

密钥加密实验平台的研究与实现

孙国梓^{1,2}, 林清秀^{1,2}, 陈丹伟^{1,2}

(1. 南京邮电大学 计算机技术研究所, 江苏 南京 210003;

2. 南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要:信息安全专业的学生在学习过程中,通常感觉密码学的教学过程比较抽象。针对这一问题,设计实现了密钥加密实验平台。通过对实验平台的总体框架进行分析,从演示算法的过程展示、密钥的生成过程、加解密过程解析等几个方面进行了详细的设计,给出了在 Microsoft Visual Studio .NET 2005 环境下运用 C# 语言设计实现密钥加密实验平台的具体方法。通过实验平台的具体实现,将相关知识点进行更好的分类,使这些知识以有趣而易于理解的方式呈现在读者的脑海中,效果强于教科书枯燥文字的形式,激发了学习者的兴趣。

关键词:实验平台; 密钥; 加密; RSA

中图分类号:TP391;TP309.7

文献标识码:A

文章编号:1673-629X(2009)08-0144-04

Research and Realization of Key Encryption Experiment Platform

SUN Guo-zi^{1,2}, LIN Qing-xiu^{1,2}, CHEN Dan-wei^{1,2}

(1. Inst. of Computer Technology, Nanjing University of Posts & Telecommunications, Nanjing 210003, China;

2. College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: In the major of information security, students always find that it is difficult to learn the cryptology. Because when they learn the cryptology, they can find that it is abstract and is hard to be understood. Aiming at this problem, designs an experiment platform to realize the key encryption. Detailed design is given from these aspects, such as the display of the algorithm procedure, the procedure of the key generation, and the analysis of encryption and decryption. After analyzing the framework of the experiment platform, presents the specific methods. Using C# language under the environment of Microsoft Visual Studio .NET 2005, the key encryption experiment platform was implemented. Through the implementation, all the correlation point of the knowledge are classified in sequence. With this platform, the learner will find it's funny and well to understand the knowledge. This style is better than the dull book, so it can arouse the learner's interesting.

Key words: experiment platform; secret key; encryption; RSA

0 引 言

信息安全的核心是密码技术,密码技术是集数学、计算机科学、电子与通信等诸多学科于一身的交叉学科。它不仅能够保证机密性信息的加密,而且能够实现数字签名、身份验证、系统安全等功能,是现代化发展的重要科学之一。我国的信息技术还不发达,因为国内网络信息安全研究起步较晚,投入少,研究力量分散,与技术先进国家有差距^[1]。另外,由于国外对加密技术的限制和保护,国内无法得到急需的安全而实用的网络安全系统和数据加密软件。由于系统安全内核

受控于人,以及国外产品的不断更新升级,基于具体产品的增强安全功能的成果,难以保证没有漏洞,也难以得到推广和应用。目前国内各种专用网内没有密码基础设施支撑,普遍处于缺乏密码保护的不安全状态^[2~4]。无论是在国内还是国外,信息经济的发展都是必然之势,为了更好地为信息经济服务,必须大力发展信息安全相关技术。密码加密算法作为信息安全的支撑技术,其特点是其理论和实现晦涩难懂,尤其对于初学者更是如此。基于此,参照网络实验平台等的类似设计思想,笔者设想建立基于密钥加密算法的实验平台,以实验平台作为学习者的学习平台,激发学习者更大的学习兴趣^[5,6]。通过平台,可以把相关知识点进行更好的分类,能使这些知识以有趣而易于理解的方式呈现在读者的脑海中,比起教科书上枯燥的文字,效果要强的多,学习时间也大大地减少了。

收稿日期:2008-11-24;修回日期:2009-02-27

基金项目:江苏省自然科学基金计划项目(05KJJD520150);南京邮电大学教学改革研究项目(JG004 07JX22)

作者简介:孙国梓(1972-),男,博士,副教授,硕士生导师,研究方向为计算机通信网与安全、计算机取证。

1 实验平台的总体框架

为了达到激发学习者兴趣的目的,本实验平台考虑以下几点:1) 实验平台使用简洁明了的界面;2) 尽量简化操作,以原理为中心展开演示;3) 将实验平台以常见网页的形式展现。由于 Visual Studio . NET 2005 (以下简称 VS 2005) 自身强大的功能,使用起来较方便,本实验平台就以其作为开发平台,使用 C# 作为编程语言^[7]。在该开发平台下制作 . aspx 动态网页实现该实验平台的功能,后台程序实现以控件下直接编写代码为主。

整个实验平台主要由以下四个部分构成。

第一部分是实验平台系统的主界面,它是整个实验平台的入口。需要实现对密码体制系统的总体介绍,简要介绍密码体制和实验平台系统的使用说明。能使用户对密码体制以及这个实验平台有最基本的了解,在此基础上,列出比较经典的加解密算法的基本原理和实验平台系统的帮助信息。

第二部分给出各密码体制的流程图,对流程图进行必要的简洁介绍,使用户能更好地理解各个算法的具体实现过程。

第三部分是构建基于密码算法的实验演示系统示例。用户自主选择相应参数,触发具体算法,用户通过系统提示自主操作完成演示,使得用户能够通过这些步骤更为深入地掌握算法的基本原理和实现流程。

第四部分给出算法可能的应用,在演示之后介绍各个算法的优缺点,通过分析密钥长度及加密过程,提出可能的破解方法,同时针对可能的攻击给出相应的防范措施。上述每个部分都由相应的子模块构成,子模块的功能集合实现每个部分的功能。系统的总体框架结构如图 1 所示。

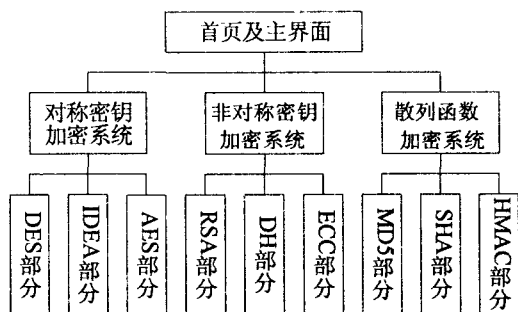


图1 实验平台的总体框架

该试验平台功能模块的总体架构总体来说功能层次比较清晰,且比较全面,它包括了对称密钥加密系统部分、非对称密钥加密系统部分和散列函数加密系统部分。整个实验平台的框架结构呈现树形,由总到分,由算法体制的总体介绍到具体算法的实例演示,这对

于初学者来说,较易入手,且容易引发学习的兴趣。

每个具体的算法部分又包括如图 2 所示的基本内容。图 2 中的 X 分别代表 DES、IDEA、AES、RSA、DH、ECC、MD5、SHA、HMAC 等算法。

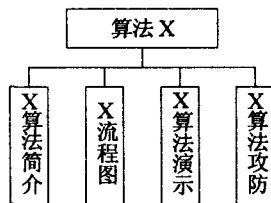


图2 单一算法的结构示意

2 主要实现方法

在实际实现过程中,通过网页的形式展示本实验平台,通过 menu. aspx 实现页面间的链接。进入主界面后链接到相应子系统形成整个实验平台系统。实验平台中所有网页的结构都为左右结构,左边是整个实验平台树型结构的索引,右边是具体模块的内容,包括欢迎界面、平台介绍、算法演示和攻击分析等内容。

2.1 演示算法的过程展示

根据网站的构建过程,首先在 VS 2005 环境下搭建起框架模块,主要包括页面和导航条。接下来的关键问题就是如何展现算法的流程,也即算法演示。

由于篇幅限制,这里不能一一介绍各个算法的演示生成过程,文中就以 RSA 演示系统为例简单介绍。图 3 给出了 RSA 算法的部分演示过程。图 3 中,用户通过实际操作,能够清晰地了解 RSA 加解密算法的流程。

RSA 加解密算法总的来说分为三步,即:1) 密钥的生成过程(这一步也是最关键的一步);2) 加密过程;3) 解密过程。具体参见图 3 的演示结果显示。通过此演示界面,用户很容易理解 RSA 加密的大体流程。

2.2 密钥的生成过程

下面结合 RSA 算法的原理具体分析此演示界面的实现过程。

对于 RSA 加密算法,关键问题是如何快速有效地生成加解密密钥。RSA 算法的密钥生成是分步完成的。首先要选取两个大的互异的大素数 p 和 q ^[8],参见图 3,要生成大素数,点击名称为“生成大素数 p ”的按钮,此时,触发相应的 Button1_Click 事件,其结果是根据生成大素数的函数 ulong getpre(),生成大素数,并在 TextBox1 控件中显示输出。函数 getpre() 是直接加载在 button 后台代码中的。接下来,要生成与 p 互异的大素数 q 。同样地,用户点击按钮“生成大素数 q ”,则在

TextBox2 控件中生成大素数 q , 其后台操作与生成 p 的方法一致, 都是后台直接加载代码的方式生成, 结果见图 3。接下来是生成 $n = p \times q$, n 在加解密中都起到很重要的作用, 因此其生成方法也是较关键的。用户根据演示界面可以很容易地理解该步骤, 如图 3 所示。其生产过程很简单, 把 TextBox1 和 TextBox2 中的数字相乘, 得到的结果即是 n 值。

一 密钥的生成过程:	
(1) 生成大素数	
生成大素数 p	25639
生成大素数 q	15269
(2) 生成参数 n	
计算 $n=p \times q$	391481891
(3) 计算 $F(n) = (p-1) \times (q-1)$	
计算 $F(n)$	391440984
(4) 取随机数 e, 使其与 $F(n)$ 互素	
取 e 得	21311
(5) 取 d, 由 $(d \times e) \% F(n)$ 得 d	
计算 d 得	215438567
(6) 得到密钥对	
得到公钥	$e=21311 \quad n=391481891$
得到私钥	$d=215438567 \quad n=391481891$

二 加解密过程	
请输入要加密的明文	
你好啊, 很高兴认识你, 我们是永远的朋友	
加密	
07a70d8f0226bcc800cdebbec0696c452136 9c1f3063a34ba0229c58d0448c4470cc2ec	
解密	
你好啊, 很高兴认识你, 我们是永远的朋友	

图 3 RSA 加密算法演示流程图

事实上, 因为 TextBox 中的文本显示是以字符串的形式显示的, 所以在 VS 2005 中, 技术方面的实现存在一个字符串到数字的转变过程和数字到字符串的转换过程。这一步的后台实现过程如下所示, 在 Button3_Click 事件中加载如下代码:

```
ulong p = ulong.Parse(TextBox1.Text.ToString());
ulong q = ulong.Parse(TextBox2.Text.ToString());
ulong n = p * q;
TextBox3.Text = n.ToString();
```

其中语句 `ulong.Parse(TextBox1.Text.ToString())` 用于把 TextBox1 中的数字字符串转换为与之对应的数字值, 以便于数字计算。`n.ToString()` 语句用于把数字转换为与之对应的数字字符串, 以便于在 TextBox 中显示输出。在整个的平台构建及所有的算法演示中, 这种变换经常用到。

如图 3 所示, 继续进行保密值 $F(n) = (p-1) \times (q-1)$ 的计算, 因其实现方法同 n 的值的实现类似, 这里不再赘述。

根据 RSA 算法的原理过程, 接下来是取随机数 e , 取 e 的关键是要与 $(p-1) \times (q-1)$ 互素。 e 可由函数 `gete()` 实现, 在函数中加入判断语句用于验证是否与 $(p-1) \times (q-1)$ 互素。下面给出其实现过程, 也即在 Button6_Click 事件下加载如下代码:

```
RSAL f = new RSAL();
ulong p = ulong.Parse(TextBox5.Text.ToString());
ulong q = ulong.Parse(TextBox4.Text.ToString());
```

```
ulong s = f.inverse(p, q);
TextBox6.Text = s.ToString();
```

设计加密类 `RSAL()`, 其中包括函数 `inverse(p, q)`, `inverse(p, q)` 用于计算 $F(n)$ 值。在上述代码中, 通过引用 `RSAL()` 的一个实例来调用函数 `inverse(p, q)` 功能。通过语句 `TextBox6.Text = s.ToString();` 把生成的值 $F(n)$ 以值字符的形式显示在 TextBox6 中。

接下来点击“得到公钥”和“得到私钥”按钮, 触发按钮事件, 分别能在 TextBox 中显示得到的密钥对。通过以上分析, 可以看出, 此演示平台的演示过程能够把 RSA 加密算法的原理清晰地表现出来。

2.3 加解密过程解析

接下来简单介绍一下加解密的过程解析。在明文文本框中输入需要加密的文本, 通过点击“加密”按钮, 触发 Button7_Click 事件, 在此事件中加载加密函数, 同时把文本框中的文本引导进来作为加密软接口, 实现对文本的实际加密。具体的加密算法不再赘述。加密理论函数为: $c = Me \bmod n$, 需要用具体的数据结构实现, 在此也不再赘述。点击“解密”按钮, 类似触发 Button8_Click 事件, 此事件的功能代码把密文作为软件接口参数引导进来, 用解密函数进行解密处理, 得到解密后的明文, 如图 3 所示。

2.4 其他问题

以上对密钥加密实验平台系统中的关键模块——算法演示部分以 RSA 算法演示为例进行了简单介绍。其它典型加密算法演示生成界面都以其算法的原理为基础进行形象展现。由于篇幅限制, 这里不再赘述。

2.4 其他问题

在密钥加密实验平台的构建中, 为了能够给用户一个清晰简单的操作环境, 有很多技术实现方面的细节都需要加以注意, 如导航条的构建、模板页的设置、格式的一致和规范性的要求等。

在密钥加密实验平台的构建中, 为了能够给用户一个清晰简单的操作环境, 有很多技术实现方面的细节都需要加以注意, 如导航条的构建、模板页的设置、格式的一致和规范性的要求等。

3 特点概述

1) 平台展示清晰、全面。参见图 1 的总体架构, 打开此平台系统, 首先进入的是登录页面, 当用户输入正确的用户名、密码后, 进入首页。首页中包括三个系统展现按钮, 分别为: 对称密钥加密系统、非对称密钥加密系统和散列函数加密系统。布局清晰简单, 用户可以根据自己的需求进入不同的加密系统。进入某个具体加密系统后, 便进入了学习页面, 每个页面的布局都是一致的, 左边是导航栏, 右边是对应的学习内容。

用户可以由导航栏快捷地选择自己想要进入的学习阶段。所有这些部件,都是为了方便用户更好地学习密钥加密算法。

2) 实验管理方便。本实验平台首页有注册及登录页面,当用户登录后能显示用户之前的登录信息。这些信息用在教学过程中,指导老师就可以方便地查询各学生登录和使用本平台软件的基本情况,有利于老师了解同学们的实验细节,利于管理。

3) 原理分析直观。在分步执行的过程中,实验平台所包括的各个算法可以实时、直观地进行原理的分析。如:在算法的演示过程中,用户可以直观并清楚地知道“数”的流向及具体算法的执行过程。相比书本上的“枯燥”内容来说,此平台演示就相当于请了个老师,一步一步地演示出算法的基本原理和过程,直观地展现给用户,有效降低了学习的难度。

4 结束语

实现了密钥加密实验平台,给出了实验平台的总体框架,分析了平台实现的主要技术方法。该实验平台最终实现了对各密钥加密算法的基本介绍,能够对算法原理进行较为深入的剖析。通过本实验平台完成了各个算法的实验演示,实际使用过程中取得了较为理想的实验效果。平台通过网页的形式将算法进行分步剖析,使得算法清晰直观,大大减少了学习者的理解

难度。下一步工作是进一步丰富和完善算法系统,并考虑和远程控制实验平台、攻击防范实验平台等的进一步融合,以便扩展成为信息安全的综合实验平台。

参考文献:

- [1] 胡向东,魏琴芳.应用密码学[M].北京:电子工业出版社,2006.
- [2] Bao Feng, Lee Cheng - Chi, Hwang Min - Shiang. Cryptanalysis and improvement on batch verifying multiple RSA digital signatures[J]. Applied Mathematics and Computation, 2006,172(2):1195 - 1200.
- [3] Ashrafi M Z, Ng S K. Privacy - preserving e - payments using one - time payment details[J]. Computer Standards & Interfaces, 2009,31(2):321 - 328.
- [4] 曹建国,王丹,王威.基于RSA公钥密码安全性的研究[J].计算机技术与发展,2007,17(1):172 - 173
- [5] 张焕国,王丽娜.信息安全综合实验教程[M].武汉:武汉大学出版社,2006.
- [6] Castagnos G. An efficient probabilistic public - key cryptosystem over quadratic fields quotients [J]. Finite Fields and Their Applications, 2007,13(3):563 - 576.
- [7] Matthew M, Erik J. C#数据安全手册[M].崔伟,毛尧飞译.北京:清华大学出版社,2003.
- [8] 张宏,刘晓霞,张若岩. RSA公钥密码体制中安全大素数的生成[J]. 计算机技术与发展,2008,18(9):131 - 133.

(上接第143页)

SuperWatchdog,该系统是在现有解决方案 Watchdog的基础上提出的。SuperWatchdog解决了 Watchdog的一个致命的问题,即一个恶意节点可以通过虚假报告其他节点行为异常来分割的网络。使用的吞吐量和系统开销作为评价 SuperWatchdog 性能的指标,Super-Watchdog 系统中一些恶意节点虚假报告其他节点行为异常。对于每一个指标,分别对 Watchdog 和 Super-Watchdog 进行了比较检验。仿真结果表明,解决方案虽然没有明显的增加吞吐量,但大大地降低了开销。

参考文献:

- [1] IETF Mobile Ad hoc Networks (MANET) Working Group [EB/OL]. 2008 - 08 - 21. www.ietf.org/html.charters/manet-charter.html.
- [2] Perkins C, Belding - Royer E. RFC3561: Ad hoc On Demand Distance Vector (AODV) Routing [EB/OL]. 2003. http://www.ietf.org/rfc/rfc3561.txt.
- [3] Johnson D B, Maltz D A, Hu Y C, et al. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) [EB/OL]. 2003 - 04. http://www.cs.cmu.edu/dmaltz/internet-drafts/draft-ietf-manet-dsr-09.txt.
- [4] Marti S, Giulì T J, Lai K, et al. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks[C]//in 6th International Conference on Mobile computing and Networking, MOBI-COM'00, IEEE CS. U S A: [s. n.], 2000:255 - 265.
- [5] Zhou L, Haas Z. Securing ad hoc networks[J]. IEEE Network Magazine Special Issue on Network Security, 1999,13(6):1 - 12.
- [6] 石硕,顾学迈,张文彬,等.移动 Ad hoc 网络的 NS2 仿真机制及代码分析[J].计算机工程与设计,2008,29(18):4639 - 4643.
- [7] 林果园,黄皓,张永平.入侵检测系统研究进展[J].计算机科学,2008,35(2):69 - 74.
- [8] 李兵.一种基于对等模型的网络入侵检测系统模型[J].计算机技术与发展,2008,18(3):173 - 176.
- [9] 吴吉义,平玲娣,范容,等.基于自适应信任报警关联的 P2P 覆盖 IDS[J].解放军理工大学学报:自然科学版,2008,9(5):455 - 459.
- [10] 高永梅,吴吉义,张启飞.基于智能信任关联的对等协同 IDS 仿真[J].系统仿真学报,2008,21(4):56 - 65.