基于 Internet 的密码学虚拟实验室的设计与实现

A Internet – Based Simulation System for Cryptology

杨路明 郭 璠 段桂华 （中南大学 信息科学与工程学院 湖南长沙 410083）

摘要：本文提出了一种采用组件技术构架的基于 Internet 的密码学虚拟实验室的设计模型和实现方法。该虚拟实验室以 Java Applet 实现客户端，具有 Java 语言的平台独立性和安全性，以 JavaBeans 的形式开发组件，提高了系统的开发效率，实现了软件重用，使得系统容易维护和扩充。利用该实验系统，用户能进行可视化的实验流程定制、仿真实验保存，对算法进行验证和性能分析实验，用户还可以加入自己编写的算法进行验证及扩充实验组件，为科研、教学等提供了一个很好的密码学虚拟平台。

关键词：密码学 虚拟实验室 组件

1 引言

密码技术是实现网络信息安全的核心技术，是保护数据最重要工具之一[1]。随着计算机和通信技术的迅猛发展，密码学广泛应用于日常生活中，如银行账号、个人隐私等。密码学往往涉及到复杂抽象的算法，而且完成一项密码学的仿真实验通常需要多个模块的协同工作。本文提出的基于组件的密码学虚拟实验室系统把每个密码学相关算法封装成一个组件（JavaBean），用户可以通过选择需要的组件来构建实验流程，从而完成复杂的算法仿真。本系统能够为密码学习和研究的人员提供检验、调试算法的实验平台，大大减轻了研究人员开发重复算法的工作量。该虚拟实验室系统还为学生提供了学习密码学课程的实验环境，学生可以完成与密码编码与分析相关的各种实验，还能按照自己的需要根据该课程的要求组合相应的实验，定制自己的实验过程，加入自己编写的算法进行验证及扩充实验组件。平台的交互界面良好，可实现可视化的实验流程的动态定制，从而进行仿真实验。

本文的第二部分介绍国内外相关的研究工作，第三部分描述系统功能和整体的设计，第四部分描述密码学相关组件的设计与实现，第五部分是结论。

2 国内外相关工作

虚拟实验室环境是目前研究的热点问题之一。文献[2]中介绍了远程编程虚拟实验室的设计，客户端采用 Java Applet，服务器端采用 CGI、Java Servlet，客户端把程序代码以文本的方式发送给服务器，服务器调用相应的语言编译器编译执行，再将结果返回客户端；在文献[3]中提出的 IP 网络虚拟实验室是以一台 Ethernet Switch 和多台运行 Linux 操作系统的 PC 机作为仿真设备，用户可以在 Web 上远程输入 Linux 网络操作命令，服务器端将仿真设备的结果返回给用户；在文献[4]提出的残疾人虚拟实验室中，用户界面采用了 Macromedia 出品的 Authorware 多媒体创作软件来开发用户界面，用 LabView 软件来接受某些真实设备的输入数据来完成模拟过程，同时可以采用 LabView 本身的“G”编程语言来编程实现用户需要的虚拟设备。

组件技术可以有效提高系统的重用性，减少应用开发的工作量，便于系统的升级和扩充。文献[5]从分布离散事件仿真的特点出发，结合基于组件的软件设计思想，建立了仿真组件模型规范，提出了一种分布仿真算法，并开发了相应的仿真环境。

基于 Internet 的密码学虚拟系统主要包括数论基础、算法验证、密码攻击、算法设计等方面。在算法验证方面，国内某些高校已采用 Delphi 开发了密码学的

实验平台，用户可以在该平台上从给定的加密、解密算法中选择一种进行验证。但是这个平台的实验流程仅仅为：先用户输入参数（如明文、密钥），然后选择算法，最后就是结果输出。由此可见，这一平台并没有从学习密码算法的用户角度出发给出直观的加密、解密过程，而且缺乏交互性。

在为密码学提供研究和实验的工具和环境方面，文献[6]中提出的基于 Internet 虚拟实验室是以 Java 语言开发实现的，客户端用 Java Applet 实现，设备组件用 JavaBean 实现。该实验室以组件的方式提供具体的仪器设备，用户可以可视化地制定自己的实验流程，动态地引入、创建实验设备对象。

能够较好应用于教学和科研的仿真系统应具备以下特点：(1) 系统开发的高效率与正确性；(2) 系统具备互联网访问能力，并具有平台独立性；(3) 系统具有良好的用户交互性；(4) 具有较好的可扩充性。

3　系统整体设计

基于 Internet 的密码学虚拟实验室主要由服务器端和客户端组成，系统体系结构如图 1 所示。服务器端主要包括提供 Internet 访问功能的 Web Server。客户端采用浏览器中嵌入 Java Applet 的方式，使得仿真系统的客户端具有 Java 语言的平台独立性、安全性等特点。

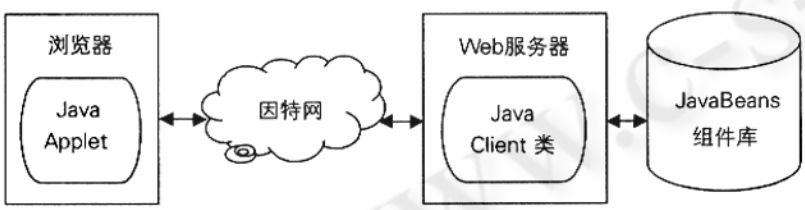

图 1　系统体系结构图

服务器端主要包括提供 Internet 访问功能的 Web Server，用户通过客户端提供的接口向 Web 服务器提交新的算法组件，经过系统测试后加入该算法组件，以备其他用户使用。通过这种方式，大大增强了系统的适用性和可扩充性。

客户端采用面向对象的设计方法和组件技术实现虚拟设备，包含了 Java Bean 容器和大量 Java Bean 组件，每个算法组件完成服务对象的获取和方法调用。系统提供了各种大量的密码学算法组件，这些组件有 2 种类型：一种是通过引用服务器端组件对象，其运算在服务器端完成；另一种直接在客户端运行。客户端提供菜单栏、工具条、设备属性编辑栏、实验操作窗口、组件栏等，用户可以选取需要的算法组件，修改组件输入参数，通过匹配组件之间的接口连接成需要的密码学实验组件流程图，运行该流程来完成仿真试验。同时，仿真系统的客户端还允许用户加入自己编写的算法组件来完成新的图像处理算法的调试、检验和对比。仿真过程如图 2 所示。

密码学虚拟实验室系统由实验流程设计模块、实验运行模块和算法提交模块组成。在实验流程设计模块中，用户可以对每个组件的属性设置，可以通过鼠标和键盘自由选择算法组件，建立组件之间的连线来进行可视化的实验流程构建；实验运行模块负责运行用户定制的实验流程，进行仿真实验的运行，输出实验结果；算法提交模块可以将本地的 Java Bean 算法组件添加到实验室中，当用户使用自己编写的组件来进行实验时，可以验证该组件，扩充实验室的功能。

密码学原理与相关应用实验中涉及的算法非常多[7]，将它们进行汇总分类，主要涉及到的有以下四类实验：数论基础实验、算法验证实验、密码攻击实验、设计型实验，学生除了可以进行可视化的实验流程定制，完成对已有的算法的验证，还可以自己设计各种密码系统和密码分析算法，以分析密钥长度、明文分组长度、初始向量、迭代次数等对算法性能的影响。

4　组件的设计与实现

对于密码学虚拟实验室所涉及的数论基础实验、算法验证实验、密码攻击实验、设计型实验这四类实验，我们分别开发了相应的各种组件。例如围绕数论基础实验开发了指数运算、乘法逆元、离散对数、求模运算、素性检测、欧几里得等算法组件，用户可以在理解加密算法或协议的原理后选择所需的数论组件进行其它实验的操作，体现了较好的重用性[8]。又

如围绕算法验证实验开发了对称密码(DES、AES 等)和非对称密码(RSA、ELGamal 等)算法组件。

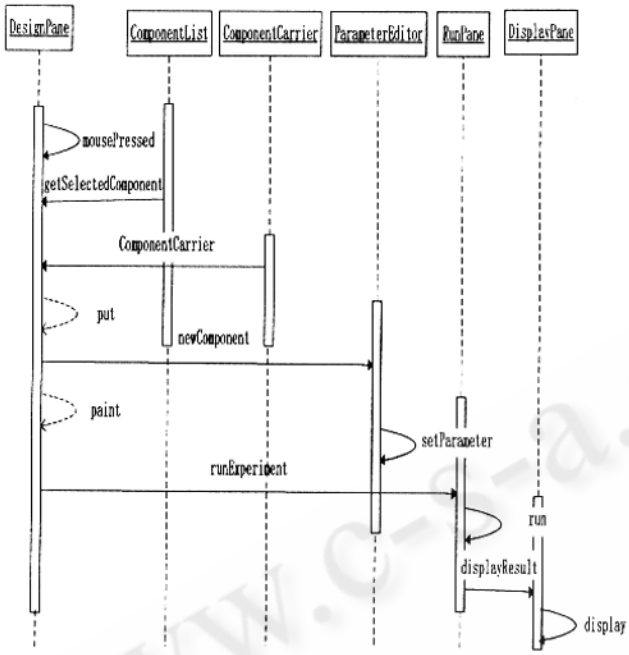

图 2　仿真过程序列图

自动检验组件数据接口和类自定义的方法是否匹配，只有相匹配的接口和方法才能连接构成实验流程，实现组件的功能，完成实验的内容。

密码学虚拟实验室提供了密码学课程中最重要的一些算法组件，现以密码算法组件为例，详细介绍组件的设计过程。

对于简单的密码算法，如移位密码、代替密码等古典密码，或 RSA 等简单的现代密码，也可以直接将算法编成组件，或者利用已有的数论组件来实现算法。如 ELGamal 算法的加密过程为：$y_1 = x \times c^r \% p$，$y_2 = b^r \% p$，其中 x 为明文，r 为随机数，b 和 p 是系统已知的，c 为公钥，(y_1, y_2) 为密文。根据其加密算法原理，可以选择指数运算组件和一个乘法模运算组件来实现，实验过程如图 4 所示。

对于比较复杂的算法，首先对算法的步骤进行分析，找出其中的共同模块编成组件。下面以 DES 算法实验为例，说明组件的分析与设计过程。

DES 算法主要由输入、置换(包括 IP 置换和 IP 逆置换)、密钥生成、Feistel 网络以及输出五大部分组成。

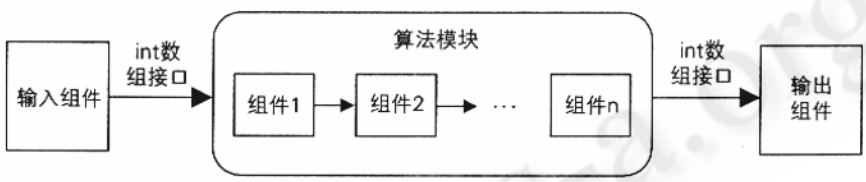

图 3　使用组件进行实验流程示意图

由于数论基础实验处理的都是整型数，而且即使密码加密解密输入的明文或密文为字母，输入组件也能将其转换为 ASCII 值，所以密码学虚拟实验室所设计的组件的输出都是 int 数组。在组件的设计中，可以将数论实验中的每一个基本算法编成一个独立的组件，以供验证实验和密码学实验使用。而各种密码算法，其实现过程都包含三大模块：明文或待解密的密文输入，加密或解密算法，输出密文或解密后的明文(见图 3)。我们规定用 int 数组来表示密码数据，组件之间的接口必须是满足该数据类型的数组。组件必须采用 XML 技术保存系统配置参数，建立复杂的树形数据模型，把算法组件装载到组件列表栏中，使用户平台能显示这些算法组件的信息。系统在运行时将

Festil 网络包括 16 轮迭代，每轮迭代都需要一个子密钥。设计中一共定义了输入、输出、置换、异或、扩展、拆分、合并、循环左移八个组件，每个组件用一个类实现，其类名和作用见表 1。

在进行 DES 算法实验时，选择相应的组件即可。DES 算法中每个模块所用的组件如表 2 所示，这些组件亦可应用到其他加密算法中。例如，在测试 DES 的弱密钥时，可以使用密钥生成模块来逐个测试，在该模块中用户可以任意选择循环次数(最大值为 16)，得到该循环次数下的子密钥生成结果。测试 DES 的弱密钥的设计中一共使用到了 9 个 JavaBeans 的类，其中有 8 个重用到了 DES 算法模块所用的类。它的类名和作用

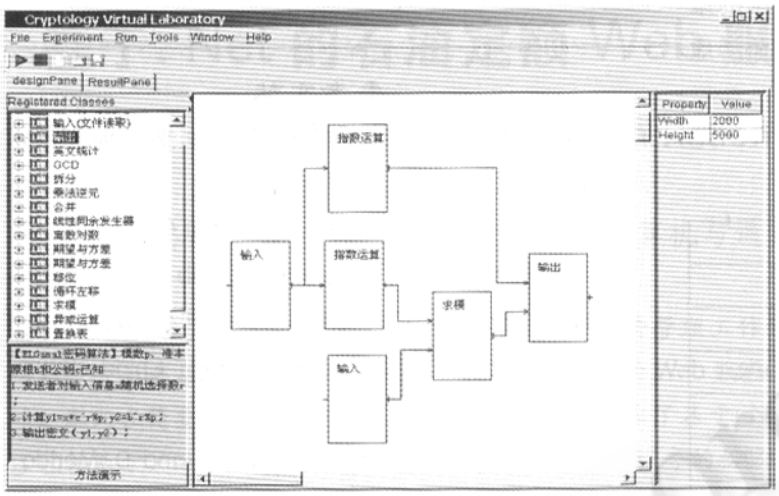

图 4　ELGamal 算法加密实验操作过程图

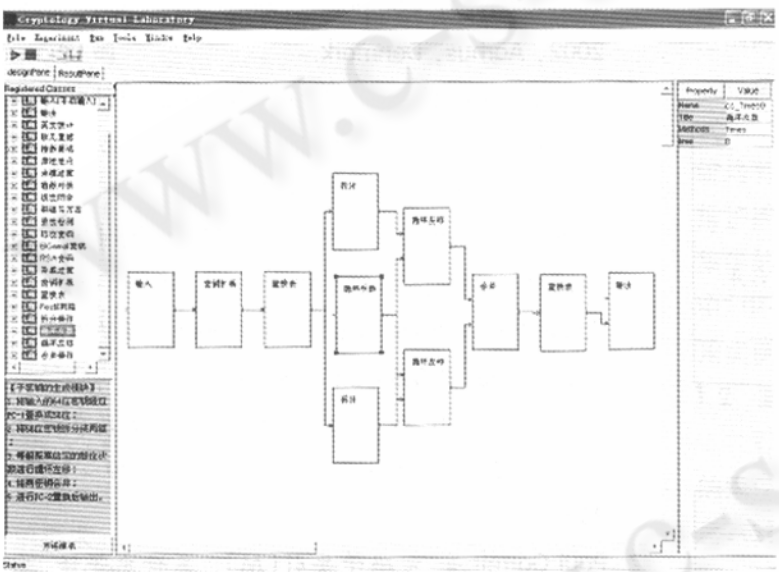

图 5　测试 DES 弱密钥的实验操作过程图

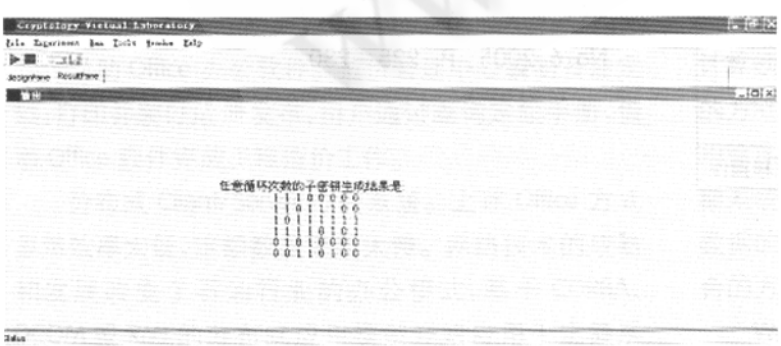

图 6　循环次数为 8 次时的子密钥生成结果图

见表 3。

在测试时，假定用户输入密钥 program，经过（密钥）输入组件的 ASCII 转换出来的是一组 56 位的密钥，该密钥以 int 型数组为接口传入类 cs_ExtendOperation 中，用大小为 64 的数组 key 存储这组扩展后的密钥值，其中扩展的 8 位为奇偶校验位。然后把数组 key 进行 PC－1 置换，由于弱密钥的测试过程要经过 PC－1、PC－2 两次置换，所以我们设置了一个通用的置换组件，通过调用 cs_TransformTable 类中不同的构造函数来实现给定规则的置换。

再将置换后的结果传入类 cs_DivideOperation 中，以此来拆分为左右各 28 位的两部分。此外，通过类 cs_LsTimes 输入任意循环左移的次数并与前面拆分后的结果分别两次传入类 cs_Lsloop 中，该类主要完成给定循环次数下的循环左移操作。

再将循环左移后的左右两部分结果传入 cs_UniteOperation 进行合并操作，然后选择置换表组件中的 PC－2 置换，最后将置换后的结果传入类 cs_DisplayText 进行结果输出。其实验流程图如图 5 所示。图 6 为循环次数为 8 次时的子密钥生成结果。

5　结论

本文在分析密码学传统实验教学中存在问题的基础上，描述了基于组件密码学虚拟实验室系统的设计及其组件的实现过程。利用该实验系统，用户能进行可视化的实验流程定制，对已有的算法进行验证实验；能按照自己的需要根据不同课程的要求组合相应的实验，进行密码算法的设计和密码攻击技术的研究；用户还可以加入自己编写的算法进行验证及扩充实验组件。

实验平台以 JavaBeans 组件形式开发，在客户端和服务器端均采用纯 Java 语言实

现，大大加快系统运行的速度，更有利于对系统的维护和扩充，为科研、教学等提供了一个很好的密码学虚拟实验平台。

表 1　DES 算法模块所用的组件表

类名	功能
cs_ PlaintextGenerator	输入明文、密钥或密文
cs_DisplayText	显示密文或解密的明文
cs_TransformTable	按照给定的置换规则进行位置换
cs_XorOperation	进行异或运算
cs_ExtendOperation	按照给定的扩展规则进行位扩展
cs_DivideOperation	按照给定的拆分规则进行拆分处理
cs_UniteOperation	进行合并操作
cs_LSloop	按照给定的移位规则进行循环左移操作

表 2　DES 算法模块所用的组件表

模块	功能	应用组件
输入	输入	输入
IP 置换	混淆	置换
密钥生成	生成子密钥	置换、扩展、循环左移、拆分、合并
Festil 网络	迭代	置换、异或、特定函数
输出	输出	输出

表 3　测试弱密钥所用的组件表

类名	功能
cs_ PlaintextGenerator	输入密钥
cs_DisplayText	显示生成的子密钥文
cs_TransformTable	进行 PC－1 或 PC－2 置换
cs_LsTimes	输入循环左移的次数，最大值为 16
cs_ExtendOperation	将 56 位的密钥扩展为 64 位
cs_DivideOperation	进行左右拆分处理
cs_UniteOperation	进行合并操作
cs_Lsloop	按照给定的移位规则进行循环左移操作

参考文献

1 胡向东等著，应用密码学教程[M]，电子工业出版社，2005，P. 26－27.

2 Jiannong Cao, Alvin Chan, Weidong Cao, and Cassidy Yeung, Virtual Programming Lab for Online Distance Learning[C], LNICS 2436, First International Conference, ICWL 2002 Hong Kong, China, 2002, P. 216－227.

3 L. Fabrega, J. Massaguer, T. Jove, and D. Merida, A Virtual network laboratory for learning IP network [C], The 7th Annual Conference on Innovation and Technology in Compute Science Education, June 2002, Aarhus, Denmark.

4 M. Duarte and B. P. Butz, The Virtual Laboratory for the Disabled[C], the 31th ASEE/IEEE Frontiers in Education Conference S1C－23, 2001.

5 R. Subramanian and I. Marsic, ViBE: Virtual Biology Experiments[C], In Proceedings of the Ten Tnternational World Wide Web Conference (WWW10), Hong Kong, P. 316－325, May 2001.

6 张耀鸿、罗雪山、余滨，基于组件的分布离散事件仿真环境[J]，系统仿真学报，14(8):1019－1021，2002.

7 Paul Garrett 著，密码学导引[M]，吴世忠等译，北京:机械工业出版社，2003.

8 王建新、凌亮、王伟平，基于 WWW 的计算机网络虚拟实验室的设计与实现[J]，计算机工程，Vol. 31, No. 6, 2005, P. 228－230.