题目来源  
密码学的课程是编码学与解密学组成，这是一门研究密码的准备和解码的技术科学。研究密文变化的客观规律，将其应用于密文编码中，以保密通信功能，并运用语言学、数学、电子学、声学、信息论、计算机科学等学科知识研究如何将明文变为密文，根据通信双方约定的规则以及密码准备的原则、方法和妙计进行加密和转换，以确保通信的机密性，称为编码；用于破译密码以获取通信信息的密码称为破译，通常称为密码术。同时，它是一门笼统而复杂的课程，索然无味，学生难以反思。在充分分析学习者需求的基础上，针对如何提高课程的有效性、趣味性和应用性等教学难点，设计并开发了一个交互式密码算法演示系统。密码学中的高级加密标准（AES。本标准用于取代最初的des（数据加密标准）。该标准已被许多方面分析。并在世界各地广泛使用。经过五年的挑选过程；国家标准与技术研究所（NIST）于2001、11、26在FIPS pub 197发布了高级加密标准，并于2002、5、26成为有效标准。2006年，高级加密标准已成为对称密钥加密中最通行的算法之一。

密码学作为信息安全的核心技术和基础，随着网络通信和应用的发展，逐渐从军事领域扩展到人们的生活领域，如Alipay、淘宝、网上银行、电子邮件加密等。所有这些都需要加密编码技术来保护和防御非法入侵。密码学是研究如何保护和抵御非法入侵和攻击的盾牌。作为密码学的另一个模块，密码分析研究如何攻击和破解加密信息。密码分析是侦查敌对势力、提取犯罪信息、防止外国入侵和国内犯罪的利刃。密码学在人们的生活中变得越来越重要。然而，人们的信息安全意识普遍薄弱，信息安全知识相对匮乏，社会对密码人才的需求相对较少。从新世纪开始，我国开始了密码学知识的普及和人才培养，但无论是密码学课堂教学还是密码学自主学习都存在着很大的问题。传统的教学模式和PPT课件无法生动地表达算法内部的抽象逻辑、复杂的数学公式和抽象的学习内容，侵蚀了人们对像淘铁这样的密码学的兴趣和毅力。学习内容多、知识点多、课堂教学时间少等问题困扰着教育者和学习者。在富媒体时代，将传统的多媒体和个性化的交互功能应用于人们的服装、食品、住房和交通等不同领域是人们的追求。针对密码学教学中存在的问题，在前人研究的基础上，结合先进的学习理念，从学习者的角度，将富媒体的特点引入密码学教学中，并将密码学的教学内容转化为可视化、交互式的富媒体表达形式，从而使该动画符合程序教学法循序渐进、易学易学的特点。以AES算法为例，本研究的特点是将算法的教学内容模块化，制作简短、有针对性、跨媒体、交互式的动画演示。该课件实现了密码学教学内容的可视化，具有交互性。它可以辅助学习者和教师的课堂教学活动，丰富自主学习密码学的学习资源和学习形式，使学习者在课堂学习和自主学习中轻松愉快地学习密码学知识。本研究旨在满足社会需求，改进密码学教学模式，促进个人发展，为社会培养应用型人才。该系统解决了现有算法演示系统动态性能差、缺乏实时性等问题[1]。

国内外研究成果及动态

国内的研究首先来自1988年全国计算机辅助教育学会第三届学术年会，以及华东理工学院刘晓燕和张元林编写的具有核心算法的“有趣数学”CAI系统。本文介绍了一个有趣的数学发现、数学游戏和数学知识的学习与实践系统，以及一些竞赛题。除了概念描述之外，系统还提供了验证过程和问题答案。该系统采用高级basica语言编程，并在IBM PC/XT上实现。它可以自动生成一些执行指令和程序的图片和动画演示，这将为提高青少年的学习兴趣和开发智力创造条件。来自吉林大学高等教育学院的黄新平，《AES加密演示系统》在充分分析学习者需求的基础上，针对如何提高理解能力的教学难点，开发了一套密码学课程算法演示系统，课程的兴趣和应用。以AES算法为例，介绍了算法演示过程的动态性、交互性和数据输入的灵活性。该系统解决了现有算法演示系统动态性能差、缺乏交互性、难以创建算法与动画之间的关涉等问题。期待能够在实际应用中，改进了我们的教学方法，帮助大家更好地掌握复杂的密码算法，取得了良好的教学效果。各种原理显示的动画非常常见，加密算法也很少。20世纪90年代，北京邮电大学开始在研究生阶段开设密码学课程。它只在21世纪初为信息工程专业的本科生开设了密码学课程，重点是选修课。直到2004年，它才作为一门必修课出现在信息安全教学中。密码学的教学是课堂讲解.教材和简单的ppt是唯一的教学资源。教材和教材都是各高校翻译的外文文献。清华大学出版社出版的《网络安全基础》由威廉·斯泰林斯撰写，白国强等人翻译，罗斯·哈曼科技公司出版。2007年以来，我国高校密码学教学开始理论与实践并重。高校在传统课堂理论讲解的基础上。结合实验室实验操作，相继开设了密码学实验教学。优秀的信息安全教学实验系统已逐步在高校实验室出现。其中,，上海交通大学“信息安全综合实验系统”（isies）是在863重大信息安全项目“信息安全工程实践综合实验平台研究与集成”的支持下，由上海交通大学和鹏跃公司共同开发的根据科技部“十五”计划，它是中国第一个也是最大的支持信息安全领域信息安全教学和培训的实验系统。同类型还包括中软吉达网络信息安全教学实验系统、西普科技simpleises信息安全实验教学系统和瑞杰公司开发的系统。中国的大多数主要大学都使用了这些实验系统。这是目前一个热门的研究项目。许多外国学校把这种学习资源作为主要的学习方式。通过课外学习，课堂小组讨论进行教学。与传统的教育相比，这种方法强调以学习者为主体，以教育者为学习资源和学习工具，帮助学习者学习的教育理念。

研究基本内容

随着信息安全在我们生活中的广泛应用，密码学专业人才的培养和高校对密码学的教学研究成为了热门。该研究从密码学理论教学和实验教学现状分析，基于密码学教学中存在的问题，针对在校学习密码学的大学二年级和大学三年级将要学习或正在学习的学生进行需求分析，将抽象、不容易理解和学习的 AES算法密码体制和加密、解密过程进行模块化划分，分别制作成可视化、可交互实验操作的动画，为密码学课堂教学和自主学习提供优质的学习资源。(1）根据参考文献、调查问卷、访谈、自身自学密码学体会和网络调查，研究密码学教育的现状，针对学习者和教育者在学和教的工程中遇到的困难和密码学课程自身的特性找到存在问题，结合以学习者为主体的教育理念，宏观把握未来密码学的教育发展趋势，探索教学资源开发方法。(2）根据密码学理论教学和实验教学方式和资源的分析，在前人原有基础上将密码学知识模块化，在多媒体教学、远程教育、网络学习、自主学习和终身学习的教学资源和教学方式多元化的基础上，制定教学资源和开发工具的选取标准。选择有价值教学资源内容:密码学教学过程中不容易讲授，学习者在抽象的内容中难以把握，并且具有极强的代表性的内容，经典的AES加密算法。本文主要研究内容为:

(1）根据参考文献、调查问卷、访谈、自身自学密码学体会和网络调查，研究密码学教育的现状，针对学习者和教育者在学和教的工程中遇到的困难和密码学课程自身的特性找到存在问题，结合以学习者为主体的教育理念，宏观把握未来密码学的教育发展趋势，探索教学资源开发方法。

(2）根据密码学理论教学和实验教学方式和资源的分析，在前人原有基础上将密码学知识模块化，在多媒体教学、远程教育、网络学习、自主学习和终身学习的教学资源和教学方式多元化的基础上，制定教学资源和开发工具的选取标准。

选择有价值教学资源内容:密码学教学过程中不容易讲授，学习者在抽象的内容中难以把握，并且具有极强的代表性的内容，经典的AES加密算法。

选择有效的开发工具:针对理论教学过程中的图文并茂结合实验教学中算法内部特点体制和逻辑，拥有强大的交互功能，这种浏览器非常合适。通过多种多媒体资源开发软件的对比，使用javascirp制作界面和，使用开源的引擎算法动画演示，用网页实现算法内部逻辑的联系和人机交互，用python库函数算法结果进行抽样验证。

研究关键创新点

使用网页开发，主要使用movy.js动画引擎。在之前的演示动画研究中，研究者主要使用flash来制造动画，但随着adobe公司停止了flash的更新，以及各种浏览器停止了flash的支持，导致flash的制作与展示都不方便。随着html5的发展，浏览器的性能更加强劲。HTML5 是 **HyperText Markup Language 5 的缩写，HTML5**技术结合了 HTML4.01 的相关标准并革新，符合现代网络发展要求，在 2008 年正式发布。HTML5 由不同的技术构成，其在互联网中得到了非常广泛的应用，提供更多增强网络应用的标准机。与传统的技术相比，HTML5 的语法特征更加明显，并且结合了 SVG 的内容。这些内容在网页中使用可以更加便捷地处理多媒体内容，而且 HTML5中还结合了其他元素，对原有的功能进行调整和修改，进行标准化工作。HTML5 在 2012 年已形成了稳定的版本。所以使用基于h5和JavaScript的网页动画设计JavaScript是基于对象和事件驱动的一门具有强大功能 的脚本语言。在高校计算机教学课程体系中，JavaScript课程 起着承上启下的作用，课程的教学内容除了基础的语法外， 还包括各种对象的应用以及利用文档对象模型（DOM）来存 取、遍历和控制HTML和XML文档等内容。因此如果在知识 点分散、教学内容覆盖面广的前提下，解决实操重点难点，同 时兼顾理论知识结构的系统性和完整性，就成为JavaScript 教学过程中的重点需要解决的问题，加之语法类课程本身枯 燥、抽象，如何解决这些问题，就显得迫在眉睫。项目设计原则遵循自下而上、由易到难、逐步完善，将融入了

JavaScript（简称“JS”） 是一种具有函数优先的轻量级，解释型或即时编译型的编程语言。虽然它是作为开发Web页面的脚本语言而出名，但是它也被用到了很多非浏览器环境中，JavaScript 基于原型编程、多范式的动态脚本语言，并且支持面向对象、命令式、声明式、函数式编程范式JavaScript多方面的技术包含：JavaScript语 言基础、JavaScript面向对象编程、界面编程、绘图技术、多 个独立定时器协同工作的编程思想等。这些都是 JavaScript语言的精髓，而又往往通过课本无法体会和学习 的部分。而随着服务器的强壮，虽然程序员更喜欢运行于服务端的脚本以保证安全，但JavaScript仍然以其跨平台、容易上手等优势大行其道。同时，有些特殊功能（如AJAX）必须依赖JavaScript在客户端进行支持。

movy.js：

相信大家都看过3B1B的科普视频一定会被其中的精妙展示给打动，3B1B使用的是自己的动画引擎，该项目为了通用性选择用开源的引擎来制作视频。快速开发，不用再考虑公共问题，专心在业务实现上，结构统一，易于学习、维护，新手也可写出好程序 。引擎技术是一个应用程序的半成品，提供可重用的公共结构，按一定规则组织的一组组件，不用再考虑公共问题，专心在业务实现上  
结构统一，易于学习、维护新手也可做出好的动画。这个项目来自于github上面的开源框架。

参考文献

[1]郭海峰. 基于富媒体的密码学教学内容可视化研究与实现[D].四川师范大学,2014.

[2]黄新平.密码学课程交互式算法演示系统的开发与应用[J].软件,2013,34(06):8-12.

[3]马景艳.用软件工程的方法实现加密演示系统[J].科学管理研究,2004(S1):67-68.DOI:10.19445/j.cnki.15-1103/g3.2004.s1.028.

[4]冯诚,石彦君,蒋黎明. 一种用于交互式网页动画的推演设备[P]. 河北省：CN215000471U,2021-12-03.

[5]刘红英.Web开发中HTML5技术的应用[J].信息与电脑(理论版),2017(05):63-65.

[6]谭文文,丁世勇,李桂英.基于webGL和HTML5的网页3D动画的设计与实现[J].电脑知识与技术,2011,7(28):6981-6983.

[7]朱倩.JavaScript在HTML5视频和音频控制中的应用[J].无线互联科技,2021,18(18):89-91.