DOI:10.16652/j.issn.1004-373x.2007.11.021

密码算法的研究综述

贾 宁
(太原理工大学 计算机与软件学院 山西 太原 030024)

摘 要:对密码算法进行了概述和分类,并在此基础上论述了密码算法的现状。在哈希函数方面,研究了在 MD_5 和 SHA-1被破解后 HMAC 的健壮性是否变化;在对称密钥算法方面,论述了 AES 的特点并将其与 DES,3DES 及 IDEA 进行了比较;在非对称密钥算法方面,比较了 RSA,DSA 和 ElGamal,并且详细说明了 ECC。最后对密码算法的发展进行了展望。
关键词:密码技术;消息摘要(MD);高级加密标准(AES);椭圆曲线加密体制(ECC)
中图分类号:TP393.08 文献标识码:A 文章编号:1004-373X(2007)11-059-03

Summarize of Cryptography Algorithm Research

JIA Ning
(College of Computer and Software, Taiyuan University of Technology, Taiyuan, 030024, China)

Abstract: This paper introduces the definition and classification of cryptography, and describes the state of cryptography algorithm. In study of hash function, the change of HMAC after MD_5 and SHA-1 were decoded. In studying symmetric key cryptography algorithm, the character of AES are analyzed, and AES are compared with DES, 3DES and IDEA. In studying dissymmetric key cryptography algorithm, the paper makes comparison among RSA, DSA and ElGamal and it explains ECC in detail. Finally, the paper views the development of cryptography algorithm in future.
Keywords: cryptography technology; Message Digest (MD); Advanced Encryption Standard (AES); Elliptic Curve Cryptosystem (ECC)

随着信息传递的增多,信息的保护也变得更加重要了。密码学(Cryptography)也已发展成为一门综合计算机科学、数学、通信以及微电子等技术的学科。他可以保证信息的保密性、完整性、安全性和不可否认性,即信息的防伪造和防窃取。

1 密码算法的概述

密码算法可以看作是一个复杂的函数变换 $C=(M, Key)$。其中 C 为密文,即加密后的字符序列;M 为明文,即待加密的字符序列;Key 为密钥,即秘密选定的字符序列。密码算法作为密码体制的核心由加密算法和解密算法组成。加密是使用一种编码而使存储或传输的信息变为不可读的信息。解密则是使用一种秘密的编码将不可读的信息还原成可读的信息。

密码算法可以按以下方法分类:首先,从功能上可分为:加解密算法、签名算法、摘要算法(哈希算法)及鉴别算法等。其次,从密码结构上可分为:不使用密钥的算法和使用密钥的算法。前者又称为哈希函数,后者又包括对称密钥算法和非对称密钥算法。

收稿日期:2006-09-05
基金项目:山西省自然科学基金资助项目(20041047)

1.1 哈希函数

哈希函数不使用密钥,是一个密文不可恢复的散列函数。他能由任意长的消息(表示成二进制字符串)计算出一个固定长度(较短)的数值的数字变换。

他的特点有:对于任意的消息,计算出哈希值相对容易;给定哈希值,寻找一个消息,很难使其哈希值等于给定的哈希值;很难找到两个哈希结果相同的数值。他的主要应用有:哈希口令、消息指纹、离线装载程序的安全性以及消息的完整性(利用哈希函数生成消息认证码)。常用的算法有:MD_2, MD_4, MD_5;SHA-1(Secure Hash Algorithm,安全哈希算法);HMAC(Keyed-Hash Message Authentication Code)。

这里需要说明的是 MD_4, MD_5 和 SHA-1 已被王小云教授等人破解了。王小云教授的成果是在已知输出时,可以容易地构造出一个输入,使其经过哈希运算后,与已知的输出一致,也就是攻破了哈希函数的第二个特点。因此,这些算法的安全性受到了质疑,一些使用这些算法的工具也逐渐不再受人们的信赖。但是使用这些算法的 HMAC 的健壮性仍然很强。

1.2 对称密钥算法

对称密钥算法是给定一个消息(明文)和一个密钥,加密生成不可读的数据。其中,加解密的密钥相同,而且容易

从一个推导出另一个;密文长度和明文长度大致相同。根据对明文消息加密方式的不同可分为分组密码和流密码。

常见的算法有:DES(Data Encryption Standard)、AES, IDEA(International Data Encryption Algorithm), RC_4, RC_5, Gost, Blowfish 等。

1.3 非对称密钥算法

非对称密钥算法(或称双密钥算法),他的核心是单向陷门函数即从一个方向求值容易,而逆向求值困难。其中,加解密的密钥不同,从私钥容易推出公钥,而很难从公钥推出私钥。该算法往往是基于一个数学难题,可以分为3类:基于大整数因子分解的非对称密钥算法,如 RSA(Rivest Shamir Adleman)算法;基于离散对数的非对称密钥算法,如 DSA(Digital Signature Algorithm)算法;基于椭圆曲线离散对数的非对称密钥算法,如 ECC 算法。

常见的算法有:DSA, RSA, ECC, ElGamal, Rabin, Diffie-Hellman、零知识证明系统、背包算法、概率算法等。

对称密钥算法和非对称密钥算法的优缺点及应用范围的比较见表1。通过比较,我们可以更好地进行信息的保护。

表1　对称密钥算法和非对称密钥算法的比较

算法	优点	缺点	应用
对称密钥算法	算法运算的速度快;密钥相对较短;可以合成强密码	通信双方要保密密钥,而且要不时更换;大型网络中密钥的分配和管理繁琐	加密大量数据;检测数据的完整性
非对称密钥算法	通信时,只保密私钥,不需要时常更换公钥/私钥对;大型网络中的密钥的分配和管理简单	算法复杂,运算的速度慢;密钥较长	加密关键数据和核心数据;进行数字签名

2 常见的算法分析

2.1 哈希算法

HMAC[1] 是一种用哈希函数做认证的机制。该算法使用迭代的已经被证实过的哈希函数以及一个共享的密钥,并且提供了基于密钥的完整性检测方法(称作消息认证码 MAC)。

HMAC 要和一个可信的加密哈希函数结合,而且要用密钥进行计算和已被确认的消息认证码。用 HNAC 函数计算数据"text"得出 MAC,见如下的操作:

$$\mathrm{MAC}(\mathrm{text})_t = H\mathrm{MAC}(K, \mathrm{text})_t$$
$$= H((K_0 \oplus o\mathrm{pad}) \| H((K_0 \oplus i\mathrm{pad}) \| \mathrm{text}))_t$$

其中,B 表示输入哈希函数的数据块大小;MAC 表示计算信息的消息认证码;H 表示已被证实过的哈希函数;K_0 表示将 B 字节长的密钥进行必要的预处理后得到的结果;ipad 表示重复计算 B 次 0x36;opad 表示重复计算 B 次 0x5c;text 表示要计算的信息长度;⊕表示按位异或;‖表示按位或。

在实际计算中,只取计算结果的最左面的 t 字节作为消息认证码。其优点是传输量减少,而且攻击者无法从中获得更多的信息;缺点是攻击者推测的范围也小了。虽然 HMAC 算法依赖的是已被破解的 MD_5 和 SHA-1 算法,但是这并没有影响 HMAC 的健壮性。因为 HMAC 既依赖于哈希函数又依赖于密钥,而且由于认证的瞬时性他也不会受到影响。

2.2 对称密钥算法

AES[2] 是美国国家标准技术研究所 NIST(National Institute of Standard and Technology)为了取代 DES 算法而征集的加密标准。NIST 最终选取了比利时人设计的 Rijndael 算法,他汇聚了强安全性、高性能、易用性和灵活性等优点。AES 算法是一个由可变长数据块和可变密钥长的迭代分组加密算法。与 DES, IDEA 类似,他使用多轮运算加密密文分组来获得明文,并使用密钥扩展算法将密钥转换为多个轮密钥。AES 选取的明文和密文的分组长度为 128 b,密钥的长度为 128 b, 192 b 和 256 b,并将其分别称为 AES-128, AES-192 和 AES-256。

以往的算法都有各自的缺点,如 DES 的密钥太短,3DES 速度太慢,IDEA 存在弱密钥且使用受阻碍。与以往的对称密钥算法相比,AES 算法的优点是:加解密速度快;占用空间小;可并行计算,适合处理器和专用芯片的实现;设计、实现简单;没有借用其他密码,没有从随机表获得随机数;抗攻击性好(尤其是差分分析和线性分析);消除了 DES 的弱密钥和半弱密钥等。因此,如果要与非对称密钥算法结合实现加密系统或是其他机制,AES 算法是较好的选择。

2.3 非对称密钥算法

在非对称密钥算法中,最常见的是 DSA, RSA 和 ElGamal 算法。其中 DSA 是基于大整数因子分解问题,而 RSA 和 ElGamal 是基于离散对数问题。这3种算法有各自的优缺点、安全性以及适用范围等,比较结果见表2。

表2　DSA, RSA 和 ElGamal 算法的比较

算法名称	速度	安全性	适用范围
RSA	很慢,硬件上比 DES 慢 1 000 倍,软件上比 DES 慢 100 倍	基于大整数的因子分解难题	少量的数据加密
DSA	比 RSA 慢	基于整数有限域的离散对数难题,安全性同 RSA 差不多	用于数字签名,如电子转帐系统
ElGamal	较慢	基于乘法群上离散对数难题,或在任意有限循环群 G 中推广	加密密钥;单重或多重签名

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[3]。

早在 1985 年, Neal Koblitz[4] 和 Victor Miller[5] 就将椭圆曲线应用到了密码学中即椭圆曲线上的密码体制 ECC。首先给出椭圆曲线域的参数来确定一条椭圆曲线。在 IEEE P1363 标准中, 定义其参数为一个七元组: $T=(p, FR, a, b, G, n, h)$, 其中 p 代表有限域 $GF(p)$ 的整数, 可以为素数或 2^m; FR 为域表示法; a, b 是方程中的系数; G 为基点; n 为大素数并且等于点 G 的阶; h 是小整数称为余因子。确定了有限域上的曲线后, 用户选取整数 d 作为私钥, 以点 $Q=dG$ 作为其公钥, 这样就形成了密码体制。

ECC 相对于经典的非对称密钥算法有了质的突破。他与常用的 RSA 算法比较, 有如下优点:

更高的安全性　与其他的非对称密钥算法比, 抗攻击性更强。113 位的 ECC 与 512 位的 RSA 的安全性差不多, 160 位的 ECC 与 1 024 位的 RSA 的安全性差不多, 210 位的 ECC 与 2 048 位的 RSA 安全性差不多。

处理数据速度快, 计算量小　因为 ECC 的密钥长度较小。

占用的存储空间较小　因为 ECC 的密钥长度和系统参数较小。

带宽要求低　主要是在对短消息进行加密时, ECC 比其他的密码系统的带宽要求低。

密钥生成简单　因此 ECC 的前向安全性好, 且费用低。

椭圆曲线数字签名(Elliptic Curve Digital Signature Algorithm, ECDSA)是椭圆曲线在密码体制种的一种应用, 他是 DSA 的椭圆曲线模拟[6]。

全局的参数: 基于 $GF(p)$ 上的椭圆曲线 E, 基点 G, G 的阶 n, 消息 m, e 是消息摘要。

消息 m 的 ECDSA 签名的生成步骤:

(1) 将消息 m 表示成二进制字符串;

(2) 使用哈希函数生成消息摘要 $e=SHA1(m)$ (SHA1, Secure Hash Algorithm, 安全哈希算法)。

(3) 选取随机整数 $k\in[0, n-1]$。

(4) 计算得出点 $kG=(x, y)$, 并令 $r=x \bmod n$, 其中 x 是 X 坐标上的整点。

(5) 计算 $k^{-1} \bmod n$。

(6) 利用私钥 d, 计算 $s=k^{-1}\left(e+r*d\right) \bmod n$。

(7) 得出签名 (r, s)。

如果 $r=0$ 或 $s=0$ 则签名验证失败。由于 k 是随机选取的, 所以签名失败的可以忽略不计。

消息 m 的验证步骤:

(1) 找到发送者的公钥 Q。

(2) 如果 $r \bmod n=0$, 则拒绝签名。

(3) 计算哈希值 $e=SHA1(M)$。

(4) 计算 $w=s^{-1} \bmod n$。

(5) 计算 $u=e*w \bmod n$ 和 $v=r*w \bmod n$。

(6) 计算点 $(x_1, y_1)=uG+vQ$。

(7) 计算 $v=x_1 \bmod n$。如果 $v=r$, 那么使用的消息和密钥是有效的。

经过分析该机制, 有两点可以改进: 在计算消息摘要时可以用 HMAC 代替 SHA-1, 以提高签名的安全性; 改进模逆算法提高算法速度。

3　结　语

随着信息技术的发展和网络的普及化, 信息安全已经成为亟待解决的重大问题。密码算法是保护信息安全的关键要素。密码算法的研究人员应从密码算法设计本身、密码算法的应用范围和密码算法的规范标准等方面进行研究, 其研究成果将会不断提高网络的安全性能。

参　考　文　献

[1] NIST. The Keyed-Hash Message Authentication Code (HMAC)[M]. Federal Information Processing Standards Publication, 2002.

[2] NIST. Advanced Encryption Standard(AES)[M]. Federal Information Processing Standards Publication, 2001.

[3] 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.

[4] Koblitz N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987(48): 203-209.

[5] Miller V S. Use of Elliptic Curves in Cryptography[J]. Advanced in Cryptography, CRYPTO' 85, Lecture Notes in Computer Science, 1985, 218: 417-426.

[6] ANSI X9 62: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm(ECDSA), 1998, 9.

作者简介　贾　宁　女, 1981 年出生, 山西太原人, 在读硕士研究生。研究方向为计算机取证技术。