数字签名技术在网络安全防护中的应用研究

徐霁桐

（南京市栖霞区妇幼保健所，江苏 南京 210046）

摘 要 网络技术的飞速发展使网络的运行更加的复杂，在极大地方便了人们的生活和工作的同时，也带来了许多的安全问题。因此，加强对网络的保护是非常必要的。其中，以数字签字技术最为普遍，它可以有效地改善网络的安全性，并能很好地适应用户对信息的要求。因此，在这种背景下，本文将对数字签名技术进行深入的探讨，以期为同行业人员提供借鉴。

关键词 数字签名技术；网络安全防护；密钥

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1007-0745(2023)08-0016-03

1 数字签名技术概述

1.1 采用对称密码算法进行数字签名

对称密码算法又称为单钥密码算法，一般使用与解密密钥一样的加密金钥，甚至可以从任何一种密匙上导出另一种，即Ke=Kd。所以，在发送和处理消息的同时，发送和接受的人都需要共享这个口令。对称加密技术的安全取决于加密密钥，泄漏密钥就是指谁都可以加密，所以加密时要严格控制。它具有较高的加密密度、较低的运算量和较高的运算速率。但它的弊端在于，在多方通讯时，由于要保持原有的密匙，所以会很麻烦，为了确保更好的保密，通常的密码都是有期限的，必须频繁的更新，一旦更新，就会出现泄漏，这就造成了很大的风险。采用数据包加密的一般方法有DES、3DES、IDEA、FEAL、AES等。

1.2 采用非对称密码算法进行数字签名

非对称密码算法也称为公开密钥算法，其主要目的在于解决传统加密技术中的密匙分发和数字签署问题。在使用对称密码的情况下，提出了两个条件：一是一方使用了一把钥匙，另一方使用了一把钥匙，这把钥匙被分发到了另一端。事实上，这种方法违背了加密技术的本质——在通讯中，它是绝对保密的。该公钥运算法则取决于加密金钥和解密金钥。作为密码使用的钥匙与作为解密的钥匙是不一样的，从该密码算法和该密码键决定该破解密钥在该运算1中是无效的；任意一种钥匙都可以用于密码，而另外一种用于进行解密。

1.3 数字签名的安全性分析

作为一种完备的数字签名体系，它首先需要考虑的是安全，RSA体系的安全取决于RSA的公钥加密技术，因此，在RSA体系中，要确保RSA体系的安全，必须考虑以下方面：

1.n的长短取决于被密码的文档的重要性和密码的时间的需要。RSA的安全取决于大质数的解析率。为了增强系统的安全性，可以从多个不同点中随机选取大的质点p和q（当前应该是512个比特），而解密密钥d的相关模式n不能太少。如果d的尺寸是n的四分之一，而e小于n，那么就有办法还原d。

2.在采用RSA的通讯网路协定中，不应当采用公用模式n，这是由于已知攻击方可以在密码/解密键索引对中对该模式进行分解，因此也可以在不对n进行拆分的情况下，算出其它的密码/解密对。

2 网络安全防护及数字签名技术的应用现状

2.1 网络安全的防护情况

根据相关部门的数据，美国每年因互联网问题造成的经济损害达170亿美金，德国和英国都有几百亿美金的损失，法国的几百亿，日本和新加坡的问题也很大。在当今世界各国刑法典所列出的最新的新罪行中，电脑犯罪位居第一。虽然我们现在已经广泛应用了各类先进的软体技术，例如防火墙、代理服务器、入侵探测器、信道控制等，然而，不管是发达国家还是发展中国家，都有愈演愈烈的骇客行为，它们无处不在，给人们的生活带来了极大的威胁。

2.2 数字签名技术在企业信息网络中的应用情况

随着办公自动化、财务管理、定值管理、市场营销等系统的投入使用，大量的关键数据、保密信息通过网络进行传递。这一类的信息管理系统，往往是针对某一类用户而设置的，所提供的资料也仅限于某一

部分的用户，因此，在系统中，用户管理的主要目的是为了建立用户、设置权限、管理和控制用户的权限。虽然从某种意义上说，这些方法可以增强网络的安全性能，但是其实施过程中却出现了诸如主观恶意欺骗、信息不完全、拒不承认等问题，从而对网络安全造成了破坏[1]。比如，在许多商业活动中，需要签字盖章，而在电子文档中，手工签字是不可能的。一些应用程序将签名图像嵌入文件中，以达到数字签名的目的，但这样做也会带来一些安全性问题，比如文件中含有签字的照片被恶意修改，或者为了避免承担法律后果而拒绝签字等。

3 数字签名技术在网络安全防护中的应用分析

3.1 数字签名技术需具备的功能

在本软件中需要实现的功能有以下几个：（1）生成 RSA 密钥：公钥 ke=（e,n），私钥 kd=（d,n）；（2）利用 MD5 算法计算出消息摘要 MD；（3）实施数字签署：利用私有密钥 d 对报文概要进行密码运算（RSA 运算）；（4）检验数字签字：用公开密钥 e 对该数字签字进行加密运算（RSA 运算），将该解密的结果与步骤（2）所算出的报文汇总相对照，若两条报文的概要相同，则签字就成功。

3.2 数字签名技术应用的要求

1. 按要求生成非对称密钥——公钥和私钥。

2. 根据任何被写入的报文字列（明文）产生所要求的报文概要 MD。

3. 按照 RSA 算法的密码原则，利用所产生的私有密钥 d 对所产生的报文概要进行密码操作，从而获得一个数字签署。

4. 按照 RSA 算法的解密原则，利用该发明的公开密钥 e 将该已编码的报文概要（在此方案中表示为已解码的信息）进行解码，并将两个报文汇总进行对比，以确认该数字签名器的识别是否属实[2]。

5. 提示信息完整，操作舒适，图形界面美观。在整个系统中，所有的数字签名系统都是以 C++ 为基础，使用微软 Visual c++6.0 进行了系统的仿真。

3.3 应用于网络安全防护的数字签名设计

3.3.1 密钥形成

在密钥的产生部分中起决定性作用的是素数的选择，对随机数作素性检测，若通过则为素数；否则增加一个步长后再做素性检测，直到找出素数。素性检测采用 Fermat 测试[3]。这个算法的理论依据是费尔马小定理：如果 m 是一个素数，且 a 不是 m 的倍数，那么根据费尔马小定理有：a=1（mod m）。实际应用时：a=1（mod m）⇔a=a（mod m）⇔a=a（mod m），因此对于整数 m，只需计算 a（mod m），再将结果与 a 比较，如果两者相同，则 m 为素数。选取 a=2，则 a 一定不会是任何素数的倍数。根据所选的素数的不同产生不同的密钥。密钥的理论产生模块流程图如图 1 所示。

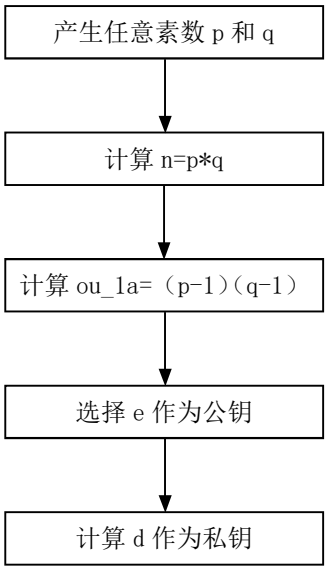

图 1 密钥产生

3.3.2 消息摘要

计算消息摘要的理论实现流程图如图 2 所示。

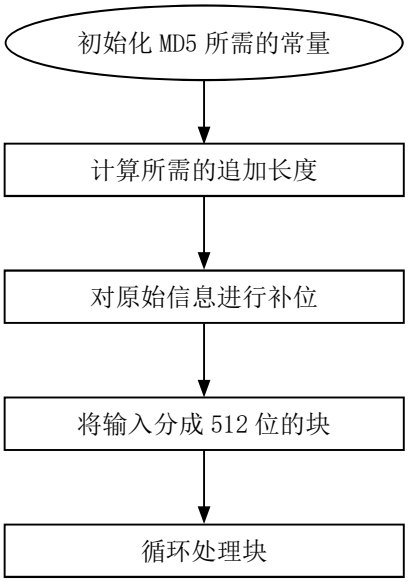

图 2 消息摘要计算流程

在以上流程图中其中循环处理块是最重要的一步，也是 MD5 的核心算法，在这一步中包括了：（1）将四个联结变数分别为 a、b、c、d 四个变数，使得 a=A、b=b、c=c、d=D；将 a、b、c、d 合并为 128 比特的暂存器，并将中间和最后的结果分别存储在实际的演算过程中；

（2）将当前的 512 位块分解为 16 个子块，每个子块为 32 位；（3）将四个回合进行一次周期，每个回合在一个区块内进行 16 次操作，四次回合的第 1 阶段执行各种操作，其余均是一样的：每个回合 16 个输入子区块 M〔0〕、M〔1〕……M〔15〕，或者用 M[i] 来表达，在这里 i 是 0~15；t 是一个由 64 个单元组成的常数阵列，其中的每一个都是 32 比特，t[1]，t[2]……t[64]，k 是 1~64。

3.3.3 数字签名设计

在数字签字中采用了 RSA 密码技术，其认证方法采用了 RSA 解密的基本原则。

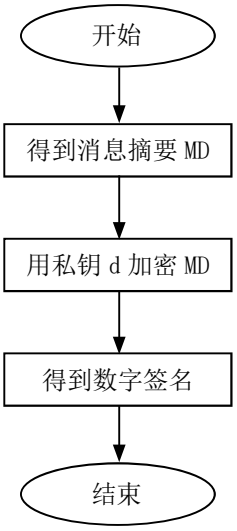

图 3 数字签名的实现流程

RSA 加密和解密都是对一个整型的方次进行运算，然后得到一个模组。如果按照它的意义来进行运算，那么它的中间结果会很大，甚至会超过电脑所允许的整数数值。在加解密操作中，减少了中间值，提高了索引运算的效率。其计算程序如下（如果计算 a^m mod n）：（1）将 m 表示为二进制的形式；（2）将 c=0，d=1，c 代表了该指标的一部分，其最终数值为 m，d 为该中间产物，其最终数值为所要得到的结果；（3）从二进制数的最高位到最低位开始对每一位都用公式 1 进行运算，得到的 d 为该步的结果，公式 1：c=2*c；d=fmod（d*d,n）；（4）如果二进制数字为 1，那么在上述操作之后，下面的操作将会进行：c=c+1；d=fmod（d* a,n）；这个步骤的最后的结论是 d。

3.3.4 数字签名验证

检验数字签章的正确率和成功率，是通过对两份报文的结果进行比对，如果核查者用签名者的公开密钥来破译报文的概要（也就是在这个设计中获得的报文概要），那么就可以证明该签名的真实性，没有被人动过手脚，也没有被伪造，而检验签字的基本原则就是 RSA 的加密方法。

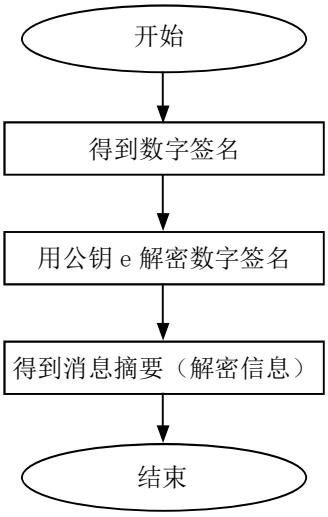

图 4 验证数字签名流程

3.3.5 数字签名运行

在这个软件中有两个报文摘要：报文摘要（明文报文），解密数字签名后的报文摘要（也就是在这个发明中的解密的消息摘要）。若两个报文的概要相同，就可以验证 RSA 的数字签名器的正确性，由此可以完成 RSA 的数字签字。所生成的报文概要与所述解密后的报文概要（这里为已解密的报文）是相同的，那么所述数码签章的可靠性就被证实[4]。

4 总结

信息技术已成为社会发展的重要战略，而网络安全技术是其不可缺少的保障。然而，互联网的安全并非单纯的技术问题，而是一种更大的社会性问题，需要加大对其的宣传与教育。网络安全是一个综合性的系统工程，它不能只依赖于防火墙等单一的安全体系，而是要充分地考虑到网络安全的要求，同时还要综合运用多种的数字签名技术，形成一个高效、通用、安全的网络体系。

参考文献：

[1] 郭浩 . 探析数字签名技术及其在网络通信安全中的应用 [J]. 网络安全技术与应用 ,2020(06):36-38.

[2] 于丹 . 关于网络通信安全中数字签名技术的应用探析 [J]. 数字技术与应用 ,2020,38(05):187-188.

[3] 肖辉远 , 肖培森 , 葛利军 . 基于 ECC 的数字签名方案在网络可信身份认证中的设计与实现 [J]. 警察技术 ,2017(04):83-86.

[4] 王森 . 数字签名技术在网络安全中的应用 [J]. 电子测试 ,2019(06):66-67.