项目三 电子商务安全环境

模块 1）电子商务安全技术环境

子模块② 电子商务数据保密技术

课堂教学设计

(2 学时)

一、学情分析

本次课主要面向市场营销专业学生，为了更好地了解学生的学习基础，在正式课堂教学前课程组利用教学 APP，有针对性的开展了问卷调查。调查结果表明：

1、理论基础薄弱。市场营销专业学生普遍是文科背景，这导致学生们的数学知识储备不足，对需要较严密逻辑思维能力的知识点容易产生注意力不够集中的情况。由于高中阶段形成的“数学不好”的自我认识，往往对涉及到一定数理知识的学习内容容易产生畏难情绪， 甚至一听到就自叹学不了。

2、信息化接受程度高。同学们普遍拥有至少一台互联网访问设备，通过网络进行信息搜索的能力较强，对于课堂上能介绍的新型应用工具兴趣浓厚 ，尤其是学生们之前从来没有接触过的软件，或者是与专业相关的有价值的信息源有较强的自己动手操作探索的兴趣，这为课程的信息化教学提供了良好的基础，但也不能忽视由于学习自律性不够，一旦离开了教师的监督，就开始做与学习无关的活动，如打游戏、浏览购物网站、与他人进行网络聊天等。面对网络良莠不齐的多元化信息，学生对于信息的辨识能力尚不足，容易在课堂中执行错误的操作。

3、自我学习要求较低。尽管学生对感兴趣的事物有较高的热情，但热情维持时间不够，对问题的学习往往停留在“老师要求”的层面，如仅仅完成课程学习“报告”，而不在乎提高“报告”的质量，甚至习惯性通过网络搜索相关内容，直接复制粘贴而成。对知识点的学习缺乏深度的理解和思考。对于课程相关的前测、预习、课堂练习、课后检测也常常抱着“六十分万岁”的心态。

鉴于以上分析，本课程在进行教学内容安排时充分的考虑到了知识的难易程度及各知识点之间的逻辑关系、采用制定尽可能详细可操作的学习目标、多样化的教学方法及活动过程紧密联系的教学设计来力图突出“学生为中心”的地位，增加学生动手动脑的机会，引导学生自行思考探索，实现最终教学目标。

二、教学内容分析

《电子商务安全技术》的课程内容是各类电子商务教材中的重要内容之一，其主要包

括：电子商务安全概述、数据加解密技术、数字签名、数字时间戳、数字信封、安全 SSL 协议、安全电子交易 SET 协议等，其中数据加解密技术是网络安全协议及数字签名等认证技术实现的前提，因此数据加解密技术是电子商务安全技术中最为基础的内容之一。

在高职计算机专业或传统工科院校，常常开设《计算机网络安全》、《密码学》等专门的课程来详细介绍该知识点，更注重理论学习。但为了突出本课程管理类专业的设置背景，区别于理工科专业课程的教学体系，结合本课程选用的“十三五规划教材”， 采用了理论够用为度，实训内容为辅，以突出对高职学生基本理论、技能和技术应用能力培养的总体教学内容选择思路。具体内容确定过程中，重点考虑了以下两方面问题：

1、以基础性内容为切入点。密码算法的安全是随着计算机网络安全性不断提升的，新的安全技术和方法不断出现，但各种加解密技术的机密性要求本质并未改变，如果一味追求课程内容的全面性，必然会致使课程重点难以突出。因此，课程组通过追根溯源，在课程内容的选择中以基础性知识点为首选，力求让学生快速抓住网络安全中信息保密性要求的本质。此外，由于当前的网络信息安全技术很大程度上依赖于数据的运算量，涉及到诸如数论、欧拉函数、模运算等数学知识，这些学习内容在高职学校，尤其是经管类专业学生中几乎没有接触过，而以凯撒密码为代表的古典密码只涉及到简单的代换、置换的数学思想，以这样的基础性教学内容作为切入点能更好的与高职学生现有的知识储备相结合，以形成学生“有兴趣”、“有自信”并且“有能力”学习的良性循环。

2、以知识应用为落脚点。理工科类电子商务安全课程侧重于数据加解密算法的数理逻辑，往往通过高级语言编程的方式来验证加解密算法，强化对算法的理解，但这一思路不适合文科背景的学生。根据课程设计中对电子商务职业的分析以及安全技术的教学目的，学生只需要掌握“简单的”数据加解密技术即可，更重要的是能够运用诸如防火墙、数字签名、数据备份等技术保障企业电子商务交易安全。不难看出加解密技术是为具体的安全工具使用服务的，因此，课程内容最终应该以是否能实际应用作为甄选落脚点。

鉴于以上分析，课程具体教学内容设计如下表所示：

数据加、解密教学内容		学时
对称密码加密体制	凯撒密码	1
	多表式密码	
	DES 算法	1
非对称密码加密体制	RSA 算法	2

其中，本次课程设计共 2 学时，主要教学内容为“对称密码加密体制”。

三、教学重、难点

数据加解密技术本身是电子商务安全技术中基础性的内容，是其他网络安全技术得以实现的前提，此外各种加解密算法也是通过设计—攻击—再设计的过程，不断地在实践中被提出来的，各算法之间有着较强的联系。因此本次课的重点在于让学生了解并掌握最基本的加解密原理，而难点在于对具体算法过程的理解。

1、重点： 凯撒密码法、多表式密码法

2、难点： DES 算法

针对本次课重点，课中设计了小运算量的密码实训模块，先通过人工手算的方式让学生理解数据加密的流程和原理，再运用 EXCEL 工具让学生们进行解密验证，加深对凯撒密码和多表式密码两种加解密方法应用的理解，突出课程重点。

针对课程难点，其难度在于 DES 算法运算过程更复杂，涉及更多的置换和代换，对数学基础要求更高。为了突破难点，本课采用了现有的免费开源软件，模拟 DES 的运输过程，从而帮助学生更直观的体验到这种加解密算法的运作流程，突破课程难点。

四、教学目标

依据学情、教学内容及重难点分析，结合企业开展电子商务业务活动的基本素质要求，设计教学目标如下：

1、知识目标：

- ✧ 理解对称密码加密体制的一般工作流程
- ✧ 掌握凯撒密码法的原理
- ✧ 掌握多表式密码的原理
- ✧ 理解 DES 的工作原理

2、技能目标：

✧ 能够运用 excel 软件实现简单的凯撒密码加、解密方法

✧ 能够运用 CrypTool 工具实现 DES 数据加解密操作

3、职业素养目标：

✧ 具备基本网络安全意识

✧ 能进行问题分析并思考解决方案

五、教学方法和手段

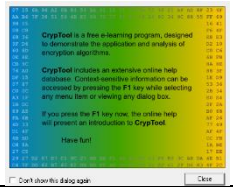
✧ 项目教学法及任务驱动法。将一种加解密算法设计为一个项目，项目内容涵盖一个“加密”的防卫与“解密”的攻击的完成过程。针对每一个项目（即加解密算法），老师首先提供实际的明文信息引导学生先实施加密操作，再布置通过给出解密任务的方式，鼓励学生思考、讨论解密思路，并实施具体的解密操作。

✧ 实验教学法。没有实践的数据加解密算法教学无疑是枯燥的纸上谈兵，能够学以致用的知识更能培养学生的学习兴趣。因此，本次课在理论教学内容的基础之上，针对性的设计了三个加解密实验模块。运用现成的开源软件工具，让学生可以将所学知识应用到实际的网络操作之中，突出学生的主体地位，增强学生参与性与体验性，进一步加深学生对加解密过程的理解，增强学生解决实际问题的能力，实现“技术应用”的教学目标。

✧ 角色模拟法。学生在具体操作一个项目的过程中，一方面从如何能实现将明文信息以“读不懂”的密文形式的“信息防卫者”的角度思考加密方法，另一方面从窃听、篡改、伪装、穷举等“信息攻击者”的角度思考加密方式的漏洞有哪些？对“如何进行攻击”的问题的讨论，让学生们仿佛“网络黑客”，其神秘莫测的形象能够充分调动学生们的学习热情，激发学生们进行更深入探索的学习欲望。

通过以上教学方法的设计，学生能够在“学中做，做中学”的环境中，仔细体会每一种加、解密算法的设计逻辑及具体的实现方式，理解并掌握“加解密算法的工作原理及流程”这一知识重点。自己动手实现加解密的全过程有利于学生形成良好的自我认知，逐步建立克服“算法涉及大量复杂数学运算”这一学习难点的信心。对解密问题的思考也有利于“分析问题、解决问题”培养目标的达成，并形成对电子商务信息的安全环境相对客观

的认识。在课堂教学过程中，除了使用了 PPT 进行理论讲解外，还选用了在线开源软件工具作为辅助手段，具体如下表所示：

序号	教学工具手段	功能和作用
1	PPT、实训任务书	基本知识原理的讲解、布置； 实训任务；
2	新闻视频、加密动画	真实新闻材料进行课程内容导入； 动画播放了解对称加密过程
3	EXCEL	制作编码表、实施凯撒密码和多表式密码； 强化教学重点
4	CrypTool 	实施 DES 算法； 突破课程难点

六、教学过程设计

自古罗马时期，凯撒大帝通过将字母按顺序进行位移来实现信息加密的凯撒密码法诞生以来，人类便迅速投入了对其进行破解的探索。事实上，密码学有着明显的攻防对抗的特点。即在防卫——攻击——再防卫——再攻击的循环中，各种新的加解密算法被设计出来，同时破解的方法也在不断改进。有“加密”的场合，“破解”就如影随形。为了能更好的保障信息的机密性，“破解”也在一定程度上为更优的加密算法提供了算法改进的依据。

基于以上分析，本课程在教学过程中引入了“攻防思维”，分别设计了围绕着加密过程和围绕着解密过程进行的教学主线。分别通过课前、课中、课后三个阶段实施，完成教学目标。

课前，指导学生预习并搭建课堂教学活动所需的计算机环境准备工作。具体包括：提供课堂 PPT 及实训资料，供学生进行简单课前预习，让学生对课程内容有一个大致的了解；统一规范课堂所需的 excel 版本，以避免因版本不同带来的实际操作问题；提供课堂教学中所需的 CrypTool 软件，进行课前软件测试安装。

课中，以每一种加解密技术为一个单独的学习项目，完成具体项目任务，实现最终教

学目标。（具体步骤见下表）

步骤		内容		教学目标	效果检测
		教师活动	学生活动		
1、课程导入（10min）		播放“男子买公民信息，利用公民信息破解资金账户密码”新闻视频； 讨论：请同学们谈谈自己对生活中网络信息安全的认识	观看新闻视频；引导学生讨论生活中的网络信息安全现状、隐患	为网络信息安全性的有初步了解	能从保护个人信息的角度说出密码设置时的一般规则
2、对称加密体制概述（10min）		PPT 讲解明文、密文、密钥、算法的概念； PPT 图示及动画短片介绍对称加密体制一般工作原理	观看 PPT； 观看动画短片；	理解对称加密体制原理	能指出对称密钥加密体制的关键之处
3、凯撒密码教学项目（20min）	加密	PPT 介绍凯撒编码编码表； PPT 演示凯撒密码加密过程； 布置加密任务；	观看 PPT； 并动手进行编码表的制作； 实施加密；	理解凯撒密码的编码原理	能制作编码表； 能利用 excel 完成凯撒密码加解密全过程
	解密	布置解密任务；	讨论并实施解密；		
4、多表式密码教学项目（20min）	加密	PPT 演示多表式密码加密过程； 布置加密任务；	观看 PPT； 实施加密；	理解多表式密码的编码原理	能利用 excel 进行多表式加解密操作
	解密	布置解密任务；	讨论并实施解密；		
5、DES 算法教学项目（20min）		PPT 介绍 DES 算法的工作原理； 使用 CrypTool 软件对 DES 加密	观看 PPT 及 DES 算法具体步骤、实现过	理解 DES 算法的工作原理	能使用 CrypTool 软件实施

	流程进行可视化功能演示	程和结果； 实施加密；		DES 加解密全过程
6、课后总结（10min）			理解并掌握对称加密体制的基本原理； 能运用 3 中加解密算法	能复述 3 种加解密算法的一般流程并用软件实施这一过程

课后，针对本次课并未涉及到的其它对称密码加密体制的具体算法，引导学生利用 CrypTool 工具实施其它加解密算法，开展自主学习。

七、教学反思

职业教育课程设计的重点在于对学习目标、教学内容及其结构、教学手段方法、评价标准的合理制定。

本次课首先从社会热点新闻着手，拉近加解密理论知识与日常生活的距离，让同学们能置身于事件之中，通过对自我信息安全性的考量引发对课程知识的兴趣。运用项目教学、理实一体化及多种教学工具手段与学生进行良好的互动。课后学生们普遍表示该知识点的学习过程比他们预想的容易，对于开源软件工具的操作及结果的可视化呈现有效地帮助学生们掌握了学习重点，突破了数学基础薄弱的难点。

通过项目任务的完成情况进行教学评价。注重加解密知识教授的同时培养学生的数据安全观，形成攻防渗透思维。