文章编号:2095-476X(2014)03-0105-04

数字图书馆信息分级保密研究

杨清兰

(郑州轻工业学院 图书馆, 河南 郑州 450002)

摘要:利用RSA密码算法和对称加密算法研究数字图书馆信息分级加密算法.在该算法中,对于核心级信息(一级信息),采用RSA密码算法进行加密和解密;对于内部级信息(二级信息),采用RSA及对称密码算法进行加密和解密.一级管理员可以解密一级信息和二级信息,而二级管理员只能解密二级信息,其他人无法解密.这种分级保密措施不仅适应数字图书馆不同用户的保密需求,而且便于对信息进行分级管理,具有可用性和有效性.

关键词:数字图书馆;RSA;信息安全;信息分级保密

中图分类号:TP309; G250.76 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2014.03.024

Study on hierarchical encryption of information of digital library

YANG Qing-lan

(*Library, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*)

Abstract: Using RSA encryption algorithm and symmetric encryption algorithm, the hierarchical encryption algorithm for different levels of information of digital library was proposed. In this algorithm, the core information (first level information) was encrypted and decrypted using RSA, and the inside information (second level information) was encrypted and decrypted using RSA and symmetric algorithm. The first level manager could decrypt the first level information and the second level information, but the second level manager could only decrypt the second level information. None but the first level manager or the second level manager could decrypt. This kind of hierarchical management could not only satisfy the security requirements for different users of digital library, but also facilitate the hierarchical management of different levels of information for digital library. The hierarchical encryption scheme had the availability and effectiveness.

Key words: digital library; RSA; information security; hierarchical encryption on information

0 引言

随着图书信息内容不断增加以及计算机网络和通信技术的不断发展及推广,图书馆的数字化建设已经成为图书馆建设的一个重要内容和发展方向.但是,鉴于网络和信息安全问题日益受到重视,数字图书馆的安全建设已提上了日程,从而成为重要的研究课题.

目前,数字图书馆信息安全具有保密性、完整性、可用性、广泛性和动态性5个特点[1].针对这些特点,很多学者进行了研究.文献[1]从技术、管理手段和法规政策3个方面给出了数字图书馆信息安

收稿日期:2014-05-09

基金项目:国家自然科学基金项目(61272525)

作者简介:杨清兰(1973—),女,河南省邓州市人,郑州轻工业学院助理馆员,主要研究方向为图书馆学、数字图书馆等.

全解决对策. 文献[2]采用基于身份的加密和数字签名,确保传递的图书电子文档的保密性和完整性. 文献[3]针对网络威胁,如非授权访问、信息泄露或丢失、数据完整性、拒绝服务攻击等,提出利用身份认证、加密解密、网络防火墙等技术手段来解决数字图书馆信息安全问题. 文献[4]指出要从技术和管理2方面加强数字图书馆信息安全防护,并强调在技术上加强环节管理,注重信息资源建设中的安全保护、信息处理存储过程的安全防护、服务传播过程中的信息保护,要求制定灾难恢复计划. 最近,刘超等[5-6]也对国内数字图书馆的信息安全问题进行了分析,并提出相应的解决对策.

2007 年,杨木锐[7]针对数字图书馆信息安全的保密性特点,给出了数字图书馆信息内容保密等级划分策略. 认为应通过对数字图书馆信息进行保密等级划分,确定机密信息的保护级别,并建议根据图书馆不同用户的安全需求,构建安全体系,力图有效保证信息的保密性. 文献[7]根据国家秘密的密级划分,结合数字图书馆信息的特点,将图书馆数字信息划分为 3 个等级:核心级(如图书管理员密码、押金情况等)、内部级(如数字化的国家级重点文献、孤本、善本等)、公开级(如图书馆概况、馆藏信息等). 为叙述方便,在本文中,记核心级信息为"一级信息",相应的管理员为"一级管理员";记内部级信息为"二级信息",相应的管理员为"二级管理员".

另外,为防止一级信息、二级信息和公开信息被篡改,可采用数字签名技术[8]对一级信息、二级信息的密文和公开信息进行数字签名. 数字签名技术也可用于对一级管理员和二级管理员之间的通信内容进行认证. 为恢复已经遭到篡改的信息,应提前做好已有一级信息、二级信息和公开信息的备份工作. 一旦检测出这些信息遭到篡改,可以启动数据备份恢复工作. 相关的数字签名技术[9]和文件备份恢复技术已经相当成熟,鉴于此,本文拟实现数字图书馆信息分级保密管理,以适应不同用户的安全需求.

1 数字图书馆信息分级保密算法

利用 RSA 密码系统[10]给出数字图书馆信息分级保密算法. 这种分级加密应该具有如下的安全性要求:1)加密和解密算法应采用安全的密码体制(如 RSA、椭圆曲线密码体制、对称密码体制等)进行设计,从而保证算法具备可靠的安全性. 2)加密和解密算法应具有分级特点. 即一级管理员可以对一级信息和二级信息进行加密和解密,二级管理员只能对二级信息进行加密和解密,其他人员无法解密.

1.1 密钥的生成

一级管理员执行如下步骤:

1)一级管理员随机选取 4 个大素数 p_1, q_1, p_2, q_2,并计算 $n_1 = p_1q_1p_2q_2, n_2 = p_2q_2$.

2)随机选取正整数 e_1,满足 $\gcd(e_1, \varphi(n_1)) = 1$,其中 $\varphi(n_1)$是欧拉函数.

3)计算 d_1,使得 $e_1d_1 = 1 \bmod \varphi(n_1)$,若 $d_1 \leqslant \varphi(n_2)$,则重新回到步骤 2).

4)计算 $e_2 = e_1 \bmod \varphi(n_2), d_2 = d_1 \bmod \varphi(n_2)$.

5)销毁 $p_1, q_1, p_2, q_2, \varphi(n_1), \varphi(n_2)$,保留$(e_1, n_1)$作为一级管理员公开密钥,而将$(d_1, n_1)$作为相应的解密密钥,由一级管理员秘密保存. 同时,一级管理员将(e_2, n_2),(d_2, n_2)秘密发送给二级管理员.

二级管理员一旦接收到(e_2, n_2)和(d_2, n_2),将(e_2, n_2)作为公开密钥,而将(d_2, n_2)作为解密密钥秘密保存.

1.2 加密和解密过程

加密和解密过程分 2 类情形:一级管理员的加密和解密,二级管理员的加密和解密.

1)一级加密和解密. 即利用一级管理员的公钥和密钥对一级信息进行加密和解密的过程.

假定待加密的数据 $m \in Z_{n_1}$. 为对消息 m 进行加密,任何人都可以利用公钥(e_1, n_1)对 m 进行加密,即计算密文 $c = m^{e_1} \bmod n_1$. 一级管理员可对图书管理员密码、读者个人基本信息、押金情况等一级信息进行一级加密,而将相应的密文 c 存在计算机中. 若想进一步保证一级信息的完整性,可以采用数字签名技术对密文再进行数字签名,并存储相应的签名信息.

为对一级加密的密文 c 进行解密,一级管理员可以针对密文 c 解密计算 $m = c^{d_1} \bmod n_1$.

下面证明一级加密和解密的正确性. 事实上,若 $\gcd(m, n_1) = 1$,则根据 Euler 定理可知 $m^{\varphi(n_1)} = 1 \bmod n_1$,从而 $m^{l\varphi(n_1)+1} \equiv m \bmod n_1$,其中 l 为任意整数. 若 $\gcd(m, n_1) \neq 1$,则由于 $m < n_1$,m 不可能同时是 p_1, q_1, p_2, q_2 的倍数. 假定 $m = cp_1$,c 是整数且与

$q_1p_2q_2$ 互素. 则由 Euler 定理有 $m^{\varphi(q_1p_2q_2)} \equiv 1 \bmod q_1p_2q_2$,则对于任意整数 l,有

$$m^{l\varphi(q_1p_2q_2)\varphi(p_1)} \equiv 1 \bmod q_1p_2q_2 \Rightarrow$$

$$m^{l\varphi(n_1)} \equiv 1 \bmod q_1p_2q_2 \Rightarrow$$

$$m^{l\varphi(n_1)} = 1 + kq_1p_2q_2(k \text{ 为某整数}) \Rightarrow$$

$$m^{l\varphi(n_1)}m = m + kcn_1 \Rightarrow m^{l\varphi(n_1)+1} = m \bmod n_1$$

类似地,可以证明,对于 $m = cp_iq_j$,或 $m = cp_iq_jp_f$ $(i \neq f)$,或 $m = cp_iq_jq_f(j \neq f)$,其中 $i,j,f \in \{1,2\}$,$m^{l\varphi(n_1)+1} = m \bmod n_1$ 总是成立.

因此,可知存在整数 w,使得 $c^{d_1} \equiv m^{e_1d_1} \bmod n_1 \equiv m \bmod n_1$,由此可证明一级加密和解密算法正确.

需要注意的是,对于一级加密所使用的密钥 (d_1,n_1),应由一级管理员秘密保存. 为保证密钥存储的安全性,一级管理员可将密钥存储在大脑以及安全的智能卡中. 也可以把密钥再次加密,并进行秘密分割,分别存入多个服务器或终端之中.

2) 二级加密和解密,即利用二级管理员的公钥和密钥对二级信息进行加密和解密的过程.

首先,二级管理员需要随机选取一个安全的对称加密密钥 key,假定 $key \in Z_{n_2}$. key 作为对称密钥,需要二级管理员秘密保存. 为此,二级管理员首先需要利用 RSA 加密算法对 key 进行加密,利用公钥 (e_2,n_2) 计算密文 $c_{key} = key^{e_2} \bmod n_2$,并在计算机中保留 c_{key},而销毁 key.

二级管理员用对称密钥 key 和对称加密算法对二级信息 m 进行对称加密. 为此,二级管理员首先由 c_{key} 恢复对称密钥,即利用 RSA 解密算法计算对称密钥 $key = c_{key}^{d_2} \bmod n_2$. 然后,二级管理员利用对称加密算法和对称密钥对二级信息 m 进行加密. 采用的对称加密算法为美国数据加密标准算法 DES(data encryption standard),得到密文 $c_m = \mathrm{DES}(key,m)$.

当需要对密文 c_m 进行二级解密时,二级管理员首先由 c_{key} 恢复对称密钥,即利用 RSA 解密算法计算对称密钥 $key = c_{key}^{d_2} \bmod n_2$,然后利用 DES 解密密文 $m = \mathrm{DES}^{-1}(key,c_m)$,最后,二级管理员销毁 key.

为保证密钥 (d_2,n_2) 存储的安全性,二级管理员可将密钥存储在大脑或安全的智能卡中. 也可以把密钥再次加密,并进行秘密分割,分别存入多个服务器或终端之中. 另外,在上述的二级加密和解密中,key 以 RSA 密文 c_{key} 的形式存储,在 RSA 安全性的保证下,key 具有较好的安全性. 但是,为保证 key 和二级信息具有更好的安全性,二级管理员可以定期更换 key,并利用 key 更新对二级信息的加密.

一级管理员通常拥有最高权限,不仅可以解密浏览一级信息,还可以解密浏览二级信息. 然而,由于二级管理员通常为数字图书馆一般工作人员,笔者限定二级管理员只能解密浏览二级信息. 本文提出的分级加密和解密算法刚好满足这个要求.

事实上,根据二级加密过程可知,一级管理人员可以通过解密二级管理员保留的密文 c_{key} 恢复对称密钥,即一级管理员可以计算 $key = c_{key}^{d_1} \bmod n_2$. 可以证明这种 RSA 解密算法的正确性. 这是因为

$$e_1d_1 = 1 \bmod \varphi(n_1)$$

即存在某个整数 h,使得 $e_1d_1 = 1 + h\varphi(n_1)$,注意到 $e_2 = e_1 \bmod \varphi(n_2)$,$d_2 = d_1 \bmod \varphi(n_2)$,则对等式 $e_1d_1 = 1 + h\varphi(n_1)$ 两边同时取 $\bmod \varphi(n_2)$,可得 $e_1d_1 \bmod \varphi(n_2) = e_2d_1 \bmod \varphi(n_2) = e_2d_2 \bmod \varphi(n_2) = 1$. 则可验证:

$$c_{key}^{d_1} \bmod n_2 \equiv key^{e_2d_1} \bmod n_2 \equiv key^{e_2d_2} \bmod n_2 \equiv key$$

所以,一级管理人员可以通过解密二级管理员保留的密文 c_{key} 恢复对称密钥.

一级管理人员在恢复 key 后,可以利用 DES 解密二级密文,从而获得二级信息 $m = \mathrm{DES}^{-1}(key, c_m)$.

下面证明二级管理人员无法解密一级信息. 一级信息的密文为 $c = m^{e_1} \bmod n_1$. 由于二级管理人员仅仅掌握二级密钥 (e_2,n_2),(d_2,n_2). 而 $e_1d_1 = 1 \bmod \varphi(n_1)$,$d_2 < d_1$,故 $e_1d_2 \neq 1 \bmod \varphi(n_1)$. 因此 d_2 无法用作一级信息密文的解密密钥. 同时,由于二级管理人员不掌握一级解密密钥 d_1,不知道 n_1 的完全分解,鉴于 RSA 的安全性,故其无法解密在模数 n_1 下的一级密文 c.

2　算法安全性与有效性分析

本文通过利用 RSA 加密和解密算法,以及对称加密算法 DES,给出数字图书馆信息分级加密算法的构造.

笔者已分析证明了一级管理员可以解密浏览一级信息和二级信息,而二级管理员只能解密浏览二级信息. 由于其他人员不掌握密钥,因而无法解密. 在一级加密和解密中,采用了 RSA 算法,仅用于对少量的一级信息进行加密和解密,无需过多的计算. 在二级加密和解密过程中,RSA 算法仅用于对对称密钥 key 进行加密和解密,无需大量的计算耗

费;DES 算法用于对大量的二级信息进行加密和解密,而相对于公钥算法而言,对称算法 DES 恰好适用于对大量数据进行加密和解密,从而保证二级加密和解密的有效性.

目前,RSA 和 DES 已在商业和相关行业中获得广泛应用,其安全性和有效性已经得到了普遍认可. RSA 算法的安全性主要基于大数分解的困难性. 目前,还未发现对 RSA 密码体制 1 024 bit 或更大的模数进行有效分解的算法. 而在本文所采用的 RSA 算法中,所采用的 RSA 模数 n_1 和 n_2 分别为 2 048 bit和 1 024 bit,因此其具有较好的安全性. 同时,文中 RSA 算法仅用于对少量一级信息或对称密钥 *key* 进行加密和解密,而非用于对大量的明文进行加密和解密. 因此,文中采用的 RSA 算法所耗费的计算量并不大,其在实践中具有有效性. DES 算法具有极高的安全性,到目前为止,除了用穷举搜索法对 DES 算法进行攻击外,还没有发现其他更有效的办法. 在 DES 算法中,根据国际标准,目前,对于一般的安全要求,可以取 *key* 为 64 bit 的密钥. 由于 DES 算法具有多轮重复性,因此它很容易利用硬件技术来实现,并具有有效性.

3 结语

本文根据数字图书馆不同用户的安全需求及保密性需要,将数字图书馆信息划分 3 个等级:一级信息、二级信息和公开信息. 对于公开级信息,无需进行保密. 为保障数字图书馆系统的安全运行和管理,对一级和二级信息,需要进行秘密保护. 采用 RSA 加密算法对一级信息进行加密和解密,而对于大量的二级信息,先采用 RSA 对二级对称密钥进行加密,然后用对称密钥对二级信息进行加密和解密. 一级管理员可以解密浏览一级信息和二级信息,而二级管理员只能解密浏览二级信息. 根据 RSA 对解密密钥的安全依赖,其他人无法解密. 这种分级管理不仅适应数字图书馆不同用户的安全需求,而且便于不同级别用户对保密信息进行分级管理.

参考文献:

[1] 李媛. 近五年来数字图书馆信息安全问题研究综述[J]. 图书馆学研究,2005(12):10.

[2] 杨清兰. 基于身份的数字签名在数字图书馆中的应用[J]. 郑州轻工业学院学报:自然科学版,2013,28(2):100.

[3] 张海波,黄铁军. 数字化图书馆信息安全保障体系的研究[J]. 现代图书情报技术,2004(S1):1.

[4] 王召龙,许军振. 数字图书馆的信息安全[J]. 济南职业学院学报,2005(4):69.

[5] 刘超. 数字图书馆的信息安全分析[J]. 现代情报,2009,29(6):72.

[6] 郑德俊,任妮,熊健,等. 我国数字图书馆信息安全管理现状[J]. 现代图书情报技术,2010(7/8):27.

[7] 杨木锐. 数字图书馆信息安全保障体系研究[D]. 长春:东北师范大学,2007.

[8] 宋维平. RSA 密码体制的数字签名[J]. 长春理工大学学报:自然科学版,2005,28(2):120.

[9] 张先红. 数字签名原理及技术[M]. 北京:机械工业出版社,2004.

[10] Rivest R L, Shamir A, Adelman L. A method for obtain digital signatures and public-key cryptosystem[J]. Communications of the ACM,1978,21(2):120.