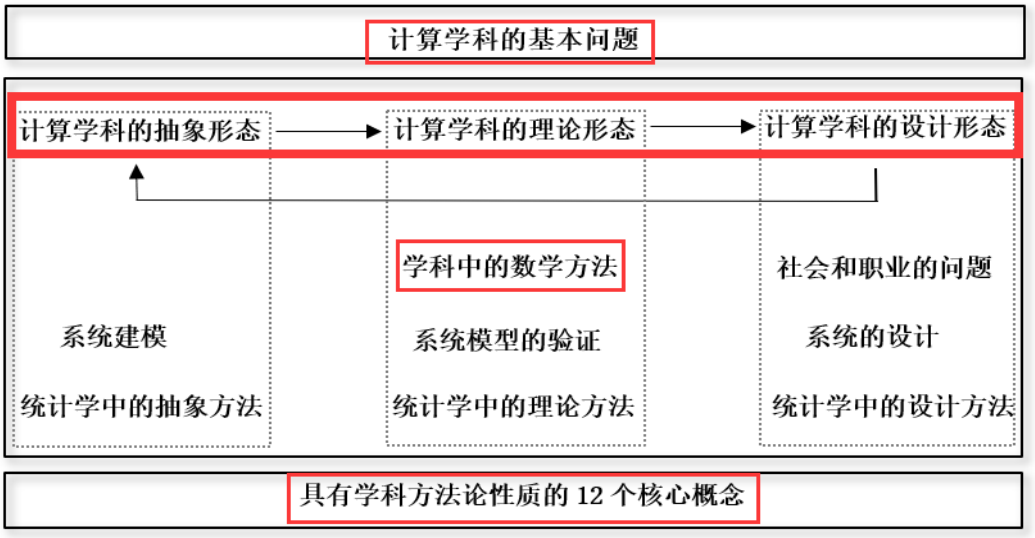
科学思维-样例：RSA 公开密钥密码系统

能力的评估：本案例能够置于 Bloom 分类法知识维度的“元认知知识”位置，学生学习后能够达到 Bloom 分类法认知过程维度的“创造”层次（针对初学者，或大学一年级学生而言）

一、本案例课程思政的关注点

1.本案例内容在计算课程思政总体结构框架中的位置



2.科学思维可拆分为可衡量、可检验、可评估的抽象、理论和设计三个过程（学科形态，或工作范式）。本例包含三个学科形态的内容，其中，RSA 形式模型和相应的算法描述可划分到抽象形态，模型中的 2 个谓词公式，以及解密公式的证明属于理论形态，实现该模型并构建轻量级密钥系统为设计形态的内容。学习该案例后，学生对抽象、理论和设计三个学科形态如何区分将有进一步的认知，这种认知将为我国在三个学科形态方面的工具（含思想与方法）的创新，实现“0 到 1”的突破种下科学思维的种子。

3.本案例包含计算学科课程思维总体框架中“计算学科中的核心概念”（形式模型），“计算学科的基本问题”（计算的时间复杂性），“学科中的数学方法”（证明）等内容，教师应将这些内容有意识的引导和激励学生。

4. 在本案例中，要求教师将 11 个品行元素中的“目标驱动、创意、严谨”与该案例绑定在一起进行可操作性解释。

二、 本案例的具体内容

计算复杂性理论在密码学研究领域起了十分重要的作用，它给密码研究人员指出了寻找难计算问题的方向，并促使研究人员在该领域取得了革命性的成果。公开密钥密码系统就是其中的典型例子。

第一个实用的在非保护信道中建立共享密钥的方法是 1976 年由迪菲（Whitfield Diffie）

与赫尔曼（Martin Hellman）建立的密钥交换方法（Diffie－Hellman key exchange，DH）。迪菲与赫尔曼为解决密钥管理的问题，在《密码学中的新方向》（*New Directions in Cryptography*）一文中给出了一种密钥交换协议。该协议允许在不安全的媒体上保证通信双方交换信息的安全。在迪菲与赫尔曼等人工作的基础上，很快出现了非对称密钥密码系统，其原理是将加密密钥和解密密钥分离，公开加密密钥，保存解密密钥。用公开密钥加密数据，数据以密文形式传播，只有拥有解密密钥才能解密。

目前，使用最为广泛的是 1978 年由李维斯特（R. L. Rivest）、萨莫尔（A. Shamir）和阿德曼（L. M. Adleman）在 *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* 一文中给出的 RSA 公开密钥密码系统，它通过 RSA 公钥算法，利用相应的“整数对”作为公钥和密钥对数据进行加密和解密。RSA 三位科学家因在公开密匙算法上所做出的杰出贡献而荣获 2002 年图灵奖。

1. RSA 公开密钥密码系统的形式模型

RSA=<p, q, n, m, e, d, k, c>

其中：

（1）$p, q, n, m, e, d, k, c \in Z^*$, $Z^*=\{1,2,3,\cdots\}$。

（2）p, q 为不同质数，$n = p \times q$。

（3）(e, n):公钥；(d, n):私钥。

（4）m: 原始报文，$m < n$。

（5）c: 加密后的报文。

（6）$\forall k(m^{k(p-1)(q-1)} (\mathrm{mod}\ n)) = 1$。

（7）$\exists k(\ ed = k(p-1)(q-1)+1)$。

（8）$c = m^e (\mathrm{mod}\ n)$。

（9）$m=c^d (\mathrm{mod}\ n)$。

2. 构建一个 RSA 公开密钥密码系统的步骤

（1）选择两个不同的质数 p, q。

（2）求 e，使得 e 与$(p-1)(q-1)$互质，且 $0<e<(p-1)(q-1)$。

（3）求 d，使 $\exists k(\ ed = k(p-1)\ (q-1)+1)$为真。

3. 在 RSA 公开密钥密码系统中的加密和解密

（1）对原始报文 m 加密，加密后的报文 $c = m^e (\mathrm{mod}\ n)$。

（2）根据加密后的报文 c，求原始报文 $m = c^d (\mathrm{mod}\ n)$。

在 RSA 公钥密码系统中，(e, n)是公钥，(d, n)是私钥，p 和 q 用来构建加密系统，由加密系统的构造者所有，不对外公开。

命题 $\forall k(m^{k(p-1)(q-1)} (\mathrm{mod}\ n)) = 1$ 可以用严密的数学方法证明，CS 导论课不做证明，但用一个例子做解释。

例 1 若 $p=3, q=11, n = 3\times11=33$。

设 $m=2$（$m<n$）, $k=1$。

$$m^{k(p-1)\,(q-1)} (\mathrm{mod}\ n) = 2^{1\times(3-1)\times(11-1)} (\mathrm{mod}\ 33)$$
$$= 2^{20} (\mathrm{mod}\ 33)$$
$$= 1\ 048\ 576\ (\mathrm{mod}\ 33)$$

$= 1$

设 $m=2$（$m<n$）, $k=2$。

$m^{k(p-1)(q-1)} (\text{mod } n) = 2^{2\times(3-1)\times(11-1)} (\text{mod } 33)$

$= 2^{40} (\text{mod } 33)$

$= 1\ 099\ 511\ 627\ 776\ (\text{mod } 33)$

$= 1$

设 $m=2$（$m<n$）, $k=3$。

$m^{k(p-1)(q-1)} (\text{mod } n) = 2^{3\times(3-1)\times(11-1)} (\text{mod } 33)$

$= 2^{60} (\text{mod } 33)$

$= 1\ 152\ 921\ 504\ 606\ 846\ 976\ (\text{mod } 33)$

$= 1$

证明 $c^d (\text{mod } n) = m$

证明：$c^d (\text{mod } n) = (m^e (\text{mod } n))^d (\text{mod } n)$

$= (m^e)^d (\text{mod } n)$

$= m^{ed} (\text{mod } n)$

$= m^{k(p-1)(q-1)+1} (\text{mod } n)$

$= m \times m^{k(p-1)(q-1)} (\text{mod } n)$

$= m \times 1$

$= m$

例 2 设 $p=3$, $q=11$, $n = 3\times11=33$，构建一个 RSA 公开密钥密码系统，并对报文 9 加密和解密。

构建 RSA 公开密钥密码系统的步骤如下。

（1）求 e

当 $p=3$, $q=11$ 时，$(p-1)\times(q-1) = (3-1)\times(11-1)= 20$

根据 RSA 公钥密码系统的构建，e 必须与$(p-1)\times(q-1)$互质，即与 20 互质。

设 $e=2$，$20 \bmod 2 = 0$

设 $e=3$，$20 \bmod 3 = 2$

由上可知，3 与 20 互质，因此，$e=3$。

（2）求 d

存在 k 使得 $ed = k(p-1)(q-1)+1$，因此，必定存在一个 k 使得

$d= (k(p-1)(q-1)+1)/e$

将 $e = 3$，$p=3$, $q=11$ 代入上式，有 $d =(20k+1)/3$

当 $k=1$ 时，$d=21/3=7$

根据题意，知 d 为整数，因此，$d=7$

因此，该 RSA 公钥密码系统的公钥为(3,33),私钥为(7,33)。

用公钥(3, 33)对 $m=9$ 进行加密

$c = m^e (\text{mod } n) = 9^3 (\text{mod } 33)$

$= 729 (\text{mod } 33)$

$= 3$

收到加密报文 3，用私钥(7, 33)进行解密

$c^d (\text{mod } n) = 3^7 (\text{mod } 33)$

=2187 (mod 33)

=9

例 3 设 p=223092827, q=218610473，n=487 704 284 333 771 171，构建一个 RSA 公钥密码系统（本题 p, q, n 的值来自“证比求易算法”）。

构建 RSA 公开密钥密码系统的步骤如下。

（1）求 e

p=223 092 827, q=218 610 473，则$(p-1)\times(q-1)$ = (223 092 827–1)×(218 610 473–1)

= 48 770 427 991 673 872

根据 RSA 公钥密码系统的构建，e 必须与 48 770 427 991 673 872 互质。

设 e=2，48 770 427 991 673 872 mod 2 = 0

设 e=3，48 770 427 991 673 872 mod 3 = 1

由上可知，3 与 48 770 427 991 673 872 互质，因此，e=3。

（2）求 d

存在 k 使得 $ed = k(p-1)(q-1)+1$，因此，必定存在一个 k 使得

$d= (k(p-1)(q-1)+1)/e$

将 e = 3，p=223 092 827, q=218 610 473 代入上式

d =(48 770 427 991 673 872k+1)/3

当 k=1 时，d=48 770 427 991 673 873/3

当 k=2 时，d=97 540 855 983 347 745/3

=32 513 618 661 115 915

根据题意，知 d 为整数，因此，d=32 513 618 661 115 915。

因此，该 RSA 公钥密码系统的公钥为(3, 487 704 284 333 771 171)，私钥为(32 513 618 661 115 915, 487 704 284 333 771 171)

在 RSA 公开密钥密码系统中，加密密钥（e, n）与加密报文(c)均通过公开途径传送，对于巨大的质数 p 和 q，计算 $n=p\times q$ 非常简单,而相对的逆运算就费时了。这种“单向性”的函数称为单向函数。任何单向函数都可以作为某种公开密钥密码系统的基础，而单向函数的安全性也就是这种公开密钥密码系统的安全性。

三、教学体会

概念模型和形式模型是计算学科中具有学科方法论性质的核心概念，它将计算学科各分支领域有机联系在一起，是对计算问题进行抽象的有力工具，它大大地降低了人们沟通的复杂性。本案例构建了 RSA 公开密钥的形式模型，给出了相关算法，以及元素之间关系的部分证明。这个案例，体现了抽象、理论和设计三个学科形态的相互关系，同学们只从模型出发，就可以用纸笔手算的方式构造一个轻量级的公开密钥系统。

四、激励、唤醒和鼓励同学们向上的途径

公开密钥的关键，就是要找到在时间和空间上足够复杂的“单向函数”，并用数学的方式进行严格的证明。通过这个案例，鼓励同学们采用严密的数学方法，通过模型，构建安全的加密系统。

五、习题

设 p=11, q=13，请构建一个 RSA 公钥密码系统，并对报文 9 加密和解密。

参考文献

1. 董荣胜. 计算机科学导论（第 3 版）. 高等教育出版社，2015