RSA数字签名解决短信欺骗

高雪寒
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:手机作为当今信息和文化传播不可缺少的媒介,尤其是智能手机对我们的教育、文化、科技、生活等有很大影响。手机提供的各种软件功能也纷纷出世,其中短信息的功能在通信中的利用率占有主导地位。由于手机短信的成本低、限制少、缺少管理和监督等特点,从而造成现在由短信产生的各种诈骗事件越来越多,文中以运用广泛的RSA数字签名来对手机短息在网络传播过程中造成的欺骗进行保护,并介绍了RSA数字签名在移动终端上的实现,同时对运用RSA数字签名的过程中的安全问题进行讨论和分析。

关键词:RSA;数字签名;短信欺骗
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)01-0161-04
doi:10.3969/j.issn.1673-629X.2013.01.040

RSA Digital Signatures to Solve SMS Spoofing

GAO Xue-han
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Mobile phone as an indispensable medium of today's information and cultural transmission, especially smart phones have a great impact on education, culture, science, life and so on. All kinds of mobile phones provide software functions have been born, and messaging functions in which the utilization play a dominant role. Because of the SMS of low cost, less restricted, lack of management and supervision, thus result in a variety of fraud generated by the SMS. With the wide use of RSA digital signatures protect the deception of the SMS in the communication process on network. And introduce the RSA digital signature in the mobile terminal realization. At the same time to use digital signatures in the process of the RSA security problems are discussed and analyzed.

Key words: RSA; digital signature; SMS spoofing

0 引 言

随着科学技术的迅猛发展,各式各样的手机已经进入了千家万户,手机中的软件功能也在不断地增加和完善,并逐渐向智能化发展。在这科技发展迅速的时代,手机已经成为了最简单最方便,也是人们日常生活中最常见的传达信息的工具。通信过程中的双方身份的相互认证、信息的完整性鉴别等存在很多网络安全方面的问题。而其中手机短信造成的安全问题很大,通信者之间发送短信和打电话具有不同的责任,但是由于短信的过程不用听到或看到对方,避免了一些不必要的尴尬,同时也给不少不法分子提供了方便来钻空子,他们利用短信的这个缺点和短信的方便、快捷、成本低等特点给很多用户群发欺骗短信。一直强调人们要高度警惕此类欺骗短信,短信只要是由陌生手机号码发来,一定要谨慎再谨慎,就是熟悉的号码发来的内容关乎到银行卡、密码等信息的时候,也需要通过别的途径确认以后再选择是否可信再做行动。但是为什么还有那么多人成功被骗呢?这其实是个概率问题,假若一次群发给100个对象,短信内容只涉及到300元的诈骗活动,在这100个对象当中假设只有百分之一的对象相信了短信的内容,也就是一个人相信的情况下:100条短信只需要投资10元钱,一个人上当就有300的回报,这"利润"得多高啊,想想就知道为什么干这行的越行越多。文中主要用RSA数字签名来解决短信欺骗的问题,现在无论移动、联通还是电信,为了实现信息的安全保障,安全系统都是以个人的身份证号码来证明该用户的身份,不管一个人同时使用几个号码,这几个号码都对应他一个人的身份证号码。所以安全机构可以按照每个身份证号码给该用户分配一个密钥对(一个公开的公钥Pa和保密的私钥Ka),运用RSA数字签名实现身份认证。发送短信者用自己的私钥Ka给信息内容签名来证明自己的身份,而接收短信者可以用对方的公钥Pa验证其身份,

收稿日期:2012-04-26;**修回日期**:2012-07-27
基金项目:国家自然科学基金资助项目(61070189)
作者简介:高雪寒(1988-),女,硕士,研究方向为网络与信息安全;导师:李顺东,教授,研究方向为密码学与信息安全。

这样就会知道发送短信的是什么人,从而大大减少或避免通过短信方式来欺骗用户。然而在手机这种计算资源较弱的环境下进行数字签名,签名算法的运行速度已经远远超出了人们可以忍受的限度,这样就没有什么使用价值了,所以之后介绍了通过中国剩余定理对 RSA 签名算法进行简化计算、预处理等来缩减签名算法的运行时间[1]。

数字签名验证身份系统包括发送者、接收者、智能卡或者认证第三方这三个部分。

身份验证流程:

(1)由智能卡或认证第三方机构给每个用户产生一个证书,证书当中有该用户的密钥对,包括用户自己的公开密钥 Pa 和私钥 Ka。一般数字证书的内容包括证书的版本信息、证书的序列号,每个证书都有一个唯一的证书序列号、证书所使用的签名算法、证书的发行机构名称、证书的有效期,现在通过的证书一般采用 UTC 时间格式、证书所有人的名称,命名规则一般采用 X.500、证书所有人的公开密钥、证书发行者对证书的签名[2]。

(2)发送者首先将想传达给接收者的短信内容 M 经过自己的私钥 Ka 加密后形成数字签名 S,然后将短信 M 和签名 S 一起发送给接收者。

(3)接收者将接收到的签名 S 用发送者的公开密钥 Pa 解密,便可以得到发送者的身份,即进行了对发送者的身份的认证。

1 RSA 数字签名在移动终端上的实现

在手机该移动终端上实现 RSA 数字签名首先需要面临的问题是公开密钥对是如何产生的,然后再进行签名和身份验证等一系列操作。文章前面说过数字签名算法的计算过程相对有些复杂,对于在前些年手机的性能不够高的情况下,从多方面限制或阻碍了数字签名在手机中的应用与实现。现在大多数智能手机的系统处理能力在不断地加强,同时手机平均内存都不断地加大,已经具备了实现数字签名的能力。

1.1 移动终端上实现数字签名

该数字签名技术可以由认证第三方或者由智能卡直接产生密钥对,公钥对的生成和签名的过程都能够在智能卡上进行[2]。终端通过机卡的接口调用卡中的 PKI 功能,并且选择在卡上实现数字签名有以下优点:

(1)在卡上生成的公共密钥对、私钥和证书将一直保留在卡上,以此来确保密钥对的安全和隐私。

(2)运营商可以将一些应用直接开展到卡上,大大地提高用户对应用的依赖程度。

(3)避免了适配不同的平台问题,方便于实现证书的统一发放[3]。

数字签名在手机移动终端中实现的框架见图 1:

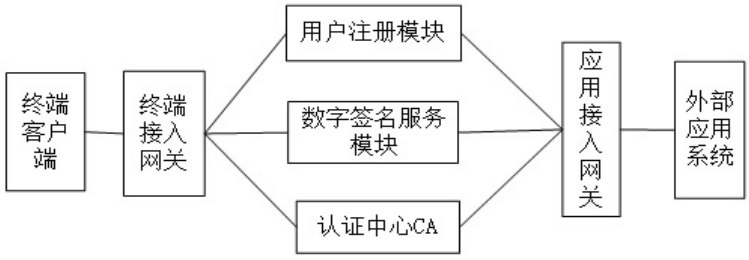

图 1 移动数字签名系统

1.2 手机数字签名系统

需要实现的是通信过程中的身份认证、信息完整性和机密性的保护,以及不可否认性等组件的系统,该系统以 PKI 技术和公钥密码体制为基础来实现[4]。

该移动数字签名系统由以下几部分构成:

(1)终端客户端。

终端客户端的性质其实就是在用户手机卡上安装一个 JAVA 程序,运营商开展不同的 SIM 卡的发展和应用。公私钥对的生成是在 SIM 卡上进行,并实行数字签名与签名的验证,客户端支持对称密钥加解密。

(2)终端接入网关。

终端接入网关是提供给手机客户端和签名服务系统的网关,从而给签名服务系统和手机客户端提供统一的通信信道。

(3)用户注册模块。

用户注册模块以提供最终用户的注册、密钥生成、证书生产和证书的生命周期管理,支持在多协议的基础上使用不同证书用户的目的、用户需求借口整合、管理用户和用户信息。

(4)数字签名模块。

应用服务提供商和最终用户提供移动数字签名和移动用户身份验证服务,移动数字签名服务请求者提供一个简单易于使用的标准的服务数字签名模块和接口通信,移动签名客户端程序处理并核查、验证数字签名和用户证书。

(5)认证中心。

认证中心提供证书的发放、撤销、终止和证书生命周期管理、信用管理、提供时间戳服务、认证服务等。

(6)应用接入网关。

应用接入网关是签名服务系统与外部应用系统的移动签名服务网关。

2 数字签名介绍

2.1 数字签名

数字签名也称为公钥数字签名,是手写版签名的电子相对应物,主要用于防止信息被篡改或者伪造、对

消息进行签名认证等。同时可以用来鉴别通信双方的身份[4]。根据数字签名的实现原理来看,数字签名就是附加在信息数据上的一些经过形式转换的数据单元。这些附加的信息单元的作用就是让接收者来确认所接收到的数据的来源,同时也可以确保数据信息的完整性和防止接收者或其他人进行伪造信息。将 RSA 数字签名运用在手机数字签名中,从而可以实现移动业务中所要求的数据完整性、身份认证及不可否认性。

手机用户 A 在给用户 B 发送信息的过程中证明自己的身份,用户 A 先用自己的私钥 Pa 对信息 M 进行数字签名,然后以级联的形式将 M 和得到的签名数据发送给用户 B。用户 B 再通过用户 A 的公开密钥 Ka 来验证用户 A 的身份,当然,用户 B 收到某些信息也许根本不需确认发送者是谁,收到信息后也就无需再经过用户 A 的公开密钥 Ka 进行身份确认了[5]。

数字签名的过程如下:

(1)用户将使用自己的私钥进行对数据的加密处理和对数据的合法签名。

(2)接收数据的用户则用发送数据的用户的公钥对收到的签名进行验证,以确认签名的合法性[6]。

数字签名的流程见图 2。

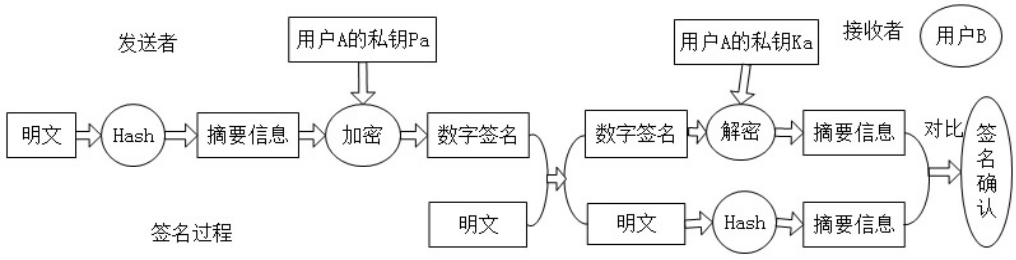

图 2　数字签名流程

2.2　公钥密码体制

公钥加密体制就是加密、解密用的是不同的密钥,并且由已知加密密钥推导出解密密钥在计算上是不可行的。公钥加密算法同时被称为非对称加密算法,一对密钥包括一个公共密钥和一个专有密钥。为了保证个人的私钥不会被泄露,用户要保证个人的私有密钥不被泄露,公共密钥则公布给大家[5]。公钥与私钥有着密切的关系,用公钥加密的信息只能用相应的私钥解密,反之亦然。因为公共密钥加密算法并不需要与密钥服务器联机,并且密钥分配协议相对简单,所以很大程度地简化了对密钥管理的复杂性。公共密钥系统可以实现加密功能也可以在同一时间实现数字签名。公钥密码体制中,加密密钥是公开信息,而解密密钥是必须保密的。加密算法和解密算法是向公众开放的。虽然私有密钥是由公开密钥决定的,但逆向计算却是不可行的,也就是根据计算出是难计算的[6]。

RSA 算法在公钥加密算法中是最常用的。RSA 算法中需要使用两个密钥,一个公钥、一个私钥。如用其中一个用来加密信息,则另一个就可以用来解密,加解密密钥长度分布于 40 至 2048 比特之间,加密过程中通常将明文分成大小可变的块,但分成块的长度不得超过密钥的长度,需要注意的是:“RSA 算法实现中把每一块明文转化为与密钥长度相同的密文块,密钥越长,加密效果越好,但加密解密的开销也大、难度也大,所以要在安全与性能之间考虑折衷,一般选择 64 位是较合适的”。

RSA 被发现的初始目标是使互联网变得更加安全可靠,同时也为了解决私有密钥在实现 DES 算法的时候需要使用公开信道传输的问题。RSA 算法解决问题的结果不但很好地解决了 DES 的这个难题,还可以通过 RSA 算法实现数字签名的电子版本,并且可以抵抗对电子数据的否认与抵赖,同时还可以利用数字签名较容易地发现攻击者对电子数据的非法篡改,以保护数据信息的完整性[7]。

一般信息安全的目标可以概括为以下几点需要解决的问题:

保密性(Confidentiality):以确保信息本身不被未经授权的人泄露。

完整性(Integrity):以防止未经授权的人对信息本身进行非法的篡改。

可用性(Availability):用来保证信息本身和信息系统确实是为授权者所用。

可控性(Controllability):对信息本身和信息系统实施安全监控,防止非法分子利用该信息或信息系统[7]。

2.3　RSA 数字签名

RSA 算法主要分为三部分:公钥和私钥的产生、非对称加密和解密、数字签名和验证,下面介绍 RSA 算法的工作原理:

(1)选取两个大素数 p、q,计算 $n = p * q$ 与 $\varphi(n)$;

(2)选取整数 e,$1 < e < \varphi(n)$,且 $\gcd(e,\varphi(n)) = 1$;

(3)计算 $d = e^{-1} \bmod \varphi(n)$,其中 e 为公钥,d 为私钥,m 是作为签名的明文;

签名过程:$s = H(m)^d \bmod n$;

验证过程:$H(m) = s^e \bmod n$。

通常 s^e 和 n 的值都非常大,直接进行 $s^e(\bmod n)$ 类型的计算对于高级计算机不是什么问题,但对于手机

来说却出现较大的问题,需要的时间太长,因此可以根据中国剩余定理对 RSA 签名算法进行简化计算[8]。

2.4 中国剩余定理简化计算 RSA 签名算法

(1)中国剩余定理。

设 $m_1, m_2, \cdots, m_n$ 是两两互素的正整数,且 $i \neq j$ 时 $\gcd(m_i, m_j) = 1$

给定 n 个整数 $b_1, b_2, \cdots, b_n$,同余式组

$X = b_i (\mathrm{mod} m_i)$, $i = 1, 2, \cdots, n$

有唯一解:

$X = M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 + \cdots + M_n M_n^{-1} b_n (\mathrm{mod} m)$

其中 $m = m_1 m_2 \cdots m_n$, M_i 满足 $m_i M_i = m$

又 M_i^{-1} 对模 m_i 的逆元

即 $M_i M_i^{-1} \equiv (\mathrm{mod} m_i)$ [9]

(2)用中国剩余定理对 RSA 签名算法作简化计算。

利用中国剩余定理对 $H(m) = s^e \mathrm{mod} n$ 作简化计算可写[10]:

$$X = H(m) = s^e (\mathrm{mod} pq) \tag{1}$$

因为 p、q 是互素的,所以满足中国剩余定理的求解条件,求一次同余式(1)中的 X,就可以通过求解如下一次同余式组来得到:

$$\begin{aligned} X &= s^e (\mathrm{mod} p) \equiv b_1 (\mathrm{mod} p) \\ X &= s^e (\mathrm{mod} q) \equiv b_2 (\mathrm{mod} q) \end{aligned} \tag{2}$$

根据中国剩余定理,一次同余式组(2)的解可表示为[11]:

$$X \equiv M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 (\mathrm{mod} n) \tag{3}$$

其中, $M_1 M_1^{-1} \equiv 1 (\mathrm{mod} p)$, $M_2 M_2^{-1} \equiv 1 (\mathrm{mod} q)$

从以上分析中可以看出,用户 A 要对发送信息 M 数字签名,即要求解(2)式,就可以转化为求(3)式。

值得提醒的是手机用户在拥有公钥对后保存好敏感参数 p、q 等。当密钥对产生后参数 p、q 已经固定,那么就可以预先计算参数 M_1、M_1^{-1}、M_2、M_2^{-1} 等,并将结果保存在手机中,方便以后的计算,同时也大大减小了计算量[12]。

3 结束语

当如今的通信技术类业务在近年来发展如此迅速的情况下,网络中的安全问题依然还是制约很多技术发展的重要原因之一。在随网络技术的普及的时候同时使得人们对网络的依赖程度加大,对网络的破坏造成的损失和混乱会比以往任何时候都大。这也就使得需要对网络安全做更高的要求,也使得网络安全的地位将越来越重要,网络安全必然会随着网络应用的发展而不断发展。

文中内容主要是以 RSA 数字签名应用于移动手机系统,从而使得手机用户对信息的传达的使用更加放心,依赖程度加强。文章首先对日常生活中频繁遇到的短信欺骗事件提出问题,然后选择常用的 RSA 数字签名算法来解决该问题。介绍了数字签名、公钥密码体制、RSA 数字签名的过程,尤其对接收到的短信息的身份认证过程进行了详细的介绍。通过分析 RSA 签名算法和数字签名的概念[13],以及中国剩余定理简化 RSA 数字签名的计算,可以对签名算法简化后大大影响其在手机环境中的运行速度。从文中分析的在手机这样的弱计算资源环境下提高数字签名在手机上的运行速度可以从中国剩余定理对 RSA 算法的简化和预先计算一些将来会用到的参数来入手。并且在文章的最后提出一点:可以将混沌密码用于移动系统中的数字签名中,在发送信息的过程中将有关数字签名和自己的混沌密码以级联的形式一起发送目的地[14],由于混沌密码的特点是动态的,每次都会在变化,因此可以进一步保证手机用户数字签名的安全。

参考文献:

[1] Prentice Hall PTR. Modern Cryptography:Theory and Practice[M]. 王继林译. 北京:电子工业出版社,2004.

[2] 黄友谦,黄东斌. 网络安全与密码技术[M]. 香港:博士苑出版社,2002.

[3] 杨义先,李名选. 网络信息安全与保密[M]. 北京:北京邮电大学出版社,1999.

[4] Burnett S,Paine S. 密码工程实践指南[M]. 冯登国译. 北京:清华大学出版社,2001.

[5] Greenstein M,Feinman T. Electronic Commerce:Security Risk Management and Control[M]. [s. l.]:Mcgraw Hill Higher Education,1999.

[6] 蔡庆华,姚 晟. 公钥密码体制 RSA 算法[J]. 安庆师范学院学报:自然科学版,2003(4):69-70.

[7] 李克洪,王大玲,董晓梅. 实用密码学与计算机数据安全[M]. 沈阳:东北大学出版社,2001.

[8] Davis C R. IPSec:VPN 的安全实施[M]. 周永彬译. 北京:清华大学出版社,2002.

[9] Mao Wenbo. 现代密码学理论与实践[M]. 王继林,伍前红译. 北京:电子工业出版社,2004.

[10] Blakley G R. Safeguarding crytographic keys[C]//Proc of National Computer Conference. [s. l.]:[s. n.],1979:313-317.

[11] 杨义先,孙 伟,钮心忻. 现代密码新理论[M]. 北京:科学出版社,2002.

[12] 潘承洞,潘承彪. 简明数论[M]. 北京:北京大学出版社,1998.

[13] 周福才,朱伟勇. 基于混沌理论身份认证的研究[J]. 东北大学学报(自然科学版),2002(8):730-732.

[14] 余东明,齐文静. 浅谈基于 RSA 的数字签名及其应用[J]. 福建电脑,2008(10):69-69.

RSA 数字签名解决短信欺骗

作者：高雪寒
作者单位：陕西师范大学 计算机科学学院,陕西 西安 710062
刊名：计算机技术与发展
英文刊名：Computer Technology and Development
年，卷(期)：2013(1)