

密码算法研究

张晓丰, 樊启华, 程红斌

(空军工程大学 工程学院, 陕西 西安 710038)

摘 要: 密码算法是信息安全的重要保证。介绍了密码体制的数学定义, 并比较了对称密码算法和非对称密码算法, 比较了 DES、AES 对称密码算法, 两者中 AES 具有比 DES 更好的安全性、效率、灵活性; 分析比较了 RSA、ECC、NTRU 等非对称密码算法, 要实现相同的安全水平 NTRU 所需要密钥长度最短。

关键词: 密码算法; 对称密码算法; 非对称密码算法

中图分类号: TP309.7

文献标识码: A

文章编号: 1005-3751(2006)02-0179-02

Research on Cryptography Algorithms

ZHANG Xiao-feng, FAN Qi-hua, CHENG Hong-bin

(Engineering Institute of Air Force Engineering University, Xi'an 710038, China)

Abstract: Cryptography Algorithms are the foundation of information security. This paper introduces the mathematical definition of cryptography, and makes a comparison of symmetric cryptography algorithms and asymmetric cryptography algorithms, then analyzes the symmetric cryptography algorithms; DES, AES and the asymmetric cryptography algorithms; RSA, ECC and RTRU. AES is better than DES in security, efficiency and flexibility, and NTRU is better than RSA and ECC in security.

Key words: cryptography algorithms; symmetric cryptography algorithms; asymmetric cryptography algorithms

信息时代中保证信息安全成为一项急迫的需求, 政府部门、金融行业、通信行业以及军队的指挥控制、通信、情报系统都非常重视信息安全, 而密码技术则是所有安全服务的基础, 用于加密和解密的数学函数的密码算法 (Cryptography Algorithm) 又是密码技术的核心, 为此, 世界各国都高度重视密码算法的研究。

1 密码算法

密码算法是密码体制的核心, 它由加密和解密组成, 加密是将明文转换成攻击者无法理解的密文形式, 解密则将密文恢复成明文。加解密算法一般是公开的, 其安全性仅依赖于密钥的保密性, 密码体制的数学定义为一个满足以下条件的五元组 $(P, C, K, E, D)^{[1]}$:

- 1) P 表示所有可能明文组成的有限集, 即明文空间。
- 2) C 表示所有可能密文组成的有限集, 即密文空间。
- 3) K 代表密钥空间, 由所有可能密钥组成的有限集。
- 4) 对任意 $k \in K$, 都存在一个加密法则 $e_k \in E$ 和相应的解密法则 $d_k \in D$ 。且对每一 $e_k: P \rightarrow C$ 和 $d_k: C \rightarrow P$, 对任意的密文 $x \in P$, 均有 $d_k(e_k(x)) = x$ 。

记加密密钥为 k_p , 解密密钥为 k_s , 按照密钥的特点可将密码算法分为私钥密码算法、公钥密码算法两类, 亦即

对称密码算法、非对称密码算法。

1.1 对称密码算法

对称密码算法中 k_p 同 k_s 相同, 或实质上等同, 即易从 k_p 推出 k_s 。对称密码体制从加密模式上可分为序列密码和分组密码两大类。在对称加密系统中, 加密和解密采用相同的密钥, 而因为加解密密钥相同, 需要通信的双方必须选择和保存他们共同的密钥, 各方必须信任对方不会将密钥泄密出去, 这样才可以实现数据的机密性和完整性。

1.2 非对称密码算法

非对称密钥算法又称双钥密码算法, 该算法中 k_p 与 k_s 不同, k_p 称为公开密钥, 简称公钥; k_s 必须保密, 简称私钥。公钥密码算法中从 k_s 可以很容易地推出 k_p , 但很难从 k_p 推出 k_s , 这种单向性是基于陷门单向函数实现的, 其中陷门单向函数是满足下列条件的函数 f :

- 1) 给定 x , 容易计算 $y = f_k(x)$;
- 2) 给定 y , 计算 x 使 $x = f_k^{-1}(y)$ 不可行;
- 3) 存在 k , 当 k 已知时, 对给定的任何 y , 若相应的 x 存在, 则计算 x 使 $x = f_k^{-1}(y)$ 是容易的。

1.3 两类算法的比较及应用

对称密码算法和非对称密码算法各有优缺点, 两者的比较如表 1 所示。在实际应用中, 非对称密码算法通常被用来加关键性数据, 如会话密钥, 而对称密码算法通常被用来加密大量的数据, 这样就较好地解决了运算速度问题和密钥分配管理的问题。

收稿日期: 2005-05-30

作者简介: 张晓丰 (1978—), 男, 天津蓟县人, 博士研究生, 研究方向为信息系统工程、智能决策系统; 导师: 张凤鸣, 教授。

表 1 对称密码算法和非对称密码算法的比较

	优点	缺点
对称密码算法	加解密速度快	密钥分发和管理复杂; 不能用于数字签名等应用
非对称密码算法	密钥分配和管理简单; 可应用到数字签名中实现鉴别、防抵赖等目标	算法复杂,加解密速率较低

2 常见密码算法分析

2.1 常见对称加密算法

对称密码算法中最著名的是美国数据加密标准 DES 和高级加密标准 AES。

1) DES 算法。

DES 算法由 IBM 公司开发,并被美国国家标准局 (NIST) 于 1977 年 2 月采纳作为“非密级”应用的标准,并得到广泛应用,它曾是世界上使用最广泛的密码算法^[1]。

DES 算法加密时把明文以 64 比特为单位分成块,采用美国国家安全局精心设计的 8 个 S 盒和 P 置换,经过 16 轮迭代,最终产生 64 比特密文,每轮迭代使用的 48 比特子密钥由原始的 56 比特产生。DES 的加密与解密的密钥和流程完全相同,区别仅仅是加密与解密使用的子密钥序列的施加顺序正好相反^[2]。

DES 算法存在以下问题:

- DES 密钥空间的规模 (256bit) 对实际安全而言太小;
- 算法的密钥存在弱密钥、半弱密钥和互补密钥;
- 除去 S 盒,DES 里的所有计算全是线性的,而且 S 盒的设计对密码算法的安全性至关重要。

然而,NIST 并未公布 S 盒的设计原则,因此,有人怀疑 S 盒里隐藏了“陷门”,同时,由于 DES 的密钥空间小,对 DES 算法进行穷举攻击很容易取得成功,此外,还有差分密码分析方法和线性密码分析方法^[2]等攻击方法。为了增强 DES 算法的安全性,密码设计者又提出了基于 DES 的 Triple、独立子密钥方法、推广的 GDES 算法等,但这些改变有些作用不大。

2) AES 算法^[3]。

NIST 于 1997 年 1 月开始了遴选 DES 替代者——高级加密标准 (AES) 的工作,其目的是确定一个非保密的、全球免费使用的分组密码算法,并于 2000 年 10 月 2 日,选择了 Joandaemen 和 Vincent Rijmen 设计的“Rijndael 算法”,Rijndael 具有如下特点:

- 运算速度快,在有反馈模式、无反馈模式的软硬件中,Rijndael 都表现出非常好的性能;
- 对内存的需求非常低,适合于受限环境;
- 算法可靠,使用非线性结构的 S 盒,具有足够的安全余地;
- 算法采用宽轨迹策略 (Wide Trail Strategy),能有效抵抗差分分析和线性分析攻击;
- Rijndael 是一个分组迭代密码,分组长度和密钥长

度设计灵活。

总之,Rijndael 算法汇聚了安全性能、效率、易实现性和灵活性等优点,是一种较 RSA 更好的算法。

2.2 非对称加密算法

目前,密码学界已提出许多非对称密码算法,如 RSA、ECC、NTRU、背包体制、Diffie-Hellman、ElGamal 算法等,但影响最大的是 RSA 和 ECC。

1) RSA 算法。

RSA 算法由 Rivet, Shamir, Adelman 于 1978 年提出^[4],它是一种分组加密算法,其安全性基于模运算的大整数素因子分解问题的困难性,它是当前应用最广泛的非对称算法。RSA 使用的密码长度一般为 512 比特,1999 年 8 月 22 日 RSA 512 被攻破,密钥长度不得不加长,随着分解大整数方法的进步、计算机速度的提高以及并行计算技术的发展,RSA 所需用的密钥将越来越长,这将使采用 RSA 系统的速度变得愈来愈慢,这对使用 RSA 的应用带来了很重的负担。

2) NTRU 算法。

NTRU (Number Theory Research Unit) 密码算法是在 20 世纪 90 年代中期由数学家小组 Jeffrey Hoffstsin, Jill Pipher 和 Joseph Silverman 设计的^[5]。NTRU 已被接受为 IEEE P 1363 标准,被标准化在文档 Working Group for Standards in Public Key Cryptography 中。NTRU 算法使用多项式代数及两个不同数的模,它的安全性基于多项式、不同模混合运算的相互作用,也依赖于最大格及寻找最短向量的困难性,NTRU 的效率比 RSA 为高,NTRU 加密、解密一个长度为 N 的信息分组需要 $O(N^2)$ 次操作,而 RSA 需要 $O(N^3)$ 次操作。但 NTRU 也有缺点,其解密可能失败,但在仔细选择系统参数的情况下,解密失效的概率可降低至小于 5×10^{-5} 。

3) ECC 算法。

ECC 算法是 1985 年由 N. Koblitz 和 Miller 提出的一种非对称密码算法,其安全性主要是基于椭圆曲线离散对数问题求解的困难性。设 P 是 $E(F_q)$ (椭圆曲线群) 上的一个点,点 Q 是 $E(F_q)$ 上为 P 的倍数的点,即存在整数 $x > 0$,使得 $Q = xP$,椭圆曲线离散问题就是由给定的 P 和 Q 确定出 x 。从目前的研究结果看,椭圆曲线上的离散对数问题比有限域上的离散对数问题更难以处理,这意味着在椭圆曲线公钥密码中采用较小的数就可以达到与使用更大的有限域同样的安全性^[6]。从目前已知的最好求解算法来看,160 比特的椭圆曲线密码算法的安全性相当于 1024 比特的 RSA 算法。

这 3 种算法的比较如表 2 所示,表中同一行记录表示相同的安全水平所需要密钥的长度。

3 结束语

随着计算机、通信、网络技术的发展,全球信息化的步

(下转第 184 页)

素的数据。

3.3 HD-JPEG

为了让 DVI/HDMI 得到最佳的发挥,应该要“点对点”播放,提供与输出显示器相同的像素数量,即 DVD 机输出 1920×1080 的影像到 1920×1080 像素的输出显示器上,输出显示器不用需再为输入信号进行插值变换。当然,若不是使用高清晰度的显示器,而是使用 640×480 甚至更低解像度的输出显示器的话,则就算使用 1080i 输出看 DVD,其画面也改善不了多少。所以要想碟片上的信息完美地变成输出显示,其中最有效的方法是尽量减少令画面失真的处理步骤,而点对点显像以及采用 DVI/HD-MI 传送,均是为了达到上述目标。

要实现点对点的播放,有两个方面。一个是碟片里的视频信号,另一个是 DVD 机的视频解码模式。从源的视频信号来讲,DVD 的 NTSC 信号为 480i/p,随着 DTV, HDTV 以及高清晰 DC,DV 的出现,480i/p 实在不能和高解像画质相比,于是现今的 DVD 机已经内置了倍线晶片,即用复制像素的方法将 480i/p 信号以高速升频至 720p 或 1080i。但是播放高解析度的 HD-JPEG,可以轻易满足输出 1080i 甚至更高解析度的图像的需求,而不必用插值的方法来增加像素点。使用 HDMI 的最终目的是为了传送高清晰的视频和音频,然而在使用了 HDMI 的同时,在视频解码方面的瓶颈不容忽视。老式的 JPEG 视频解码模式将视频源按照标准清晰度输出,而标准清晰度产品的典型分辨率为 640×480 和 720×480 。在使用了具有 1280×720 或 1920×1080 分辨率的产品作为输出显示器时,若依旧使用标准清晰度输出,显示高清晰图像的时候,由于显示器又对输入信号做了一次变换处理,图像的失真效果就显现的比较突出。如果使用高清晰度标准(1280×720 或 1920×1080)输出,则清晰度将大有改观。正是因为有了支持高清晰度信号无压缩传输的数字接口,才使得高清晰度的视频解码模式能够得以应用。另外 HD-JPEG 的采样方式将 JPEG 图像编码成高清晰度格式(YUV-4:2:2),而不是过去的标准清晰度格式(YUV-4

:2:0),由于提高了采样率,使得能提供 clearer 的数据流传输到终端显示器上。在配合使用了高清晰的媒体接口 HDMI 以及 HD-JPEG 解码方式下,能使得图像更加逼真地呈现出来。另外,对于解析度大于输出显示器支持标准(如 1920×1080)的高清晰度 JPEG 图像,需由输入设备(如 DVD)进行采样率从 1/8 到 7/8 的压缩。

最后,值得注意的是,这里只对那些需要防复制的媒体文件进行 HDCP 加密编码,其他的媒体文件,如消费者自己制作的 JPEG 影像,必须跳过 HDCP 加密编码这一步,直接从 HDMI 接口输出。

4 结束语

“通过 HDMI 可以将 DVD 播放机、DVD 录像机、数字视信转换盒、D-VHS 播放机、影音接收器这些数字来源装置和数字电视、等离子显示器、液晶电视、投影机这些数字显示装置之间的未压缩信号,以全数字的方式互通^[5]。”而高分辨率的 HD-JPEG 填补了目前 DVD 碟片视频码流和 HDMI 可传输视频码流之间的传输带宽的裕量,将 HDMI 在视频显示上的魅力真正发挥出来。

参考文献:

- [1] Hitachi Ltd, Matsushita Electric Industrial Co. Ltd, Philips Consumer Electronics International B V, Silicon Image Inc, Sony Corporation, Thomson Inc, Toshiba Corporation. HDMI - High - Definition Multimedia Interface, Specification Version 1.1[Z],2004.
- [2] Weeks J R. JPEG Header Information[Z]. BioElectroMech, 1998.
- [3] Tachibanaya T. Description of Exif file format(rev. 1.4)[Z]. JEIDA,2001.
- [4] Jack K. Video Demystified(3rd Edition)[Z]. Demystifying Technology,2001.
- [5] Taylor J. DVD Demystified(2nd Edition)[Z]. [s. l.]: McGraw - Hill,2000.

(上接第 180 页)

伐越来越快,信息安全,尤其是网络信息安全问题已成为一项亟待解决的重大问题。密码算法作为实现信息安全的基础必然将得到越来越多的重视,而其研究结果将不断地提高信息安全性能。

表 2 RSA,NTRU 和 ECC 的比较

RSA	NTRU	ECC
512	167	113
1024	263	160
2048	503	282

参考文献:

- [1] Stinson D R. Cryptography theory and practice(2nd edition)

[M]. Beijing: Publishing house of electronics industry,2002.

- [2] US National Bureau of Standards. Data Encryption Standard [S]. Federal Information Processing Standard(FIPS). Publication46,1977.
- [3] National Institute of Standards and Technology. Federal Information Processing Standard (FIPS) [S]. Department of Commerce,US,Advanced Encryption Standard,2001.
- [4] 范红,冯登国.安全协议理论与方法[M].北京:科学出版社,2003.
- [5] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Transaction on Information Theory, 1976,22(6): 644 - 654.
- [6] 林华,彭代渊.椭圆曲线代理数字签名体制[J].计算机应用,2004,24(6):216 - 217.