：明文“pay more money”可编码为：15 0 24；12 14 17；4 12 14；13 4 24。

由于：

$$(15\ \ 0\ \ 24)\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = [303\ \ 303\ \ 531]\ \mathrm{mod26}=[17\ 17\ 11]$$

$$(12\ \ 14\ \ 17)\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = [532\ \ 490\ \ 677]\ \mathrm{mod26}=[12\ 22\ 1]$$

$$(4\ \ 12\ \ 14)\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = [348\ \ 312\ \ 538]\ \mathrm{mod26}=[10\ 0\ 18]$$

$$(13\ \ 4\ \ 24)\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = [353\ \ 341\ \ 605]\ \mathrm{mod26}=[15\ 3\ 7]$$

故对应的密文为：RRLMWBKASPDH。

**四、（15 分）设通信双方使用 RSA 加密体制，接收方的公开密钥是（5,35），接收到的密文是 10，求明文。**

解：据题意知：$e = 5$，$n = 35$，$C = 10$。

因此有：$\varphi(n) = \varphi(35) = \varphi(5)\varphi(7) = 4\times6 = 24$

$d = e^{-1} \bmod \varphi(n) = 5^{-1} \bmod 24 = 5$

所以有：$M = C^d \bmod n = 10^5 \bmod 35 = 5$。

**五、(15分)利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是$E_{11}(1,6)$，生成元$G=(2,7)$，接收方A的秘密密钥$n_A = 7$。求：**

**（1）A的公开密钥$P_A$。**

**（2）发送方B欲发送消息$P_m = (10,9)$，选择随机数$k=3$，求密文$C_m$。**

**（3）显示接收方A从密文$C_m$恢复消息$P_m$的计算过程。**

**解：（1）** $P_A = n_A \times G = 7 \times (2,7) = (7,2)$。

**（2）**
$$C_m = \{kG, P_m + kP_A\} = \{3(2,7), (10,9) + 3(7,2)\}$$
$$= \{(8,3), (10,9) + (3,5)\}$$
$$= \{(8,3), (10,2)\}$$

**（3）** $P_m = (10,2) - 7(8,3) = (10,2) - (3,5) = (10,2) + (3,6) = (10,9)$。