文献综述

1、**前言**

密码学的课程是密码学。这是一门研究密码的准备和解码的技术科学。研究密码变化的客观规律，将其应用于密码编码中，以保密通信，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、方法和技术手段进行加密和转换，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，它是一门抽象而复杂的课程。枯燥乏味，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加密算法演示系统。密码学中的高级加密标准（AES），也称为Rijndael加密方法，是美国联邦政府采用的块加密标准。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。经过五年的严格筛选，正式于 高级加密标准（AES）是美国政府为保护机密信息而选择的对称分组密码。

AES在世界各地的软件和硬件中实现，用于加密敏感数据。这对政府计算机安全、网络安全和电子数据保护至关重要。美国国家标准与技术研究所（NIST）于1997年开始开发AES，当时它宣布需要替代数据加密标准（DES），DES开始变得容易受到暴力攻击。NIST表示，更新的高级加密算法将是不保密的，必须“能够在世纪保护敏感的政府信息”它旨在易于在硬件和软件以及受限环境（如智能卡）中实现，并针对各种攻击技术提供良好的防御。AES是为美国政府创建的，它在提供加密服务的公共或私人、商业或非商业程序中提供额外的自愿、免费使用。然而，选择使用AES的非政府组织受到美国政府的限制。高级加密技术标准问题已成为对称密钥加密系统中最流行的算法研究之一。

密码学作为信息安全的核心技术和基础作为密码学的另一个模块，随着网络通信和应用的发展与应用，逐渐从军事领域扩展到人们的生活领域。密码学的另一个模块，密码进行分析问题研究企业如何攻击和破解加密技术信息。密

2**、国内外研究现状**

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算法演示系统》在充分分析学习者需求的基础上，针对如何提高有效性的教学难点，设计开发了一套密码学课程交互式算法演示系统，课程的兴趣和应用。以AES算法为例.介绍了算法进行演示教学过程的动态性。该系统解决了现有算法演示系统动态性能差、缺乏交互性、难以建立算法与动画之间的关联等问题。在实际应用中，改进了教师的教学方法，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。交互性和数据信息输入的灵活性。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。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。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。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。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，我国企业开始了密码学知识的普及和人才进行培养。但无论是密码学课堂教育教学方法还是密码学自主合作学习都存在着一个很大的问题。传统的教学模式和PPT课件无法生动地表达算法内部的笼统的逻辑。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。学习内容过多、知识过多、课堂教学时间过短是困扰教育者和学习者的问题。在互联网时代，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，将互联网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、交互式的互联网表达形式，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。它可以进行辅助学习者和教师的课堂教育教学实践活动，丰富学生自主合作学习密码学的学习环境资源和学习内容形式，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。本研究旨在适应社会的需要，改进密码学的教学模式，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。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、中国的大多数主要大学都使用了这些实验系统。对于自主学习和在线学习，国外有很多值得学习的教学模式，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，通过课外学习和课堂小组讨论进行教学。与传统教育相比，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。

3**、正文**

计算机科学教学越来越依赖于动画作为一种方式来解决复杂性和动态性质的许多核心课题。它还提供了一种激励动力，并为学生提供了更大的自主权。推动动画研究的教育关注也塑造了互动模式，这种模式的使用要求并限制了动画的应用;这些系统设计中的一个主要问题是确保元工具保持准确性，并以透明的方式促进对主题的理解。算法动画一直是备受关注的主题，各种系统被提出并对其影响进行了评估。在这种情况下，学习内容不仅仅是看书，它允许学习者在数据被转换为时控制和跟随算法的动态展开。

这一领域的研究是由一种信念驱动的，即算法动画可以是一种比仅仅基于文本的静态资源更有效的教学手段。

人们也越来越意识到，所谓的新一代的出现正在影响着课件材料的传播。正在大力提倡与多媒体环境的普遍性质有更大亲和力的交互方式。

这些操作模式被认为比基于文本的方法有更大的激励力量，并促进以学生为中心的学习。从一般的模拟和动画的交互中获得的好处是验证和完善的基础研究对象的概念模型。

在综合考察后决定使用使用网页为基本平台开发该系统，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，能够满足加密与动画渲染的要求，而且h5的使用人数在急剧增加所以h5的资源更加丰富。

**4、总结与展望**

一些AES动画的评价在交互程度、抽象粒度和学习者沉重的认知负荷等方面突出不足。除了CrypTool的相对例外，操作框架是静态的，而数据是动态修改的。相比之下，本文中提出的AES工具展示了操作框架和数据的动态特性。学习者能够与诸如排列表之类的独立成分进行互动。它还在不同的抽象级别上提供了高度的交互性。该动画增强了算法的动态展开，适用于加密。然而，操作框架的更多静态方法在许多应用程序中更合适。本文中描述的AES动画满足了具有足够教学价值的工具所需的大多数标准。它的重要性通过它与正式模型的相关性、它符合良好的人机交互原则以及它与实证研究得出的良好实践的一致性得到了证实。这涵盖了学习者在课堂之外直接与动画互动的能力，以及在元工具的最小干扰下专注于算法的逻辑步骤的能力。它还意味着文本和动画的有意义的集成，并明确表示加密过程在任何阶段的状态。算法和动画之间的映射也增强了它的相关性。所有这些特性赋予DES动画内在的教学价值。**4、参考文献**

[1]王歌，上海浦东发展银行长春分行资产业务风险管理案例研究[D],吉林,吉林大学，2020年

[2]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.

[3]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.

[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.