# 《应用密码学（Applied Cryptography)》教学大纲

制定时间：2024 年 3 月

## 一、课程基本信息

**（一）适用专业：**本科计算机科学与技术

**（二）课程代码：**3ZN1010A

**（三）学分/课内学时：**2 学分/32 学时

**（四）课程类别：**专业教育

**（五）课程性质：**选修/理论课

**（六）先修课程：**《高等数学（理工）》、《C 语言程序设计与应用》、《数据结构 B》

**（七）后续课程：**《Web 安全技术》、《TCP/IP 网络程序设计》、《网络安全技术》、《网络安全技术综合训练》、《区块链》

## 二、课程教学目标

《应用密码学》是计算机、通信、应用数学、软件工程等专业的交叉学科，在网络与信息安全领域应用广泛，受到高度重视。

本课程主要通过理论教学、实验教学等环节，全面介绍应用密码学的基本概念、基本理论和典型实用技术。课程以精选的具有良好代表性的经典、实用密码算法为对象，力争从工程应用的角度把密码学基本原理讲清楚、讲透彻，并深入分析它们在不同典型领域中的应用方法，以此推动“学用结合”、“能力与素质并进”。使学生奠定密码学基础，具备密码应用能力，能够基于科学原理，采用适当的工程方法对计算机应用系统的安全问题进行研究，解决面临的复杂问题，支撑毕业要求中的相应指标点。课程目标及能力要求具体如下：

### （一）具体目标

**目标 1：**通过本课程的学习，使学生能够掌握密码学的基本概念、古典密码体制、序列密码体制、对称密码体制和非对称密钥体制、消息摘要算法等基础密码理论及典型算法。

**目标 2：**使学生掌握密码学在密钥管理、密码协议、数字签名、身份认证、电子商务、数字通信和工业网络控制等方面的应用。

**目标 3：**能以工程应用为背景，结合先修课程知识编写加密程序。

**目标 4：**提高学生在实际项目中的分析能力，准确判别信息系统的安全防护能力，以及可能带来的影响。

### （二）课程目标与毕业要求的对应关系

| 毕业要求 | 毕业要求指标点 | 课程目标 | 教学单元 | 评价方式 |
| --- | --- | --- | --- | --- |

| | | | | |
|---|---|---|---|---|
| 1.掌握专业必需的数学、自然科学、工程基础和专业知识，能够用于解决计算机软件开发中的复杂工程问题。 | 指标点 1.3：掌握计算机软件与理论、计算机系统结构、计算机应用技术的基本理论、基本知识和基本技能。 | 目标 1 | 信息安全概述及密码学的基础知识、古典密码体制、分组密码体制、序列密码体制、非对称密码体制、认证理论与技术、身份认证技术、密钥管理技术 | 纸笔考试 |
| 2.能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析系统中的密码安全问题，以获得有效结论。 | 指标点 2.5：能运用密码学基本原理分析实际工程的影响因素，证实解决方案的合理性。 | 目标 2 | 分组密码体制、序列密码体制、非对称密码体制、认证理论与技术、身份认证技术、密钥管理技术 | 纸笔考试<br>平时作业 |
| 5.能够针对计算机应用系统的复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，实现对复杂工程问题的预测与模拟，理解其局限性。 | 指标点 5.3：能够选择和使用适当的密码学原理，解决计算机网络应用过程中遇到的网络安全问题。 | 目标 3 | 实验一：DES 算法的部分实现、实验二：RSA 算法的实现、实验三：消息摘要算法 SHA-1 的实现、实验四：PGP 软件的使用 | 实验 |
| 6.能够基于工程背景知识和技术标准，对计算机应用系统工程进行合理分析，评价系统及其复杂工程问题解决 | 指标点 6.3：能识别和分析计算机应用系统的安全潜在影响；能评价系统失效对社会、健康、 | 目标 4 | 密码学的应用 | 纸笔考试 |

| | | | | |
|---|---|---|---|---|
| 方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。 | 安全、法律以及文化的潜在影响。 | | | |

## 三、教学内容与方法

### （一）教学内容及要求

| 序号 | 教学单元 | 教学内容 | 学习产出要求 | 推荐学时 | 推荐教学方式 | 支撑课程目标 | 备注 |
|---|---|---|---|---|---|---|---|
| 1 | 信息安全概述及密码学的基础知识 | 信息安全的基本概念和问题根源、信息安全模型、密码学的基本概念、密码体制的构成与分类和密码体制的安全性。 | 掌握信息安全的基本概念，理解信息安全的问题根源，了解信息安全模型；了解密码体制的构成与分类和密码体制的安全性。 | 2 | 讲授 | 目标 1 | |
| 2 | 古典密码体制 | 古典密码中的基本运算，古典密码算法：移位密码、仿射密码、维吉尼亚密码和希尔密码等及其安全性分析。 | 了解古典密码中的基本运算，掌握移位密码、仿射密码、维吉尼亚密码和希尔密码等古典密码算法及其安全性分析。 | 2 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 3 | 分组密码体制 | 分组密码的定义、原理，典型分组密码体制 DES、AES、SMS4，分组密码的工作模式。 | 了解分组密码的原理，掌握典型分组密码体制 DES、AES、SMS4，掌握分组密码的工作模式。 | 4 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 4 | 实验一：DES 算法的部分实现 | 实现 DES 算法中 S 盒查找功能。 | 掌握S盒功能的实现原理。 | 2 | 讲授<br>实验 | 目标 1<br>目标 2<br>目标 3 | |

| 序号 | 教学单元 | 教学内容 | 学习产出要求 | 推荐学时 | 推荐教学方式 | 支撑课程目标 | 备注 |
|---|---|---|---|---|---|---|---|
| 5 | 序列密码体制 | 序列密码的概念及模型，线性反馈移位寄存器，常用的序列密码算法。 | 掌握序列密码的概念及模型，熟悉线性反馈移位寄存器，掌握常用的序列密码算法。 | 2 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 6 | 非对称密码体制 | 非对称密码的数学基础，非对称密码体制的原理、设计准则和分类等，典型的非对称密码体制，如 RSA、ElGamal、ECC 算法等，非对称密码算法的比较。 | 了解非对称密码的数学基础，理解 非对称密码体制的工作原理、设计准则和分类等，理解典型的非对称密码体制，如 RSA、ElGamal、ECC 算法等，了解非对称密码算法的比较。 | 4 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 7 | 实验二：RSA 算法的实现 | 使用小素数，实现 RSA 功能。 | 掌握 RSA 算法加密原理。 | 2 | 讲授<br>实验 | 目标 1<br>目标 2<br>目标 3 | |
| 8 | 认证理论与技术 | 散列算法的概念、结构与发展现状，典型的散列算法，如 MD5、SHA-1 等，散列函数的攻击现状，消息认证，数字签名的原理，典型的数字签名方案（如基于 RSA、ElGamal 和 DSA 的签名方案）。 | 了解散列算法的概念、结构与发展现状，掌握典型的散列算法，如 MD5、SHA-1 等，了解散列函数的攻击现状，理解消息认证，掌握数字签名的原理，了解典型的数字签名方案。 | 4 | 讲授 | 目标 1<br>目标 2 | 自主学习 |

| 序号 | 教学单元 | 教学内容 | 学习产出要求 | 推荐学时 | 推荐教学方式 | 支撑课程目标 | 备注 |
|---|---|---|---|---|---|---|---|
| 9 | 身份认证技术 | 认证模型及认证协议，身份认证技术，基于零知识证明的身份认证技术，Kerberos 及 X.509 身份认证技术。 | 了解认证模型及认证协议，掌握身份认证技术，掌握基于零知识证明的身份认证技术，理解 Kerberos 及 X.509 身份认证技术。 | 2 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 10 | 实验三：消息摘要算法 SHA-1 的实现 | 按照标准的要求，用程序实现 SHA-1 算法的填充部分。 | 掌握定长消息摘要计算算法。 | 2 | 讲授<br>实验 | 目标 1<br>目标 2<br>目标 3 | |
| 11 | 密钥管理技术 | 密钥的结构与分类，密钥管理的周期，密钥托管，密钥协商与分配。 | 了解密钥的结构与分类，理解密钥管理的周期，掌握密钥托管，掌握密钥协商与分配。 | 2 | 讲授 | 目标 1<br>目标 2 | 自主学习 |
| 12 | 密码学的应用 | 密码学在电子商务中的应用，密码学在数字通信中的应用，密码学在工业控制中的应用。 | 了解密码学在电子商务、数字通信和工业控制中的应用。 | 2 | 讲授 | 目标 1<br>目标 2<br>目标 4 | |
| 13 | 实验四：PGP 软件的使用 | 掌握 PGP 加密软件的密钥生成及管理。 | 掌握密码软件的实际应用 | 2 | 讲授<br>实验 | 目标 2<br>目标 3 | 自主学习 |

## （二）教学方法

### 1.课堂讲授

（1）采用启发式教学，激发学生主动学习的兴趣，培养学生独立思考、分析问题和解决问题的能力，引导学生主动通过实践和自学获得自己想学到的知识。

（2）在教学内容上，系统讲授密码学基础、古典密码、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、密钥管理以及密码学的新进展；课程从密码学在数

字通信安全、工业网络控制安全以及电子商务支付安全等典型领域，讲授密码学的应用方法和技术。

（3）在教学过程中采用电子教案，多媒体教学与传统板书、教具教学相结合，提高课堂教学信息量，增强教学的直观性。

（4）理论教学与工程实践相结合，引导学生应用数学、自然科学和工程科学的基本原理，采用现代设计方法和手段，解决安全模型建立、加密算法选择领域面临的问题，培养学生解决网络安全问题的思维方法和实践能力。

**2.实验教学**

实验教学是密码学理课程中重要的实践环节，目的是培养学生运用实验方法研究解决网络安全领域数据保护的能力。课程必做实验 4 个，各实验按照实验指导书的要求学生独立完成，并提交实验报告。

鼓励学生结合自己的兴趣进行自主实验。

# 四、考核及成绩评定

## （一）考核内容及成绩构成

| 课程目标 | 考核内容 | 成绩评定方式 | 成绩占总评分比例 | 目标成绩占当次考核比例 | 学生当次考核平均得分 | 目标达成情况计算公式 |
|---|---|---|---|---|---|---|
| 目标 1：通过本课程的学习，使学生能够掌握密码学的基本概念、古典密码体制、序列密码体制、对称密码体制和非对称密钥体制、消息摘要算法等基础密码理论及典型算法。 | 信息安全基本概念和问题根源、信息安全模型、密码体制的分类、古典密码原理及典型算法、分组密码原理及典型算法、序列密码原理及典型算法、非对称密码原理及典型算法、消息摘要原理、身份认证原理。 | 纸笔考试 | 35% | 58.3% | A1 | $\frac{\frac{A_1}{58.3\%}\times 35\%}{35}$ |
| 目标 2：使学生掌握密码学在密钥管理、密码协议、 | 分组密码典型应用、非对称密码典型应用、消息摘要 | 纸笔考试 | 15% | 25% | A2 | $\frac{\frac{A_2}{25\%}\times 15\%+\frac{B_2}{100\%}\times 10\%}{25}$ |

| 课程目标 | 考核内容 | 成绩评定方式 | 成绩占总评分比例 | 目标成绩占当次考核比例 | 学生当次考核平均得分 | 目标达成情况计算公式 |
|---|---|---|---|---|---|---|
| 数字签名、身份认证、电子商务、数字通信和工业网络控制等方面的应用。 | 算法典型应用、认证算法典型应用、密钥管理典型应用。 | | | | | |
| | 分组密码、非对称密码、消息摘要算法、认证算法、密钥管理技术应用分析。 | 平时作业 | 10% | 100% | B2 | |
| 目标 3：能以工程应用为背景，结合先修课程知识编写加密程序。 | DES 算法、RSA 算法、SHA-1 算法编程，PGP 软件使用。 | 实验 | 30% | 100% | A3 | $\frac{\frac{A_3}{100\%}\times 30\%}{30}$ |
| 目标 4：提高学生在实际项目中的分析能力，准确判别信息系统的安全防护能力，以及可能带来的影响。 | 密码学技术在通信网络、电子商务等领域的选择及应用分析，可能带来的安全影响分析。 | 纸笔考试 | 10% | 16.7% | A4 | $\frac{\frac{A_4}{16.7\%}\times 10\%}{10}$ |
| 总评成绩（100%）= 平时作业（10%）+实验（30%）+纸笔考试（60%） | | | 100% | —— | —— | $\frac{\text{学生总评平均分}}{100}$ |

## （二）平时考核成绩评定

**1.平时作业：**平时作业 2 次，支持目标 1、目标 2，共占总评分 10%，目标 1 占 60%、目标 2 占 40%。对应目标评分标准如下：

| | | |
|---|---|---|
| **对应目标** | 目标 1：通过本课程的学习，使学生能够掌握密码学的基本概念、古典密码体制、序列密码体制、对称密码体制和非对称密钥体制、消息摘要算法等基础密码理论及典型算法。 | 目标 2：使学生掌握密码学在密钥管理、密码协议、数字签名、身份认证、电子商务、数字通信和工业网络控制等方面的应用。 |
| **考查点** | 分组密码、非对称密码应用分析。 | 消息摘要算法、认证算法、密钥管理技术应用分析。 |

| | | | |
|---|---|---|---|
| **总评分占比** | | 50% | 50% |
| **评分标准** | **100%至90%** | 分析案例选择合理，密码技术应用原理分析透彻，语言描述准确通畅，符合规范。 | 分析案例选择合理，密码技术应用原理分析透彻，语言描述准确通畅，符合规范。 |
| | **89.9%至80%** | 分析案例选择合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。 | 分析案例选择合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。 |
| | **79.9至70%** | 分析案例选择较为合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。 | 分析案例选择较为合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。 |
| | **69.9%至60%** | 分析案例选择较为合理，密码技术应用原理分析较为恰当，语言描述较为准确通畅，基本符合规范。 | 分析案例选择较为合理，密码技术应用原理分析较为恰当，语言描述较为准确通畅，基本符合规范。 |
| | **59.9%至0** | 分析案例选择不恰当，密码技术应用原理分析错误，语言描述错误较多，多处不符合规范。 | 分析案例选择不恰当，密码技术应用原理分析错误，语言描述错误较多，多处不符合规范。 |

**2.实验：**实验 4 次，支持目标 1、目标 3，共占总评分 30%，目标 1 占 50%、目标 3 占 50%。对应目标评分标准如下：

| | | | |
|---|---|---|---|
| **对应目标** | | 目标 1：通过本课程的学习，使学生能够掌握密码学的基本概念、古典密码体制、序列密码体制、对称密码体制和非对称密钥体制、消息摘要算法等基础密码理论及典型算法。 | 目标 3：能以工程应用为背景，结合先修课程知识编写加密程序。 |
| **考查点** | | 实验内容 | 实验报告 |
| **总评分占比** | | 50% | 50% |
| **评分标准** | **100%至90%** | 编程实现加密功能，代码简洁高效。 | 有很强的总结实验和撰写报告的能力，实验报告内容完整、正确，有很好的分析与见解。文本表述清晰，书写工整，格式规范。 |
| | **89.9%至** | 编程实现加密功能，代码较为高效。 | 有较强的总结实验和撰写报告的能力，实验报告内容完整、正确，有较好的分 |

| | | | |
|---|---|---|---|
| | **80%** | | 析与见解。文本表述较为清晰，书写比较工整，格式规范。 |
| | **79.9至70%** | 编程实现加密功能，代码较乱、效率较低。 | 有良好的总结实验和撰写报告的能力，实验报告内容较完整、正确，有自己的分析与见解。文本表述较为清晰，书写较为工整，格式较为规范。 |
| | **69.9%至60%** | 编程实现加密功能，代码有逻辑漏洞。 | 有一定的总结实验和撰写报告的能力，实验报告内容基本完整、正确，没有分析或见解。文本表述基本清晰，书写基本工整，格式基本规范。 |
| | **59.9%至0** | 未编程实现加密功能。 | 总结实验和撰写报告的能力差，实验报告内容不完整、错误多。文本表述不清晰，书写潦草、格式不规范。 |

## 五、参考学习资料

**（一）推荐教材：**吴世忠，祝世雄，张文政等译. 应用密码学：协议、算法与 C 源程序. 北京：机械工业出版社，2014.

**（二）参考资料：**杨波. 现代密码学（第四版）. 北京：清华大学出版社，2017.

**（三）在线资源：**《密码学基础》http://www.icourse163.org/course/XIYOU-1206460819

制订人： 刘金源　　审核人：