第17卷 第1期
2007年1月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 17 No. 1
Jan. 2007

基于RSA公钥密码安全性的研究

曹建国,王 丹,王 威
(西南交通大学 信息科学与技术学院,四川 成都 610031)

摘 要:RSA是目前最重要的公开密钥密码算法之一。文中介绍了该算法的实现、基本原理等,重点是对其攻击方法和安全性进行分析,相应给出了防止攻击的方法。通过对RSA密码特点以及目前的密码技术发展形势分析,RSA在将来相当一段时期内依旧是应用最广泛的密码算法之一。

关键词:RSA密码算法;公开密钥密码体制;安全性;攻击
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)01-0172-02

The Research on Security of RSA Public-Key Cipher

CAO Jian-guo, WANG Dan, WANG Wei
(College of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: At present RSA is one of the most important public-key cipher algorithms. The realization and the basic principle of it are described in the paper, in addition, the ways of attack and the security are also analyzed in detail. Some ways are given to prevent from attacking. In terms of the analysis of RSA' characteristic and current situation in cryptography, RSA will remain the position Which as one of encryption algorithms widely used in quite a long time.

Key words: RSA cipher algorithm; public-key cipher system; security; attack

0 引 言

计算机网络技术的飞速发展极大地改变了人们的生活,促进了社会的发展。随着网上办公、网上购物、网上银行、网上证券等的日益推广和普及,信息保密和网络安全就显得尤为重要。在保障信息安全的诸多技术中,密码技术无疑是信息安全的核心和关键技术,通过数据加密技术,可以在很大程度上提高数据的机密性,保证传输数据的确定性和完整性,防止被篡改、伪造和假冒。

密码技术中,密钥是密码体制的关键。公开密钥密码体制是由Diffie和Hellman于1977年提出,它使用不同的加密密钥和解密密钥,是一种由已知加密密钥推导出解密密钥,这种密码体制在计算上是不可行的。公开密钥体制的产生主要是为满足常规密钥体制中密钥分配和数字签名的要求。由Rivest,Shamir和Adleman联合提出了一种基于数论中欧拉定理的公钥密码系统,简称RSA公钥系统,其安全性是基于大数因子分解[1]。目前,它在数学上是一个困难问题。RSA算法既能用于数据加密,也能用于数字签名,其理论依据为:寻找两个大素数比较简单,而将它们的乘积分解开则异常困难。

收稿日期:2006-04-10

作者简介:曹建国(1979-),男,湖北荆州人,硕士研究生,研究方向为密码算法的FPGA实现、EDA技术与应用、集成电路设计等;王丹,副教授,研究方向为EDA技术与应用、COMS集成电路设计。

1 RSA公钥密码简介

RSA体制用户 i 的公开加密变换 E_i 和保密的解密变换 D_i 的产生:(1)随机选取两个100位(十进制)以上的素数 p_i 和 q_i;(2)计算 $n_i = p_i q_i$, $\Phi(n_i) = (p_i - 1)(q_i - 1)$;(3)随机选取整数 e_i 满足 $(e_i, \Phi(n_i)) = 1$;(4)利用欧几里得算法计算 d_i,满足 $e_i d_i \equiv 1 \bmod \Phi(n_i)$;(5)公开 n_i, e_i 作为 E_i,记为 $E_i = < n_i, e_i >$,保密 p_i, q_i, d_i, $\Phi(n_i)$ 作为 D_i,记为 $D_i = < p_i, q_i, d_i, \Phi(n_i) >$。

加密算法:$c = E_i(m) = m_i^e (\bmod\ n_i)$

解密算法:$m = D_i(c) = c_i^d (\bmod\ n_i)$

在RSA算法中,包含两个密钥:加密密钥PK和解密密钥SK,加密密钥公开。

2 RSA参数的选取

要选用足够大的 n,就要产生足够大的素数 p 和 q,一般应在 $10^{100} \sim 10^{150}$,这样可以基本保证不会在有效时间内被密码分析人员译出参数。这个问题在理论上很好解决,利用计算机产生100多位的素数也并不困难。同时,它们必须是随机数并且不包含在素数表中[2]。

其次,两个素数不能太接近。当 p 和 q 的大小很接近时,n 就容易分解。因为 $n = pq = (p+q)^2/4 - (p-q)^2/4$,当 $(p-q)/2$ 较小时,$t = (p+q)/2$ 和 $\sqrt{n}$ 很接近,只比 $\sqrt{n}$ 稍大一点,因此逐个检查大于 $\sqrt{n}$ 的整数 x,直到找到一个,使得 $x^2 - n$ 是一个平方数,记为 y^2,则 $p = x +$

$y, q = x - y$。一般说来,选择 p 和 q 使其二进制表示的长度有几比特不同即可。

3 RSA 公钥密码攻击方式的分析

3.1 RSA 公钥密码的选择密文攻击

选择密文攻击指的是密码分析者可以选择不同的待解密的密文,并且可以得到被加密的明文。破译者的工作是推出密钥。一些攻击是针对 RSA 公钥密码的使用过程的,而不是攻击基本算法。

方案一:E 窃听 A 的通信过程,并设法收集到一个用他的公钥进行的 RSA 加密的密文 c,E 想读出明文。从数学上讲,也就是想得到 m,即

$$m = c^d$$

为恢复出 m,E 首先选取一个小于 n 的随机数 r,并得到 A 的公钥 e,然后计算

$$x = r^e \bmod n \quad y = xc \bmod n \quad t = r^{-1} \bmod n$$

如果 $x = r^e \bmod n$,则 $r = x^d \bmod n$。然后 E 让 A 用他的私钥对 y 签名。注意,以前 A 从未见过 y,A 将 $u = y^d \ mod\ n$ 发给 E。最后,E 计算

$$tu \ mod\ n = r^{-1}y^d \ mod\ n = r^{-1}x^d c^d \ mod\ n = c^d \ mod\ n = m$$

于是 E 就获得 m。

方案二:T 是一个公开的可信的第三方,如果 A 想公证一份文件,便将它发给 T,T 将文件进行 *RSA* 数字签名并发送回去,这里没有使用单向 *hash* 函数,T 用他的私钥加密整个文件。

如果 B 想让 T 对一个他本不愿意签名的文件签名,即该文件为 m'。首先,B 任选一个值 x,并计算 $y = x^e \ mod\ n$,因为 e 很容易得到,它是 T 的公钥,必须公开以便用来验证他的签名。然后 B 计算 $m = y\,m' \ mod\ n$,并将 m 送给 T 签名。T 将 $m^d \ mod\ n$ 送回。现在 B 计算 $(m^d \ mod\ n) \cdot (x^{-1} \ mod\ n) \equiv m'^d \ mod\ n$,这就是 m' 的签名。

因为 $(m^d \ mod\ n) \cdot (x^{-1} \ mod\ n) = (y^d \ mod\ n) \cdot (m'^d \ mod\ n) \cdot (x^{-1} \ mod\ n) = (x \ mod\ n) \cdot (m'^d \ mod\ n) \cdot (x^{-1} \ mod\ n) = m'^d \ mod\ n$,

以上所利用的弱点就是指数运算保持了输入的乘法结构,即

$$(xm)^d \ mod\ n \equiv x^d m^d \ mod\ n$$

方案三:E 想让 A 对 m_3 签名,它产生两份信息 m_1,m_2,使得

$$m_3 \equiv m_1 m_2 \ mod\ n$$

如果 E 能对 m_1,m_2 签名,则能计算 m_3 的签名,即

$$m_3^d \ mod\ n \equiv (m_1^d \ mod\ n)(m_2^d \ mod\ n)$$

通过对以上攻击算法的分析,不难得到一个教训:即绝对不要对一个陌生人提交给你的随机文件签名,同时总要使用一个单向的 hash 函数。只有这样,才能有效防止 RSA 公钥密码的选择密文攻击。

3.2 对 RSA 公钥密码的共模攻击

在 RSA 公钥密码的实现中,为简化问题,可以采用给每个人相同的 n 值,但不同的指数值 e 和 d。不幸的是,这样做是不可行的。如果一个信息用两个不同的指数(具有相同的模)加了密,这两个指数是互素的,则不需要任何解密密钥就能恢复出明文。

设 m 是明文,两个加密密钥分别是 e_1,e_2,共同的模是 n,两个密文分别为

$$c_1 = m^{e1} \bmod n$$

$$c_2 = m^{e2} \bmod n$$

密码分析者知道 n,e_1,e_2,c_1 和 c_2。由于 e_1 和 e_2 是互素的,由扩展的 Euclidean 算法可以找出 r 和 s,使之满足

$$re_1 + se_2 = 1$$

假设 r 是负数(r 或 s 必有一个为负数,不妨设 r 为其中的负数),再次使用 Euclidean 算法可计算出 c_1^{-1},故可得到 $(c_1^{-1})^{-r} c_2^s \equiv m_1^{re} m_2^{se} \equiv m \bmod n$。

3.3 对 RSA 公钥密码的加密及签名攻击

数字签名是一种以电子形式存储的消息签名方法。正因为如此,签名之后的消息能通过计算机网络传输。一个数字签名方案包括两部分:签名算法和验证算法。在对一个信息加密之前对它进行签名是一种常识,但并不是每个人都按此执行。下面给出了一个对先加密,后签名的 RSA 签名算法的攻击。

A 要发送信息 m 给 B,首先他用 B 的公钥,记为 e_B 对其加密,然后再用他的私钥 d_A 进行签名,用 n_A,n_B 表示他们各自的模,A 加密后再签名的信息为

$$(m_B^e \bmod n_B)^d A \bmod n_A$$

因为 B 知道 n_B 的因子分解,因为其因子为 B 的私钥,所以他能计算对应于 n_B 的离散对数。即 B 能找到满足 $m'^x \equiv m \bmod n_B$ 的 x,然后,他可以公开 xe_B 作为他新的公钥,n_B 还为他的模,这样他就能断言 A 送给他的是用新指数加了密的 m'。这种情况的攻击很难对付,比较好的解决方法是强制每个用户使用一个固定的加密指数。

4 RSA 公钥密码的安全性探讨及发展前景

(1)RSA 公钥密码体制在加密和解密变换中存在大量的数值运算,其加密和解密运算时间比较长,开销更大,在某种程度上限制了其应用范围。

(2)由于数学方法的进步和计算机技术的飞速发展,RSA 公钥密码的破译能力也逐渐增强。破解 RSA 密码,实际中普遍采用二次筛选方法分解 n。1994 年,RSA-129(129 位十进制)被成功分解,它耗去了由世界各地 600 多个研究人员贡献的 5000MIPS 年的计算时间。RSA-155 的分解在 1999 年完成。尽管如此,RSA 依然是当今使用最为广泛的密码算法,安全性较高[3]。

(3)由于产生密钥很麻烦,受到素数产生技术的限制,因而很难做到一次一密。

(4)公钥密码的优点是适应网络开放性的要求,且密钥管理比较简单,但是算法复杂,加密数据速率较低。

(下转第 176 页)

新实例时,需要重新计算原训练集 D 中每个元素的新类型支持概率 θ' 值,有了额外的时间开销,时间开销为 $N(\sum_{i=1}^{m}[(n+i)(m-i)])$ 级。在空间和时间的额外开销方面,都在可接受范围,所以该算法是可行的。

在增量学习算法中,反复用训练数据检验,这使得样本实例属性值之间的条件相关性不断弱化,减小其负面影响。因而,在朴素贝叶斯分类算法的基本限制和明显缺陷方面,增量学习算法都对其有不错的完善。

5 结束语

如何改善朴素贝叶斯分类算法,提高其在入侵检测系统中的性能,仍然是目前一个比较重要的课题。除了文中所述的方法外,还有很多诸如贝叶斯分类算法与决策树结合[3]、贝叶斯分类算法与信念网络结合[1]等等的方法。但各种方法不是降低实例属性值之间的条件依赖程度,就是提高用先验知识来预测后验数据的准确率。增量学习策略是一种相对简便实用的弥补方法,而怎样选择新实例加入到训练集 D 中,更好地完备训练集 D 来改善文中算法,仍然值得做深入的研究工作。

参考文献:

[1] Lee Wenke, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Models[C]//Proceedings of the 1999 IEEE Symposium on Security and Privacy. Los Alamos, CA: IEEE Computer Society Press, 1999: 120 - 132.

[2] Firedman N, Geiger D. Bayesian network classifier[J]. Machine Learning, 1997, 29: 103 - 130.

[3] 张王番. 多种策略改进朴素贝叶斯分类器[J]. 微机发展, 2005, 15(4): 35 - 37.

[4] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范 明, 孟小峰, 等译. 北京: 机械工业出版社, 2005.

[5] 张 琨, 徐永红, 王 珩, 等. 用于入侵检测的贝叶斯网络[J]. 小型微型计算机系统, 2003, 24(5): 913 - 915.

[6] Yager R R. An extension of the naive Bayesian classifier[J]. Information Sciences, 2006, 176: 577 - 588.

[7] 宫秀军, 刘少辉, 史忠植. 一种增量贝叶斯分类模型[J]. 计算机学报, 2002, 25(6): 645 - 650.

(上接第 171 页)

该系统针对不同的领域配以不同的应用软件,可应用于远程网络数据库的访问权限及身份的确认、银行储蓄防冒领及通存通兑的加密方法、保险行业中投保人的身份确认、期货证券提款人的身份确认、医疗卫生系统中医疗保险人的身份确认等领域。可以说,指纹识别技术实现了身份鉴定领域的世纪革命,解决了困扰身份识别多年的问题。

4 结束语

随着硬件技术的提高和互联网的广泛应用,指纹身份认证系统的开发和应用将得到进一步的拓宽,指纹身份认证的普及应用指日可待。

参考文献:

[1] 戴平阳. 指纹识别技术研究进展[J]. 厦门大学学报: 自然科学版, 2002, 41(6): 750 - 755.

[2] 卢朝阳, 张岗山, 刘 琳. 指纹识别系统性能评价方法[J]. 西安电子科技大学学报: 自然科学版, 2002, 29(6): 804 - 808.

[3] 于秀霞. 指纹识别技术及其应用[J]. 长春大学学报, 2005, 15(2): 30 - 32.

[4] 李海雄, 刘国清. 活体指纹识别系统及其应用[J]. 计算技术与自动化, 2003, 22(4): 68 - 70.

[5] 刘 旭, 田 捷. 自动指纹识别算法在嵌入式系统上的实现[J]. 计算机工程与应用, 2002(21): 120 - 124.

(上接第 173 页)

(5)分组长度太大,为保证安全性, n 至少也要 600 bits 以上,使运算代价很高,尤其是速度较慢,较对称密码算法慢几个数量级;且随着大数分解技术的发展,这个长度还在增加,不利于数据格式的标准化[4]。

5 结 论

主要对公钥密码 RSA 算法的安全性、攻击方法进行了探讨和分析,并对 RSA 的发展前景进行了简单介绍。在公开的密钥加密算法中,RSA 已经作为标准几乎在各种信息安全需求中给出很好的解决方案,其最大的优点是密钥空间大,缺点是长密钥带来巨大的计算量,导致加密速度慢。随着解密方法的进步和计算硬件技术的不断发展,RSA 算法应用显得越来越笨拙。RSA 加密算法是目前应用最广泛的公钥加密算法,特别适用于通过 Internet 传送数据[5]。不管怎样,RSA 算法还是会在将来很长一段时间继续成为公开密钥加密算法的主流。

参考文献:

[1] 朱文余, 孙 琦. 计算机密码应用基础[M]. 北京: 科学出版社, 2003.

[2] Stinson D R. 密码学原理与实际[M]. 冯登国译. 北京: 电子工业出版社, 2003.

[3] Menezes A J, van Oorschot P C. 应用密码学手册[M]. 胡磊等译. 北京: 电子工业出版社, 2005.

[4] 周玉洁, 冯登国. 公开密钥密码算法及其快速实现[M]. 北京: 国防工业出版社, 2002.

[5] Spillman R. 经典密码学与现代密码学[M]. 叶阮健等译. 北京: 清华大学出版社, 2004.