

文章编号:1001-9081(2006)09-2114-02

同余方程加密方案的研究

李 伟,方江涛,郝 林

(云南大学 信息学院,云南 昆明 650091)

(7ime1@163.com)

摘 要:目前基于公钥的加密和会话密钥交换方案容易受到中间人攻击且效率不高。为此,提出了一种基于同余方程的加密和会话密钥交换方案,该算法可以安全高效地实现会话密钥的协商和加密消息的传输,并且还能防止中间人攻击。该方案在一定程度上防止第三者对传输消息的篡改,其安全性是建立在大数因子分解的困难性基础上的。

关键词:同余方程;会话密钥;认证中心

中图分类号:TP309.02;TP309.07 **文献标识码:**A

Cryptography scheme based on congruence equation

LI Wei, FANG Jiang-tao, HAO Lin

(School of Information, Yunnan University, Kunming Yunnan 650091, China)

Abstract: Most current cryptography and session key exchange schemes based on public key are vulnerable to intermediate attack and have low efficiency. In order to solve this problem, a cryptography and session key exchange scheme based on congruence equation was proposed in this paper. Through this scheme, session key exchange and private message transmission can be realized efficiently and safely, and the intermediate attack can also be avoided. To some extent, we can also prevent the third party to garble the transmission message through this scheme. The security of the algorithm is built upon the difficulty of big integer factorization.

Key words: congruence equation; session key; CA

0 引言

在保密通信中,参与的双方需要交换会话密钥,然后用会话密钥对通信内容进行加密。现在通用的会话密钥交换方式有基于对称密钥的方式(如 Kerberos v4)^[1]和基于公钥的方式,如 Diffie-Hellman 体制,而这一体制需要进行大数模指数,所以效率不高。另外这一体制不提供身份认证的功能且容易受到中间人攻击。

本文提出了用同余方程组的方式实现会话密钥的交换和保密消息的传输,这种方法效率较高,能够快速的实现加解密运算,且不容易受到中间人攻击。

1 同余方程及相关问题

1.1 同余方程^[2]

设整系数多项式 $f(x) = a_n x^n + \dots + a_1 x + a_0$,讨论是否有整数 x 满足 $f(x) \equiv 0 \pmod{m}$,这时方程就是模 m 的同余方程。如果整数 c 满足 $f(c) \equiv 0 \pmod{m}$,则称 c 是同余方程的解。显而易见,这时同余类 $c \pmod{m}$ 中的任一整数都是方程的解,这些解应被看作相同的,它们的全体构成同余方程的一个解,记为 $x \equiv c \pmod{m}$ 。

1.2 二次剩余

设 n 为正整数, Z_n 表示小于 n 的非负整数, $Z^* = \{k \in Z_n, \gcd(k, n) = 1\}$ 为模 n 的一个乘法群。设存在 $x, a \in Z_n^*$,且 $x^2 \equiv a \pmod{n}$,则称 a 是模 n 的二次剩余,否则称 a 是模 n 的

二次非剩余。

二次剩余的集合记为 Q_n ,二次非剩余集合记为 Q_n' 。

1.3 Legendre 符号和 Jacobi 符号^[3]

设 p 是一个奇素数, a 为一整数,Legendre 符号定义为:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$$

当 a 不是 p 的倍数时,则整数 a 关于素数 p 的勒让德符号取值为 $+1$ 或 -1 ,它取决于整数 a 是或不是模 p 的平方。 P 的倍数关于素数 p 的勒让德符号为 0 。设 n 为奇正整数,并设 a 是一个正整数,整数 a 关于整数 n 的雅可比符号等于整数 a 关于 n 的素因子的勒让德符号之乘积。所以,如果 $n = pq$,则:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

任何整数 a 关于任何整数 n 的雅可比符号可以有效地计算而无需知道 n 的素因子。

1.4 $GF(p)$ 上的二次方程的一些性质^[4]

定理1 p 是奇素数, $a, b, c \in Z_n^*$,则方程 $ax^2 + bx + c \equiv 0 \pmod{p}$ 的解的个数是:

$$1 + \left(\frac{b^2 - 4ac}{p}\right)$$

定理2 设 p 是素数, $f(x)$ 为一 n 次多项式, $f(x) \equiv 0 \pmod{p}$ 在 $GF(p)$ 上有解 a ,则一定有 $f(x) = (x - a)g(x)$,其中 $g(x)$ 为 $n - 1$ 次多项式。

定理3 设 p 是一奇素数, c 为 $GF(p)$ 上的一元素, $\left(\frac{c}{p}\right) =$

收稿日期:2006-03-27; 修订日期:2006-05-30

基金项目:云南省自然科学基金资助项目(2002F0010M); 国家自然科学基金资助项目(60573104)

作者简介:李伟(1980-),男,山东淄博人,硕士研究生,主要研究方向:信息安全; 方江涛(1979-),男,安徽合肥人,硕士研究生,主要研究方向:信息安全; 郝林(1955-),男,云南昆明人,教授,主要研究方向:信息安全。

-1 , 方程 $x^2 + mx + c = 0 \pmod p$ 有解 a , 且 $\left(\frac{a}{p}\right) = 1$, 则有 $\gcd(x^{p-1/2}, x^2 + mx + c) = x - a$ 。

2 会话密钥的交换

在这一体制中, 需要有一个可信的认证中心(CA)。在网络中, 认证中心保存各个实体的证书, 其中含有双方的共享主密钥。现在假设网络中只有两个实体 A 和 B , 如果 A 要和 B 通信, 那么它应首先(通过其工作站)向认证中心申请会话密钥 S_A , 然后CA将 A 与 B 通信的会话密钥 K_{AB} 用 S_A 加密后发送给 A 。

假设 A 与CA共享的主密钥是 (p_A, q_A, m_A) , 其中 p_A 和 q_A 是两个大素数, m_A 是任意形式的整数, 系统计算 $M_A = p_A q_A$, 并公布 M_A 。下面实体 A 与CA将要实现会话密钥交换。

A 首先选取素数 $x = p_A^{-1}$, 其中 $x \in [1, M_A]$ 并且使得

$$\left(\frac{x \bmod p}{p}\right) = 1 \quad \left(\frac{x \bmod q}{q}\right) = 1$$

$\left(\frac{x \bmod p}{p}\right)$ 和 $\left(\frac{x \bmod q}{q}\right)$ 是 Legendre 符号。然后构造下列同余方程:

$$\begin{cases} x^2 + m_A x + c_1 = 0 \pmod p \\ x^2 + m_A x + c_2 = 0 \pmod q \end{cases} \quad (1)$$

其中 c_1 满足 $(c_1/p) = -1$ 且 $(m_A^2 - 4c_1/p) = 1$, c_2 满足 $(c_2/q) = -1$ 且 $(m_A^2 - 4c_2/q) = 1$, 然后 A 将 (c_1, c_2) 发送给CA, 由于CA知道 (p_A, q_A, m_A) , 所以它能够解同余方程(1)得到 x 的两组解, 有二次曲线的性质知, 两个解中必有一个 $\left(\frac{x_{11}}{p}\right) = 1$, 另外一个 $\left(\frac{x_{21}}{p}\right) = -1$, 有前面的假设知这里应该选择 x_{11} , 另外CA也能够解(2)得到另外一组解, 其中 $\left(\frac{x_{12}}{p}\right) = 1, \left(\frac{x_{22}}{p}\right) = -1$, 这里同样选择 x_{12} , 这样便得到了下面的一次同余方程组:

$$\begin{cases} x = x_{11} \bmod p \\ x = x_{12} \bmod q \end{cases}$$

根据 $x \in [1, M_A]$, 由中国剩余定理可以得到唯一的 x , 这里的 x 便是实体 A 当初选择的素数 p_A^{-1} 。

同时CA选择 $y = q_A^{-1} \in [1, M_A]$, 使得 $\left(\frac{y \bmod p}{p}\right) = 1$, $\left(\frac{y \bmod q}{q}\right) = 1$, 用同样的方式可以使得实体 A 得到 q_A^{-1}, m_A^{-1} 的交换方式与上面类似, 双方可以选择任意一方生成 m_A^{-1} 。

这样, 实体 A 便和CA有了共享的会话密钥 $(p_A^{-1}, q_A^{-1}, m_A^{-1})$ 。

现在实体 A 和 B 要实现秘密通信, 则它们首先应该建立通信的会话密钥, 这里假设 B 和CA的主密钥是 (p_B, q_B, m_B) , 其中 p_B 和 q_B 是两个大素数, m_B 是任意形式的整数, 系统计算 $M_B = p_B q_B$, 并公布 M_B 。

首先 A 选择大素数 $p_{AB} \in [1, M_B]$, (如果 $M_B > M_A$ 且 $p_{AB} \in [M_A, M_B]$, 则可以把 p_{AB} 分解成两个较小的整数再发送), 然后用共享的会话密钥 $(p_A^{-1}, q_A^{-1}, m_A^{-1})$ 将 p_{AB} 发送给CA, 然后CA用它与 B 的主密钥 (p_B, q_B, m_B) , 将 p_{AB} 发送给 B , 同时 B 选择大素数 $q_{AB} \in [1, M_A]$, 用同样的方式将 q_{AB} 发送给 A , m_{AB} 的交换方式类似。这样 A 和 B 就成功的交换了会话密钥, 它们的会话密钥是 (p_{AB}, q_{AB}, m_{AB}) 。

3 加密消息的传输

现在实体 A 和 B 之间已经有了会话密钥 (p_{AB}, q_{AB}, m_{AB}) , 接下来它们就可以用它来进行加密消息的传输。

假设 A 要传送消息 m 给 B , 它首先将 m 分解为一定数量的子消息 m_1, m_2, \dots, m_t , 其中 $\left(\frac{m_i \bmod p}{p}\right) = 1, \left(\frac{m_i \bmod q}{q}\right) = 1, i = 1, 2, \dots, t$, 且 $m_i \in [1, M_{AB}]$, $M_{AB} = p_{AB} q_{AB}$, 然后 A 构造下面的方程组(这里设 $y = m_i$):

$$\begin{cases} y^2 + m_{AB} y + c_{1i} = 0 \pmod{p_{AB}} \\ y^2 + m_{AB} y + c_{2i} = 0 \pmod{q_{AB}} \end{cases} \quad (3)$$

其中 c_{1i} 满足 $\left(\frac{c_{1i}}{p_{AB}}\right) = -1$ 且 $\left(\frac{m_{AB}^2 - 4c_{1i}}{p_{AB}}\right) = 1$, c_{2i} 满足 $\left(\frac{c_{2i}}{q_{AB}}\right) = -1$ 且 $\left(\frac{m_{AB}^2 - 4c_{2i}}{q_{AB}}\right) = 1$, 且 c_{1i} 和 c_{2i} 要尽可能短(这里当找不到满足条件的 c_{1i} 和 c_{2i} 时可以对子消息进行比特填充), 然后 A 将 (c_{1i}, c_{2i}) 发送给 B , 由于 B 知道会话密钥 (p_{AB}, q_{AB}, m_{AB}) , 所以它能够解同余方程组(3)和(4), 这里根的选择与解同余方程组(1)和(2)一样。然后由中国剩余定理实体 B 就可以解出唯一的 m_i 。

4 安全性和效率

4.1 安全性

在这一方案中, 窃听者知道的信息有大素数 p 和 q 的乘积 M 以及传输的消息 (c_1, c_2) , 根据大数分解的困难性可以假设除了通信的合法参与者之外, 任何人不可能从 M 中分解出 p 和 q , 所以窃听者不可能从消息 (c_1, c_2) 中求解同余方程组(1)和(2), 所以他不能得到会话密钥, 同样的道理, 他也不能解同余方程组(3)和(4)得到传输的消息。

另外, 即使窃听者得到消息 (c_1, c_2) , 他也不可能进行中间人攻击。

4.2 效率分析

方案中较大的计算量主要集中在以下两个部分: 一是在构造方程组(1), (2)和(3), (4)时 Legendre 符号的计算; 二是在利用中国剩余定理求解一次方程组时的求逆运算。

在第二种情况下, 由于是针对实体之间的共享密钥求逆, 而共享密钥一般不会过于频繁的更新, 所以这一部分可以预先计算。

求解 Legendre 符号的复杂度 $O((\lg p)^2 + (\lg q)^2)$, 而在传统的 Diffie-Hellman 体制中要计算模指数, 而模指数运算在指数的二进制表示已知的前提下复杂度为 $O((\lg n)^3)$ 。

在双方交换大素数时可以实行并行计算, 以提高密钥交换的效率。

5 说明

1) 消息 (c_1, c_2) 在传输过程中可能被篡改, 由于假设 $\left(\frac{c_1}{p}\right) = -1$ 且 $\left(\frac{c_2}{q}\right) = -1$, 而 pq 是公开的, 设篡改者篡改的结果是 (d_1, d_2) , 那么 $\left(\frac{d_1 d_2}{pq}\right) = 1$, 所以 d_1 有一半的可能性是 p 的二次剩余, 所以消息 (c_1, c_2) 被成功篡改的可能性是

(下转第 2120 页)

精确的数学定义;并提出了七条准则,对密码协议的形式化过程进行规范,使得形式化更加清晰准确。在此基础之上,对密码协议的安全特性重新进行了规范定义,为协议安全特性分析和证明提供了一个合理可靠的基础。

在下一步的工作中,我们将进一步研究基于 eWoo-Lam 模型中的形式化推理机制,分析影响推理过程的各种因素;在此基础上,设计有关该模型的自动化验证算法,并将算法应用于密码协议自动化验证器中。

参考文献:

- [1] DOLEV D, YAO AC. On the Security of Public-Key Protocols[J]. IEEE Transactions on Information Theory, 1983, 2(29): 198 - 208.
- [2] BRIAIS S, NESTMANN U. A Formal Semantics for Protocol Narrations[A]. Trustworthy Global Computing, International Symposium, TGC 2005[C], Edinburgh, UK, 2005. 163 - 181.
- [3] CHEVALIER Y, COMPAGNA L, CUELLAR J, et al. A High-Level Protocol Specification Language for Industrial Security — Sensitive Protocols[A]. Proceedings of Workshop on Specification and Automated Processing of Security Requirements(SAPS 2004)[C], 2004.
- [4] BOUROULET R, KLAUDEL H, PELZ E. A Semantics of Security Protocol Language Using a Class of Composable High-level Petri Nets[R]. Laboratory of Algorithms, Complexity and Logic of University of Paris, France, 2004.
- [5] HALPERN JY, PUCELLA R. Modeling Adversaries in a Logic for Security Protocol Analysis[A]. Formal Aspects of Security, FASec'02[C], 2002.
- [6] WOO TYC, LAM SL. A Semantic Model for Authentication Protocols[A]. Proceedings IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA, 1993. 178 - 194.
- [7] GUTTMAN JD, HERZOG JC, RAMSDELL JD, et al. Programming Cryptographic Protocols[R]. The MITRE Corporation, 2004.
- [8] DELAUNE S, JACQUEMARD F. A Decision Procedure for the Verification of Security Protocols with Explicit Destructors[A]. Proceedings of the 11th ACM Conference on Computer and Communications Security[C], 2004. 278 - 287.
- [9] 季庆光, 冯登国. 对几类重要网络安全协议形式模型的分析[J]. 计算机学报, 2005, 28(7): 1071 - 1083.
- [10] SONG D. Athena: a New Efficient Automatic Checker for Security Protocol Analysis[A]. Proceedings of the 12th IEEE Computer Security Foundations Workshop (CSFW'99)[C], 1999. 192 - 202.
- [11] CLARKE EM, JHA S, MARRERO W. Verifying Security Protocols with Brutus[J]. ACM Transactions on Software Engineering and Methodology (TOSEM), 2000, 9(4): 443 - 487.
- [12] MEADOWS C. The NRL Protocol Analyzer: an Overview[J]. Journal of Logic Programming, 1996, 26(2): 113 - 131.
- [13] DATTA A, DEREK A, MITCHELL JC, et al. A Derivation System and Compositional Logic for Security Protocols[J]. Journal of Computer Security (Special Issue of Selected Papers from CSFW-16), 2005, 13(3): 423 - 482.
- [14] LOWE G. Casper: A Compiler for the Analysis of Security Protocols[A]. Proceedings of the 1997 IEEE Computer Society Symposium on Research in Security and Privacy[C], 1997. 18 - 30.
- [15] STOLLER SD. A Reduction for Automated Verification of Authentication Protocols[R]. Computer Science Department, Indiana University, 1998.
- [16] THAYER FJ, HERZOG JC, GUTTMAN JD. Strand spaces: Why is a security protocol correct? [A]. Proceedings of IEEE Symposium on Security and Privacy[C], 1998. 160 - 171.
- [17] 刘怡文, 李伟琴. 网络支付协议的形式化安全需求及验证逻辑[J]. 通信学报, 2004, 25(4): 174 - 181.
- [18] CREMERS CJF, MAUW S, VINK EP. A Syntactic Criterion for Injective of Authentication Protocols[A]. Proceedings of ARSPA'05 (The Second Workshop on Automated Reasoning for Security Protocol Analysis)[C], 2005.
- [19] FOCARDI R, MAFFEI M, PLACELLA F. Inferring Authentication Tags[A]. Proceedings of 2005 IFIP WG 1.7, ACM SIGPLAN and GI FoMSESS Workshop on Issues in the Theory of Security (WITS'05)[C], 2005. 41 - 49.
- [20] 胡成军, 郑援, 吕述望, 等. 安全协议的形式化规范[J]. 电子与信息学报, 2004, 26(4): 556 - 561.
- [21] BLANCHET B. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules[A]. 14th IEEE Computer Security Foundations Workshop (CSFW-14), IEEE Computer Society[C]. Los Alamitos, CA, 2001. 82 - 96.
- [22] LOWE G. A Hierarchy of Authentication Specifications[A]. Proceedings of the 10th Computer Security Foundations Workshop (CSFW'97)[C]. Rockport, Massachusetts, 1997.
- [23] LOWE G, ROSCOE B. Using CSP to Detect Errors in the TMN Protocol[J]. IEEE Transactions on Software Engineering, 1997, 23(10): 659 - 669.

(上接第 2115 页)

$1/4$, 当接受者收到消息后, 首先验证 $\gcd(x^{p-1/2}, x^2 + mx + c) = x - a$, 这里 a 是方程的解, m 和 c 是方程组中选定的参数, 含义与(1), (2) 和(3), (4) 相同。如果等式不成立, 则说明消息被篡改。由于消息 (c_1, c_2) 被成功篡改的可能性是 $1/4$, 所以在密钥交换中, 有必要利用哈希函数和时间戳的方式来防止篡改。

2) 在实际的系统中, 有一些实体可能不是经常参与通信, 这时 CA 可以不存储它们的会话密钥, 而是由实体存储 (c_1, c_2) , 通信是临时计算会话密钥, 这使得 CA 不需要存储任何临时性的信息, 而只需要维持一个大的静态数据库, 每次收到一个请求发一个响应, 然后忘掉所有的一切。这种模式有很多好处, 比如可以很容易地实现 CA 的备份以及在系统崩溃前不需要保存状态等。

6 结语

本文根据大数分解的困难性, 利用同余方程的性质提出了一种新的加密算法, 这一算法可以有效地实现会话密钥的交换和加密消息的传输, 并且能够防止中间人攻击。

参考文献:

- [1] STALLINGS W. 密码编码学与网络安全: 原理与实践[M]. 第3版. 刘玉珍, 王丽娜, 傅建明, 译. 北京: 电子工业出版社, 2004.
- [2] 潘承洞, 潘承彪. 初等数论[M]. 第2版. 北京: 北京大学出版社, 2003. 155 - 157.
- [3] MENEZES AJ, VAN OORSCHOT PC, VANSTONE SA. 应用密码学手册[M]. 胡磊, 王鹏, 译. 北京: 电子工业出版社, 2005.
- [4] 李子臣, 戴一奇. 二次剩余密码体制的安全性分析[J]. 清华大学学报(自然科学版), 2001, 41(7): 80 - 82.