RSA 公开密钥密码系统

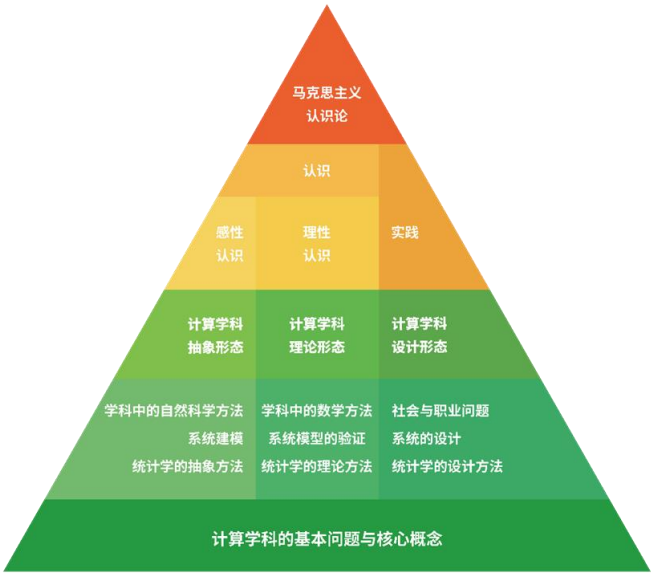
计算机课程思政虚拟教研室 科学思维样例 2

一、 教学目标

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。

二、 本案例课程思政的关注点

1.本案例内容在计算学科课程思政总体框架中的位置：计算学科抽象、理论和设计三形态，学科中的数学方法，计算学科的基本问题与核心概念。



2.科学思维可拆分为可衡量、可检验的抽象、理论和设计三形态。其中，RSA 公开密钥密码系统的抽象形态包括形式模型、算法过程、加密和解密的过程。理论形态包括欧拉定理、费马小定理、密钥选择、加密过程和解密过程的时间复杂度以及系统的空间复杂度。设计形态包括 RSA 公开密钥密码系统的 Python 程序。

3.在本案例中，要求与 CC2020 中的“**主动性**”品行，以及 CS2023“安全”中的“**严谨性、自我指导、协作性、责任感、负责任**”品行对齐，并与该案例绑定在一起进行可操作性解释。

三、 本案例中的抽象、理论和设计三形态

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抽象形态

a） RSA公开密钥密码系统的形式模型

b） RSA算法过程

c） RSA算法中的关键谓词公式：其中包括了模指数运算的性质，即如果知道公钥(e, n)，无法直接推算出私钥d，这是基于数论中模线性方程无有效解析解的特性。

d） RSA公开密钥密码体制的定义：RSA是一种非对称密码系统，它的核心在于公开的加密密钥与私有的解密密钥之间存在着数学上的关联但不能轻易被第三方推算出来，从而保证了数据的安全传输。

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

（7）$\exists k(\ ed = k(p-1)(q-1)+1)$。

（8）$c = m^e(\text{mod } n)$。

（9）$m=c^d(\text{mod } n)$。

（2）RSA公开密钥密码系统的算法过程

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 $c = m^e(mod\ n)$。

2）根据加密后的报文 c，求原始报文 $m = c^d(mod\ n)$。

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。

下面用几个例子来加深对形式模型和算法的理解。

例 1 若 p=3, q=11, n = 3×11=33。

设 m=2（$m<n$）, k=1。

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

$= 2^{20}(mod\ 33)$

$= 1\ 048\ 576\ (mod\ 33)$

$= 1$

设 $m=2$（$m<n$）, $k=2$。

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

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

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

$= 1$

设 $m=2$（$m<n$）, $k=3$。

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

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

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

$= 1$

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 $e=2$，$20\ mod\ 2 = 0$

设 $e=3$，$20\ mod\ 3 = 2$

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

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

$= 729\ (mod\ 33)$

$= 3$

收到加密报文 3，用私钥(7, 33)进行解密

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

$=2187\ (mod\ 33)$

$=9$

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) ×(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。

2. RSA **公开密钥密码系统的理论形态**

（1）欧拉定理：在数论中,欧拉定理（也称费马-欧拉定理），它是一个关于同余性质的定理。欧拉定理表明，若 n、a 为正整数，且 n、a 互质，则

$a^{\varphi(n)}(mod\ n) = 1$

其中，欧拉函数 $\varphi(n)$表示不大于 n 且与 n 互质的正整数的个数。

$$\phi(n)=\begin{cases} n-1, & n为质数 \\ \phi(p)\phi(q)=(p-1)(q-1), & n=pq且p、q均为质数 \end{cases}$$

（2）费马小定理：若 p 为质数，且 a、p 的最大公约数 $Gcd(a,p) = 1$，则 $a^{(p-1)}(mod\ n) = 1$。

即：若 a 为整数，p 为质数，且 a、p 互质（即两者只有一个公约数 1），则 $a^{(p-1)}$除以 p 的余数恒等于 1。

费马小定理在选择公钥和私钥时确保加密和解密过程的可行性上起着关键作用。

证明这个定理非常简单，由于 p 是质数，所以有 $\varphi(p) = p - 1$，代入欧拉定理即可证明。

（3）密钥选择：公钥 e 需要满足与 $\varphi(n)$互质的条件，而私钥 d 则是 e 模 $\varphi(n)$的乘法逆元，满足 $ed \equiv 1(mod\ \varphi(n))$。

（4）加密过程的时间复杂度为 $O(log_{2(m)})$，解密过程的时间复杂度为 $O(log_{2(c)})$。

（5）空间复杂度为 $O(log_{2(n)})$。

下面给出一个简单的例子帮助理解欧拉定理

令 a=3、n=7，a、n 互质。在比 7 小的正整数集合中与 7 互质的数有 1、2、3、4、5、6，所以 $\phi(7)$=6.

计算 $a^{\phi(n)}(mod\ n) = 3^6(mod\ 7) = 729\ mod\ 7 = 1$，与定理结果相符。

下面分别对公式 6、7、9 进行证明

证明公式 6：$\forall\ k(m^{k(p-1)(q-1)}(mod\ n)) = 1$

为了证明这个公式，需要用到欧拉定理。欧拉定理指出：如果 $(\ gcd(a, n) = 1\ )$，那么 $a^{\phi(n)} \equiv 1(mod\ n)$，其中 $\phi(n)$是欧拉函数。

对于 RSA，$(\ n = pq\ )$ 是两个不同质数 p 和 q 的乘积，所以 $\phi(n) = (p-1)(q-1)$ 。

现在，根据欧拉定理，对于 Z 中的任何数 m，有：

$m^{\phi(n)} \equiv 1(mod\ n)$由于$\forall k \in Z$，$k\phi(n)$是 $\phi(n)$的倍数，可以写成：

$m^{k\phi(n)} \equiv (m^{\phi(n)})^k \equiv 1^k \equiv 1(mod\ n)$这就证明了对于所有整数 k，m 的 $k(p-1)(q-1)$次幂模 n 总是等于 1，符合公式（6）的要求。

所以，对于$\forall k \in Z$，公式 $(\ m^{k((p-1)(q-1))}\ mod\ n = 1\ )$ 成立，这基于 m 和 n 互质的假设，这在 RSA 算法中是成立的，因为 m 是明文消息，通常选择为小于 n 的非负整数，并且当 n 是两个不同质数的乘积时，除了这两个质数外，m 与 n 是互质的。

证明公式 7：$\exists k(\ ed = k(p-1)(q-1)+1)$

公式（7）是基于 ed 是模 $\phi(n)$ 下的逆元。如果两个数是某个数的模逆元，它们相乘的结果模这个数为 1。这个数在 RSA 中就是 $\phi(n)$。所以，如果 $ed \equiv 1(mod\ \phi(n))$，则存在一个整数 k，使得：

$ed-1=k\phi(n)$

$ed-1=k(p-1)(q-1)$

将上面的等式两边同时加 1，得到：

$ed=k(p-1)(q-1)+1$

这就证明了存在一个整数 k，满足 $ed=k(p-1)(q-1)+1$，即公式（7）。

证明公式 9：$c^d(mod\ n) = m$

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

$=(m^e)^d(mod\ n)$

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

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

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

$=m \times 1$

$=m$

2. RSA 公开密钥密码系统的设计形态

根据 RSA 公开密钥密码系统计算的形式模型和算法过程，使用 Python 语言实现该算法。

```
from sympy import randprime, mod_inverse, gcd
import random
# Step 1: Choose two different prime numbers p and q
p = randprime(100, 300)
q = randprime(100, 300)
while p == q:
    q = randprime(100, 300)
```

```
# Step 2: Compute n = p * q and phi(n) = (p - 1) * (q - 1)
n = p * q
phi_n = (p - 1) * (q - 1)

# Step 3: Choose e such that e is coprime to phi(n) and 1 < e < phi(n)
e = random.randrange(2, phi_n)
while gcd(e, phi_n) != 1:
    e = random.randrange(2, phi_n)

# Step 4: Calculate d, the mod inverse of e with respect to phi(n)
d = mod_inverse(e, phi_n)

# Public and private keys
public_key = (e, n)
private_key = (d, n)

# Example message
m = 42    # Original message

# Encrypt the message: c = m^e mod n
c = pow(m, e, n)

# Decrypt the message: m = c^d mod n
decrypted_m = pow(c, d, n)

# Output the results
print(f"Prime p: {p}")
print(f"Prime q: {q}")
print(f"Public Key (e, n): {public_key}")
print(f"Private Key (d, n): {private_key}")
print(f"Original Message: {m}")
print(f"Encrypted Message: {c}")
print(f"Decrypted Message: {decrypted_m}")
```

运行得到计算结果：

```
Prime p: 137
Prime q: 277
Public Key (e, n): (623, 37949)
Private Key (d, n): (37295, 37949)
Original Message: 42
Encrypted Message: 22965
Decrypted Message: 42
```

四、 专业品行

在教授 RSA 公开密钥密码系统的案例中，学生不仅学习了如何应用形式模型进行加密和解密计算，还体会到了计算学科中几个重要品行元素的实际应用。具体到本案例，这些品行元素包括主动性、严谨性、自我指导、协作性、责任感和负责任。下面结合教学目标、课程思政的关注点以及三形态的相关内容，对这些品行元素进行具体的可操作性解释。

1.主动性（Proactivity）

在 RSA 公开密钥密码系统的案例中，主动性体现在学生主动探索公钥和私钥生成的数学原理，并将其应用于实际的加密和解密过程中。学生被鼓励主动寻找 RSA 算法的额外应用场景，比如数字签名和安全通信，从而将理论知识与实践相结合。

2.严谨性（Meticulous）

在计算公钥和私钥、进行加密和解密操作的每一步中，严谨性都至关重要。学生必须仔细遵循算法的步骤，确保每个数学操作和编程实现的准确性，从而保证加密系统的安全性。

3.自我指导（Self-directed）

本案例鼓励学生自主学习 RSA 算法背后的数学原理，如欧拉定理和模反元素的概念。在学习过程中，学生需要自我引导，通过在线资源、教科书和学术论文深化对算法的理解。

4.协作性（Collaborative）

在实现 RSA 算法的编程任务中，学生通过团队合作来分担编程任务和解决问题。这不仅提高了他们解决复杂技术问题的能力，也培养了他们在团队环境中有效沟通和合作的能力。

5.责任感（Responsible）

学生在了解 RSA 公开密钥密码系统的过程中，将认识到信息安全在现代通信中的重要性，并理解作为未来的计算机科学家和工程师，在设计和实现加密技术时需要承担的社会责任和道德义务。

6.负责任（Accountable）

通过反复的编程实践和测试，学生学会了在整个加密和解密过程中承担责任，确保每一步操作都符合安全和正确性的标准。当面对编程错误和逻辑问题时，他们学会了负责任地解决问题，直到找到正确的解决方案。

通过 RSA 公开密钥密码系统案例的学习，学生不仅获得了关键的计算机科学知识和技能，更通过实践活动学会了如何展现良好的专业品行，这些品行将指导他们在未来面对挑战时展现出主动性、严谨性、自我指导、协作性、责任感和负责任。

五、 激励、唤醒和鼓励同学们向上的途径

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相关证明。这个案例，体现了抽象、理论和设计三形态的相互关系，同学们只从模型出发，就可以用笔纸手算的方式构造一个轻量级公开密钥系统。

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。

六、 习题

1. 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。

2. 设 p=17，q=19，请构建一个 RSA 公钥密码系统，并对报文 m=123 进行加密和解密。

3. 给定 RSA 公钥为 (e,n)=(7,143)，其中 n 是两个质数的乘积，试找出这两个质数并构建对应的私钥。

4. 如果你有一个 RSA 加密的报文 c=65，公钥 (e,n)=(5,221)，试计算解密后的报文 m。

5. 假设在 RSA 系统中，某人选取了 p=23 和 q=29 作为密钥的一部分。如果公钥的 e 值为 3，请计算对应的私钥。

参考文献

[1] 陈国良.计算机课程思政虚拟教研室文化建设[J].计算机教育, 2023(11):1-2.

[2] 董荣胜，古天龙，殷建平.计算学科课程思政教学指南[J].计算机教育,2024(01): 7-15.

[3] 董荣胜.计算机科学导论—思想与方法（第 4 版）[M].北京：高等教育出版社，2024.