河南中医药大学课堂教学设计

授课章节	第 07 章：网络安全（1）		授课学时	2 学时
所属课程	计算机网络原理	授课年级	2023 级	
设计者	计算机网络原理教学团队	授课专业	计算机大类、信管、智医	

1.教学目标：含知识、技能（能力）、学习态度与价值观（情感）目标

知识目标：

1. 了解网络安全的定义；
2. 掌握两类密码体制工作原理。

能力目标：

1. 综合运用能力；
2. 推导分析能力。

素质目标：

1. 提升学生对网络安全的了解，增强学生对网络安全学习兴趣；
2. 提升学生将理论知识运用到实际生活的能力。

思政目标：

1. 信息安全与社会责任；
   信息泄露不仅会给个人带来损失，还可能给整个社会带来不良影响。比如，一些黑客攻击事件可能会破坏国家安全、经济发展等方面。因此，保护信息安全不仅是个人的责任，也是每个人的社会责任。通过引导学生思考信息安全与社会责任的关系，可以增强他们的社会责任感和使命感。
2. 密码学与文化传承。

2.教学内容：依据教学大纲；含教学重点难点

教学重点：

1. 两类密码体制；
2. 密钥分配。

教学难点：

1. 两类密码体制；
2. 密钥分配。

课堂教学内容：

1. 网络安全问题概述

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全涉及的问题主要有病毒问题、非法访问和破坏、管理漏洞以及网络的缺陷及漏洞等。网络安全的目标主要是保证网络系统的可靠性、可用性、保密性、完整性、抗抵赖性和可控性等方面。

（1）计算机网络面临的安全性威胁（10 分钟）

计算机网络主要面临四种威胁，包括截获、中断、篡改和伪造。其中，截获信息的攻击称为被动攻击，而中断、篡改和伪造信息的攻击称为主动攻击。此外，恶意程序也是一种特殊的主动攻击，包括计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹等。

（2）安全的计算机网络（10 分钟）

一个安全的计算机网络应该能够保护其硬件、软件和数据资源，不因偶然或恶意的原因遭到破坏、更改、泄露。这需要采取一系列的安全措施，如数据加密、访问控制、防火墙、入侵检测等，以确保网络系统的连续可靠运行和网络服务的正常有序。

（3）数据加密模型（5 分钟）

数据加密模型是一种保护数据安全的方法，它通过对数据进行加密，使得即使数据被截获，也无法获取到真实的信息。数据加密模型通常包括四个步骤：发送明文、加密、防止截获和解密。在加密过程中，需要使用加密算法和加密密钥将明文转换为密文，而在解密过程中，需要使用解密算法和解密密钥将密文还原为明文。加密密钥和解密密钥可以是相同的，也可以是不同的，这取决于所使用的加密算法。

2. 两类密码体制

（1）对称密钥密码体制（20 分钟）

对称密钥密码体制，也称为私钥密码体制，是一种传统密码体制。在对称加密系统中，加密和解密采用相同的密钥。因为加解密密钥相同，需要通信的双方必须选择和保存他们共同的密钥，各方必须信任对方不会将密钥泄密出去，这样就可以实现数据的机密性和完整性。对称密码体制的优点是计算开销小，加密速度快，是用于信息加密的主要算法。然而，它也存在一些缺点，例如对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了问题。此外，对称加密系统仅能用于对数据进行加解密处理，提供数据的机密性，不能用于数字签名。

（2）公钥密码体制（20 分钟）

公钥密码体制则是一种更为现代的密码体制。在公钥密码体制中，加密和解密使用不同的密钥，即公钥和私钥。公钥是公开的，而私钥是保密的。公钥用于加密数据，而私钥用于解密数据。公钥密码体制的优点是交换密钥容易，可以实现数字签名，具有更高的安全性。然而，它的加密速度相对较慢，计算开销较大。

3. 鉴别

（1）报文鉴别（10 分钟）

报文鉴别是对所接收的报文进行验证，以确认其真实性和完整性。这包括验证报文是否确实来自声称的发送者，以及报文在传输过程中是否被篡改。报文鉴别通常通过使用密码散列函数（如 MD5、SHA-1 等）或数字签名来实现。密码散列函数将报文作为输入，并生成一个固定长度的散列值。如果报文在传输过程中被篡改，那么接收方计算出的散列值将与发送方提供的散列值不匹配，从而可以检测出篡改。数字签名则是一种更强大的报文鉴别机制，它使用发送方的私钥对报文进行加密生成签名，接收方可以使用发送方的公钥进行解密验证签名。这样，只有拥有私钥的发送方才能生成有效的签名，而任何拥有公钥的人都可以验证签名的真实性。

课堂教学内容：

（2）实体鉴别（5 分钟）

实体鉴别则是对通信的对方实体进行验证，以确认其身份的真实性。实体可以是一个人，也可以是一个进程或服务器。实体鉴别通常通过共享对称密钥或公钥证书来实现。

在对称密钥实体鉴别中，双方共享一个对称密钥，并使用该密钥对报文进行加密和解密。只有知道该密钥的实体才能生成有效的加密报文，从而证明其身份。

在公钥证书实体鉴别中，每个实体都拥有一个公钥和一个由可信第三方（如证书颁发机构）签名的证书。证书包含了实体的公钥和其他身份信息。当一个实体想要与另一个实体通信时，它会首先验证对方的证书是否由可信第三方签名，并检查证书中的公钥是否与用于加密报文的公钥匹配。这样，就可以确保与正确的实体进行通信。

3.思政知识点：

课程思政案例	思政点映射
密码学是一门古老的学科，其历史可以追溯到几千年前的埃及、希腊等地。在密码学的发展过程中，涉及到了很多文化的传承和交流。比如，凯撒密码就是一种古罗马时期的加密算法，而维吉尼亚密码则是由英国女王伊丽莎白一世的密室谋杀案启发而来。通过引导学生了解密码学的历史和文化背景，可以帮助他们更好地理解和传承人类的文化遗产。	密码学是信息安全领域的重要分支，对于保护信息安全具有重要意义。通过引导学生学习密码学知识，可以增强他们的信息安全意识，提高他们防范网络攻击、保护个人和组织信息安全的能力。

4.学情分析及教学预测：

学生的知识基础：

1. 计算机文化基础。

学生的认知特点：

1. 对网络安全感兴趣；
2. 对网络安全机制不太了解。

学生的学习风格：

1. 学生对密码学的历史和文化背景表现出浓厚的兴趣，积极参与课堂讨论，主动提问，展现出对知识的渴望和好奇心；
2. 学生对密码体制有一定的了解，有着继续深入学习的兴趣。

教学预测：

1. 对网络加密、网络安全感兴趣，学生学习积极性比较高；
2. 当讲到报文鉴别和实体鉴别的工作原理时，由于原理往往比较抽象，学生缺乏学习的兴趣和动力。

5.教学策略与方法：

教学策略：

1. 结合现实生活、古代虎符、近现代军事信息破获，理解常见的网络安全防护机制；
2. 利用 PPT 讲解访问控制、加密等工具。

教学方法：

1. 案例式教学法：可以通过实例引导学生学习和理解密码体制的基本原理；
2. 合作学习法：鼓励学生参与到小组讨论、增强合作意识，提高团队协作和问题解决能力。

6.板书设计：

① 黑板（白板）设计：	② 现代信息媒体设计：
网络安全 两大类威胁　四个目标 密钥 对称密钥密码体制 公钥密码体制	（1）使用 PPT《计算机网络原理-第 7 章：网络安全》进行讲解。 （2）使用课堂派上传课件、教学设计，发布预习任务。 （3）使用课堂派发布作业、并批改反馈

7.教学互动环节设计：

课堂上的提问和互动交流：

1. 你平时生活中都会遇到哪些网络安全问题，如何应对？（教师提问，点名回答，教师讲解）
2. 对称密钥密码体制与公钥密码体制的区别？（教师提问，集体回答，教师讲解）

8.学习资源，课外自主学习设计：

自建学习资源：

1. 课程学习平台：https://internet.hactcm.edu.cn
2. 课堂派：https://www.ketangpai.com

网络学习资源：

1. 教材网站：http://network.book.51xueweb.cn/resource.html
2. 教材网站：https://internet.hactcm.edu.cn/security/

9.教学测量与评价：

课堂教学测量评价：

1. 课堂测试：使用课堂派开展阶段性测试；
2. 课堂提问：通过提问及利用课堂派与学生互动，及时了解学生知识点掌握情况。

课外学习测量评价：

1. 课前预习：通过课程学习平台开展预习；
2. 课后作业：通过课堂派布置作业，每个章节 1 个作业，内容见课堂派。

10.教学反思与改进：（授课后教师总结）

11.授课教师认为尚未包含在内的设计内容：（授课后教师总结）