# 密码学课程思政教学设计--以 RSA 算法为例*

周素芳 袁科* 杜晓玉 王钰野 杨欣欣 闫永航

1 河南大学计算机与信息工程学院，开封 475004
2 河南大学河南省空间信息处理工程研究中心，开封 475004

**摘 要** 网络空间安全是维护国家安全的关键环节，密码学是保障网络空间安全的核心技术，是密码科学与技术专业、信息安全专业和网络空间安全等专业的基础课，结合该课程开展思政教育至关重要。文章结合 RSA 算法的教学设计，探讨如何将思政内容与密码学专业知识深度融合。首先根据国家和行业发展需要设计教学目标，在深入挖掘和提炼思政元素的基础上，通过案例引入思政内容。同时通过思政教育进行价值塑造，培养学生维护国家安全的意识、民族文化自信、科学精神和责任担当意识，实现育人与育才过程的统一。最终通过对比密码学课程加入思政元素前后教学结果发现学生学习效果有较好地提升。

**关键字** 课程思政，密码学，教学设计，RSA 算法

# Ideological and Political Course Teaching Design of Cryptography -- Taking RSA Algorithm as an Example

Sufang Zhou Ke Yuan* Xiaoyu Du Yuye Wang Xinxin Yang Yonghang Yan

1. School of Computer and Information Engineering, Henan University, Kaifeng 475004, China
2. Henan Province Engineering Research Center of Spatial Information Processing, Henan University, Kaifeng 475004, China；yuanke@henu.edu.cn

**Abstract—Cyberspace security is a key link to maintain national security. Cryptography is the core technology to ensure cyberspace security. It is a basic course for cryptology science and technology, information security, cyberspace security and other majors. It is vital to carry out ideological and political education in combination with this course. Combining the teaching design of RSA algorithm, this paper discusses how to deeply integrate the ideological and political content with the professional knowledge of Cryptography. Firstly, design teaching objectives based on the development needs of the country and industry, and introduce ideological and political content through case studies based on in-depth exploration and refinement of ideological and political elements. At the same time, ideological and political education is used to shape values, cultivate students' awareness of maintaining national security, national cultural confidence, scientific spirit, and sense of responsibility, and achieve the unity of education and talent cultivation processes. Finally, by comparing the teaching results before and after adding ideological and political elements to cryptography courses, it was found that the learning effectiveness of students was significantly improved.**

**Keywords—Ideological and political courses, cryptography, teaching design, RSA algorithm**

## 1 引 言

我国高等教育的一个核心任务就是培养德智体美全面发展的人才，其根基在于立德树人[1]。习近平总书记在全国高校思想政治工作会议上指出，高校要把“立德树人”作为中心环节，把思想政治工作贯穿教学全过程，实现全程育人，全方位育人，努力开创我国高等教育事业发展的新局面[2]。课程思政形式灵活多样，没有统一的范式，其落地见效的主要渠道是课内外教学活动。在教学中，教师要结合教学内容，适时适度进行价值观引领和品行塑造[3]。高层次密码人才素质和水平是实施网络安全战略极其重要的支撑，高层次密码人才要有较高的技术水平，更要有过硬的思想政治素质[4]。在密码学人才培养的过程中，专业课教师应根据密码学的特色和知识，挖掘和提炼专业知识中蕴含的家国情怀、高尚品格、专业理论、科学精神等价值内涵，培养学生的爱国主义精神，促进学生的全面发展，实现育人与育才的过程相统一。

密码学是集数学、计算机科学以及通信与信息系统等多学科一体的交叉学科，其能有效保证信息的机密性、完整性、可用性、可控性和不可否认性，为保护信息安全提供了理论依据和丰富的应用实践[5]。目前密码学课程思政还存在一些误区，据权威显示，有近 90%的教师认为思政教育不属于专业课的

* **基金资助**：本文得到河南大学本科教学改革研究与实践项目“新工科背景下《大数据分析数学基础》金课建设教学改革（HDXJJG2021-120）”、“新工科背景下面向小班授课的《C++程序设计》混合式教学研究”、河南省教师教育课程改革研究项目（2022-JSJYYB-025），河南省重点研发与推广专项项目（科技攻关 222102210007）资助。

职责范围[6]，有近 70%的学生认为专业课于思政教育融合不足[7]。在思政教育的大背景下，密码学任课教师应紧密结合教学目标和教学内容，积极探索发掘思政元素，开展密码学教学中的思政教育，提升思政水平和科学文化知识水平。

## 2 教学设计

按照工程教育认证标准[8]以目标为导向进行教学设计[9]，包括课程目标设计、课程导入设计和教学过程设计三个部分。

### 2．1 课程目标设计

教师要从专业角度出发，深度挖掘提炼课程专业知识中蕴含的思想价值与精神内涵，增强课程的知识性与人文性，拓展学生知识的同时，培育学生的家国情怀。课程目标的设置从三个层面着手：

① 知识目标：使学生了解 RSA 算法涉及的理论和定理，掌握基本实现原理，重点掌握公钥加密算法的加密和解密过程。

② 能力目标：使学生能够主动对知识进行信息检索，激发学生的内在学习动力，成为具备自主学习的能力。

③ 育人目标：使学生明白维护国家安全的重要性，坚定民族自信，弘扬爱国主义精神，树立科技报国的情怀。

### 2．2 课程导入设计

导入引言：2007年起，美国国家安全局展开了一项绝密的电子监听计划，在9家互联网公司进行数据挖掘，秘密监听用户的通话信息、即时通讯、电子邮件、聊天记录、视频文件等，收集了970亿条用户数据，监控范围覆盖全球近70亿人，其中包括35个国家的政要。

通过美国“棱镜”监听事件使学生了解到安全管理的重要性，密码学在国家安全维护中的重要地位，进而引入课程RSA公钥加密的内容。

### 2．3 教学过程设计

教学过程设计离不开知识的讲解，首先以科学知识为基础开始进行内容讲授。随后为提升课程的高阶性和趣味性，引入共模攻击实验，使学生了解安全的辩证思维，以激发和培养学生的内生探索精神。在进行知识讲授的同时有机地抓住知识中的关键点开展思政教育延伸。

（1）内容讲解

① RSA简介

RSA是Rivest、Shamir和Adleman三位密码学家姓氏首字母的缩写以纪念他们在1977年一起提出的RSA加密算法[10]。RSA是第一个提出来的基于大整数因式分解困难性的算法，也是被研究得最广泛的一种加密算法。该算法既可以用于对传输信息的加密也可以用于实现数字签名系统，被公认为应用最多的算法，是目前网络上进行保密通信和数字签名的最有效的安全算法之一。

② RSA算法

RSA加密算法包括密钥生成、加密和解密算法，具体如下。

**密钥生成：**任意选取两个不同的大素数$p$和$q$，计算乘积$n=p*q$，计算$n$的欧拉函数

$$\phi(n)=(p-1)(q-1)。$$

任意选取一个大整数$e\in Z_n^*$，使得

$$\gcd(e)=(e,\phi(n))=1，$$

整数$e$用做加密密钥。计算解密密钥

$$d=e^{-1}\bmod\phi(n)。$$

将$e$公开，$d$保密，RSA算法的公钥PK=($e$,$n$)，私钥SK=($d$,$n$)。

**加密：**设$m\in Z_n^*$为明文，$E$为加密算法，利用公钥PK=($e$,$n$)加密，得到密文

$$c=E(m)=m^e \bmod n。$$

**解密：**设$c\in Z_n^*$为密文，$D$为解密算法，利用私钥SK=($d$,$n$)解密，得到明文

$$m=D(c)=c^d \bmod n。$$

使用RSA算法进行数字签名的过程类似于加密过程，但在签名过程中需要签名者使用私钥进行签名，以保证签名的不可伪造性，同时任何人可以作为验证者根据公钥能对签名者进行验证。

③ RSA的正确性

根据欧拉定理可知：

$$m=D(c)=m^{ed} \bmod n$$
$$=m^{\phi(n)} \bmod n=m。$$

④ RSA的安全性

RSA的安全性依赖于大整数分解的困难。当只有公钥时，很难从密文中恢复出明文，其难度等价于分解两个大素数之积。RSA算法的安全强度随着密钥长度的增加而增强，所以RSA需要采用足够大的整数密钥，现有的整数分解方法有二次筛选法、随机

平方法等分解1024位以上的大整数仍然比较困难，因此采用1024位以上密钥时可以认为是安全的。

⑤ 基于中国剩余定理的RSA改进

RSA中计算耗时最大的部分是解密操作，由于$d$值往往较大，故计算难度较高。中国剩余定理可用于RSA解密运算，使其解密速度大约提高4倍左右，这对于无论软件还是硬件实现RSA密码算法都是非常重要的。

**定理1（中国剩余定理）：**设$m_1,...,m_k$是$k$个两两互素的正整数，

$$m = m_1 \cdot m_2 \cdot \ldots \cdot m_k，\text{且} m = m_i \cdot M_i,$$

同时

$$M'_i \cdot M_i \equiv 1(\bmod m_i)，\ \text{i=1,2,...}k,$$

则对任意的整数$b_1,\ldots,b_k$，同余式组

$$\begin{cases} x \equiv b_1(\bmod m_1) \\ \ldots\ldots \\ x \equiv b_k(\bmod m_k) \end{cases} \tag{1}$$

有唯一解：

$$\sum_{i=1}^{k} b_i M'_i M_i(\bmod m)。$$

所以解密RSA的流程可以分解为

$$m_1 = c^d(\bmod p)和m_2 = c^d(\bmod q)$$

的方程组，根据欧拉定理，可以进一步降阶为

$$m_1 = c^{d \bmod (p-1)}(\bmod p)，$$

$$m_2 = c^{d \bmod (q-1)}(\bmod q)，$$

其中

$$d_P = d\ mod\ (p-1) = \frac{1}{e}\ mod\ (p-1)，$$

$$d_Q = d\ mod\ (q-1) = \frac{1}{e}\ mod\ (q-1)。$$

则在生成密钥时需要参数$p$，$q$，$d_P$，$d_Q$，以及

$$q_{inv} = q^{-1}\ mod\ p\ ，$$

最终生成的私钥就是$(p,q,d_P,d_Q,q_{inv})$。

基于中国剩余定理解密：

$$m_1 = c^{d_P}(\bmod p)，$$

$$m_2 = c^{d_Q}(\bmod q)，$$

$$h = q_{inv}(m_1 - m_2)\bmod p，$$

$$m = (m_2 + hq)\bmod (p * q)$$

这样虽然要计算两次模幂运算，但是效率依然比直接计算高。

```
Step1   调用函数gcdEx(e1, e2, &rr, &ss); //求满足e1*rr+e2*ss=1的rr,ss, gcd(e1,e2)=1
Step2   计算c1^rr
        if (rr < 0)     //如果rr<0, 计算1/(c1^(-rr)):先计算c1^(-rr),再计算其关于mod n的逆元
                        {
                        int tmppower1 = Quick_Power(c1, -rr, n);
                        mm1 = ext_eculid(tmppower1, n); //求逆元
                        }
        else            mm1 = Quick_Power(c1, rr, n); //计算c1^rr mod n
Step3   计算c2^ss
        if (ss < 0)     //如果ss<0, 计算1/(c2^(-ss)):先计算c2^(-ss),再计算其关于mod n的逆元
                        {
                        int tmppower2 = Quick_Power(c2, -ss, n);
                        mm2 = ext_eculid(tmppower2, n); //求逆元
                        }
        else            mm2 = Quick_Power(c2, ss, n); //计算c2^ss mod n
Step4   破解出明文
        mm = Quick_Multiply(mm1, mm2, n); //计算c1^rr*c2^ss mod n,即为明文
```

图 1 共模攻击实验步骤

（2） 实验

为了避免出现“满堂灌”等枯燥乏味的理论教学方式，选择具有实际应用背景、典型的案例融入教学设计中，使课程内容更加形象、丰富，加深学生对知识的理解，提高学生的实践能力[11]。

**案例：** RSA算法中的共模攻击

**问题：** 若用户user1和user2共享模数n=524747，

他们的公钥e1、e2分别是30283，8209。若攻击者截获user1和user2对同一明文m加密的结果分别是c1=51 297、c2=365 457。求解攻击者破解明文m的方法并进行验证。具体实验步骤如图1。实验运行结果如图2。

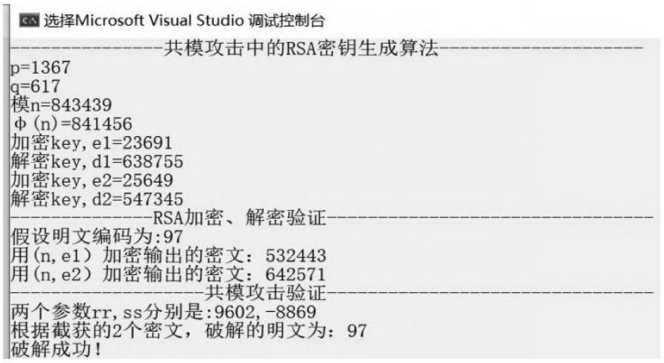


图 2 共模攻击实验验证结果

（3） 思政教育延伸

中国剩余定理又称孙子定理，出自中国古代数学著作《孙子算经》，是我国古代杰出的数学成果。《孙子算经》在汉明帝年就存在了，也就是公元四、五世纪，大约一千五百年前，这反映了中国古代劳动人民很早就在数论方面做出了杰出贡献。南宋数学家秦九韶将其进一步发展为“大衍求一术”，明朝数学家程大位在《算法统宗》中将“大衍求一术”总结为一首通俗易懂的歌诀：“三人同行七十稀，五束梅花廿一枝，七子团员正月半，除百令五便得知。”将数学问题融入诗歌中，极具美学意义，体展现了中国传统文化的独特魅力。

中国剩余定理在代数学、分析学中有着及其重要的应用，在工程技术中经常使用的拉格朗日插值公式其本质就是中国剩余定理。苏联数学家尤里马季亚谢维奇在解决希尔伯特提出的23个问题中的第十个问题时，就用到了中国剩余定理。中国剩余定理不是中国人自己命名的定理，而是西方学者命名的，由此可见此定理受到西方数学界的认可，他们认为这个定理就是我们中国人发现的。由此可以窥见古代中国人在数学上的巨大贡献，中国剩余定理是我们中国人的骄傲。

## 3 思政元素分析

① 自觉国家安全维护

密码学是维护国家安全的重要战略资源，密码工作关系到国家的政治安全，经济安全，国防安全和信息安全。通过美国“棱镜”监听事件，让学生有更强烈的国家安全维护意识。

② 增强民族文化自信

通过中国剩余定理让学生了解到中国人是有很高的数学天赋的，具有很强的创造力，中国数学在历史上很长一段时间是领先的，增强民族文化自信。

③ 勇担科技强国使命

通过我国在近代数学的没落，高精尖科技的落后，让学生明白科学强国的重要性，培养其责任感，潜心研究，使其自主地为国家科学事业的发展做出努力。

## 4 教学反思

本次思政教学选取 RSA 算法作为案例，将对中国剩余定理的介绍作为思政内容的导入点，在教学过程中通过典型案例的练习来避免枯燥的理论教学。在课后布置作业要求学生编写一段代码，对已有文本进行加密，让学生进一步理解掌握所学内容；让学生查阅资料了解量子计算机的发展对破解 RSA 算法的挑战，让学生理解科技的发展对安全发展的要求；同时布置文献撰写工作，拓展思政教育的广度与深度。另外，通过自主查阅资料，学生进一步坚定民族自信，坚定爱国主义信念。通过思政课程的实施，增强学生的学习动力。

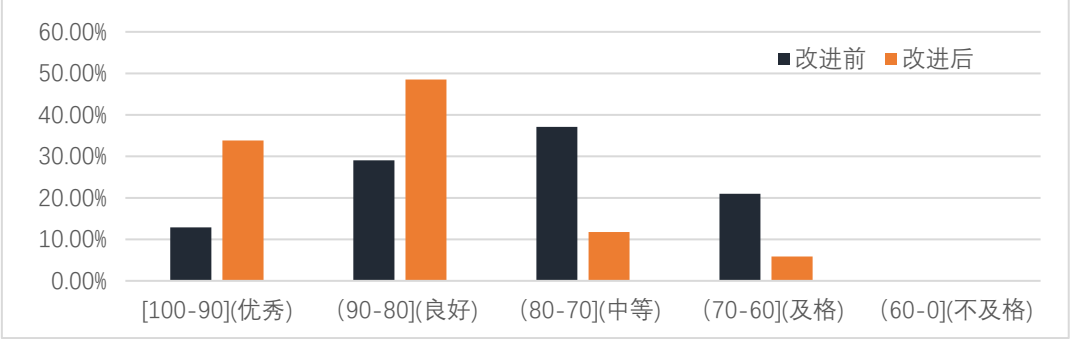


图 3 思政教学改进前后学生成绩分布对比

思政课程必须以学生为中心，以学习成果为导向，依据课程目标不断改进。同时，教师应及时关注每个学生的学习状况，根据学生反馈及时调整教学内容提升课程思政成效。通过教学评价分析知识、能力和育人目标达成情况，进而优化教学设计、教学方法和教学内容，持续改进教学，不断提高专业教育目标和思政育人目标的达成度，持续提升课程育人实施质量。

我院于 2018 年获批信息安全专业，并于 2019 年开始招生，密码学是该专业的核心课程，开设在大二下学期，现已开展两次完整教学，2021 年春季和 2022 年春季。通过课程组成员的筹备，在 2022 年春季学期开始将本文所述课程思政教学方法引入实际教学过程中，取得了良好成效。

2021 年春季学期密码学课程授课学生 62 人，期末成绩满分 100 分，最终成绩在[100-90]分的学生 8 人占 12.90%，(90-80]分的学生 18 人占 29.03%，(80-70]分的学生 23 人占 37.10%，(70-60]分的学生 13 人占 20.97%，(60-0]分的学生 0 人。2022 年春季学期密码学课程授课学生 68 人，期末成绩满分 100 分，最终成绩在[100-90]分的学生 23 人占 33.82%，(90-80]分的学生 33 人占 4853.%，(80-70]分的学生 8 人占 11.76%，(70-60]分的学生 4 人占 5.88%，(60-0]分的学生 0 人。实施思政教学后学生成绩相较于之前有明显提升，具体对比分布如图 3 所示。

## 5 結束語

课程思政是教学中的必要环节，也是实现“立德树人”的重要举措。本文以 RSA 公钥算法教学为例，将密码学课程内容与思政教育紧密结合，并探讨了如何从教师的角度做好课程思政。在具体的教学实施中，立足密码学人才培养目标，确定了知识、能力和育人目标，通过情景导入法引入思政元素，实施案例教学，进行思政教育拓展，实现了思政元素与专业教学内容之间的深度融合，做到在专业课教学中实现价值构建，培养德才兼备的信息安全人才。

## 参 考 文 献

[1] 窦本年,许春根,金晓灿.密码学课程中的人文素质教育[J].计算机教育,2019,No.291(03):1-3+7.

[2] 习近平. 习近平总书记在全国高校思想政治工作会议上的重要讲话[N]. 人民日报, 2016-12-09(1).

[3] 朱成,袁河.基于图表的密码学课程思政教学探索[J].计算机教育,2022,326(02):26-29.

[4] 张仕斌,万武南,蒋海龙等.应用密码学课程思政教学探索[J].计算机教育,2022,No.335(11):47-51.

[5] 张薇,周潭平,刘文超.密码学课程思政设计[J].计算机教育,2022,No.327(03):81-84.

[6] 何源.高校专业课教师的课程思政能力表现及其培育路径[J].江苏高教,2019, 225(11):80-84.

[7] 赵鹤玲.新时代高校“课程思政”建设的现状及对策分析[J].湖北师范大学学报(哲学社会科学版),2020,40(01):108-110.

[8] 刘雪花.工程教育认证背景下《单片机原理与应用》课程思政初探[J]. 计算机技术与教育学报,2022,10(02):79-82.

[9] 于延,李英梅,李红宇,范雪琴,于龙.融合 OBE 导向的案例式课程思政教学模式设计[J]. 计算机技术与教育学报,2021,9(01):63-65.

[10] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems [J].Communications of the Acm, 1978, 21(2):120-126.

[11] 邓芳,叶文,卢向群,梁美玉.《数据库系统原理》实验环节课程思政研究与实践[J]. 计算机技术与教育学报,2022,10(03):43-46.