基于哥德尔β函数的数据加密*

魏建香[1], 罗军舟[2]

(1. 南京人口管理干部学院信息科学系, 210042, 南京; 2. 东南大学计算机科学与工程系, 210096, 南京)

[摘要]　数据加密是计算机安全技术中重要的研究方面. 文根据哥德尔β函数的构造思想, 提出了现代计算机中一种数据加密的方法, 详细说明了数据加密的全部流程, 并通过一个实例进行了验证.

[关键词]　数据加密, 哥德尔β函数, 加密流程

[中图分类号] TP309. 2;　[文献标识码] A;　[文章编号] 1672- 1292(2002)01- 0014- 04

0　引言

在计算机网络中要安全地传输数据, 数据加密是一种可行的方法. 数据加密的基本思想是通过变换信息的表示形式来伪装需要保护的敏感信息, 使非授权者不能了解被保护信息的内容[1]. 数据加密过程是由各种加密算法来具体实施, 它以很小的代价提供很大的安全保护. 到目前为止, 已经公开发表的各种加密算法多达数百种. 按照收发双方密钥是否相同来分类, 可以将这些加密算法分为常规密码算法和公钥密码算法. 在常规密码中, 数据加密- 解密采用了相同的算法, 即加密密钥和解密密钥是相同或等价的. 比较著名的常规密码算法有: 美国的 DES 及其各种变形. 常规密码的优点是有很强的保密强度, 且经受住时间的检验和攻击, 但其密钥必须通过安全的信道进行传输. 因此, 其密钥管理成为系统安全的重要因素. 在公钥密码中, 数据的加密与解密采用了不同的算法. 比较著名的公钥密码算法有: RSA、背包密码、McEliece 密码等. 其中最有影响的是 RSA, 它能抵抗到目前为止已知的所有码攻击. 公钥密码的优点是可以适应网络的开放性要求, 且密钥管理问题也较为简单, 尤其可方便的实现数字签名和验证. 但其算法复杂, 加密数据的效率较低. 尽管如此, 随着现代电子技术和密码技术的发展, 公钥密码算法将是一种很有前途的网络安全加密体制. 数学的发展对现代计算机有着很大的启示, 早在计算机产生之前, 1934 年哥德尔提出的一些设想, 对现代计算机数据的加密安全传输具有十分重要的参考意义. 现基于哥德尔β函数构造方法[2], 提出的一种数据加密的方法. 由于加密与解密采用了不同的算法, 这是一种公钥密码算法, 但其算法实现相对较为简单.

1　一个重要的事实

设有 n 个两两互质的除数 $d_1, d_2, \cdots, d_n$, 当被除数 c 增加的时候, 余数 $\mathrm{rm}(c, d_1), \mathrm{rm}(c, d_2), \cdots, \mathrm{rm}(c, d_n)$ 的情况, 例如当 $n = 2$ 时, 取除数 $d_1 = 3, d_2 = 4$ 时的情形:

c	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…
$\mathrm{rm}(c, 3)$	1	2	0	1	2	0	1	2	0	1	2	0	1	2	…
$\mathrm{rm}(c, 4)$	1	2	3	0	1	2	3	0	1	2	3	0	1	2	…

* 收稿日期: 2002- 03- 17.
基金项目: 国家"十五"重大攻关项目"网络教育关键技术及示范工程"研究基金资助项目(2001. BA101A)和教育部"现代远程教育关键技术与支撑服务系统和天地网结合项目"的支持.
作者简介: 魏建香, 1971- , 南京人口管理干部学院讲师, 主要从事网络教育、数据交换技术的研究.

可以发现, 当 c 从 1 变化到 12 时, 在 $a_1 < 3$, $a_2 < 4$ 时余数 $\mathrm{rm}(c, 3)$ 和 $\mathrm{rm}(c, 4)$ 正好穷尽了 a_2, a_2 的所有组合:

$(1, 1)$、$(2, 2)$、$(0, 3)$、$(1, 0)$、$(2, 1)$、$(0, 2)$、$(1, 3)$、$(2, 0)$、$(0, 1)$、$(1, 2)$、$(2, 3)$、$(0, 0)$

注意这个例子中 c 取 1 和 13 时, $\mathrm{rm}(c, 3)$ 和 $\mathrm{rm}(c, 4)$ 的余数相同. 类似地, c 取任何两个相隔为 12 的倍数的时候, 都会出现余数相同. 而 12 正好是这两个除数的最小公倍数. 通过这个事实, 我们可以得到以下相应的结论:

结论 **1** 如果 c 分别取 j 和 $j + k$ 时各分别除以两两互质的数 $d_1, d_2, \cdots, d_n$ 时都能取到相同的余数 $a_1, a_2, \cdots, a_n$, 则 k 必然为 $d_1, d_2, \cdots, d_n$ 积的倍数.

证明: 因为 j 和 $j + k$ 除以 $d_1, d_2, \cdots, d_n$ 后余数相同, 所以 $j + k - j$ 必然能被 $d_1, d_2, \cdots, d_n$ 整除. 即 k 能整除 $d_1, d_2, \cdots, d_n$, 又因为 $d_1, d_2, \cdots, d_n$ 两两互质, 所以 k 为 $d_1, d_2, \cdots, d_n$ 积的倍数.

结论 **2** 已知 $d_1, d_2, \cdots, d_n$ 两两互质, 设 $D = d_1 \times d_2 \times \cdots \times d_n$, 对给定的自然数列 $a_1, a_2, \cdots, a_n$ 满足 $a_1 < d_1$, $a_2 < d_2$, $\cdots$, $a_n < d_n$, 则在 $1 \sim D$ 中必然存在唯一的 c, 使 n 个余数 $\mathrm{rm}(c, d_0)$, $\mathrm{rm}(c, d_1)$, $\cdots$, $\mathrm{rm}(c, d_n)$ 正好是 $a_1, a_2, \cdots, a_n$.

证明: 存在性证明, 当 c 从 1 变化到 D 时, c 降以 d_i 的余数 $\mathrm{rm}(c, d_0)$, $\mathrm{rm}(c, d_1)$, $\cdots$, $\mathrm{rm}(c, d_n)$ 组成的数列, 正好穷尽了所有小于 d_i 的自然数可能作成的对偶, 即其中必然包括 $a_1, a_2, \cdots, a_n$ 这个数列, 证明了这样的 c 是存在的.

唯一性证明(用反证法), 如果在 $1 \sim D$ 中存在 c_1 和 c_2, 它们除以 d_i 后余数都为 a_i. 显然由结论 1 可知, c_1 与 c_2 的差必然是 D 的倍数, 而 c_1 与 c_2 最大之差为 $D - 1$, 从而假设不成立, 唯一性得以证明.

2 构造 β 函数

根据上述结论, 可以构造一个具有下列性质的函数 $\beta_0(c, d, i)$.

(1) 谓词 $\beta(c, d, i) = w$ 是算术的;

(2) 对任何一个有限自然数列 $a_1, a_2, \cdots, a_n$ 都可以找出两个码 c, d 使得 $\beta(c, d, i) = a_i (i = 1, 2, \cdots, n)$.

我们知道, 只要 $d_1, d_2, \cdots, d_n$ 使得:

(1) $d_1, d_2, \cdots, d_n$ 两两互质,

(2) $a_1 < d_1, a_2 < d_2, \cdots, a_n < d_n$,

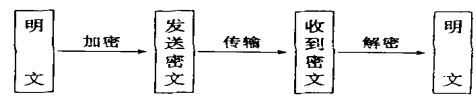

图 1 数据加密的基本方法

则总可以找到唯一的 $c (c \leqslant d_1 \times d_2 \times \cdots \times d_n)$ (依据结论 2) 使得余数 $\mathrm{rm}(c, d_i) = a_i (i = 1, 2, \cdots, n)$.

所以, 我们能找出函数 $\alpha(d, i)$ 使得数 $d_1, d_2, \cdots, d_n$ 为 $\alpha(d, i)$ 在 $i = 1, 2, \cdots, n$ 时的值, 满足 $\beta(c, d, i) = \mathrm{rm}(c, \alpha(d, i))$.

取 $s = \max(a_1, a_2, \cdots, a_n, n)$, $e = s!$, $di = \alpha(d, i) = 1 + i \times e$, 验证:

当 $i = 1, 2, \cdots, n$ 时, $d_i = 1 + ie$ 两两互质.

用反证法证明: 如果 d_i 之间不两两互质, 不失一般性, 可假设 d_j 与 d_{j+k} 即 $1 + je$ 与 $1 + (j + k)e$ 有除 1 外的质因子 p, 则 p 能整除这两数的差 ke 即 $ks!$.

另一方面, p 不能除尽 $s!$, 否则 p 整除 je, 与已知 p 整除 $1 + je$ 矛盾, 同时由于 $k < n \leqslant s$, 而每个小于或等于 s 的数都能除尽 $s!$, 所以 p 不能除尽 k (否则 p 将除尽 $s!$). 又因为 p 是一质因子, 所以 p 不能整除 k 和 $s!$ 的乘积.

因此两方面结论矛盾, 假设不成立. 所以 d_i 之间两两互质. 且对每个 $i (i = 0, 1, 2, \cdots, n)$, 都有 a_i

$<= s <= s! < 1+ is! = \alpha(d, i) = d_i$.

3　数据加密的实现

3.1　基本思想

数据在计算机中安全传输的基本方法如图 1.

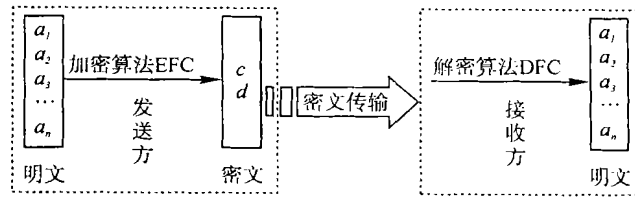

图 2　数据加密流程图

假设明文为 $a(a_1, a_2, \cdots, a_n)$, 根据哥德尔 β 函数的构造方法, 可求出相应的 $d(d_1, d_2, \cdots, d_n)$(d 具有唯一性且 d_i 两两互质), 把 a_i 作为余数, d_i 作为除数, 依据一定的算法在 1 ~ D 中找出唯一的被除数 c, 这时可用密文(c, d) 代替要传送的明文 a; 在收到密文(c, d) 后, 求 c 除以 d 后的余数即为明文 a.

3.2　实现步骤

图 2 给出了基于哥德尔β 函数的数据加密的流程. 加密算法 EFC 流程如图 3. 解密算法 DFC 流程如图 4.

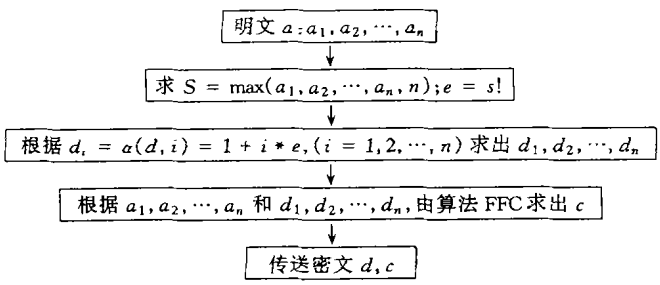

图 3　加密算法 EFC 流程图

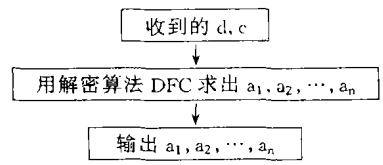

图 4　解密算法 DFC 流程图

加密流程中的核心 FFC 算法(略). 解密算法 DFC 非常简单, 只要用收到的 d 除 c 后, 得到的余数序列就是明文.

3.3　实例

根据上述的加密方法, 下面用一个实例加以具体说明. 假设要发送的信息编码 A 为(2, 3, 1), 这时

$n = 3$, s= max(2, 3, 1, 3) = 3　　$e = s! = 3! = 6$

由 $d_i = 1 + i \times e$ 得:

$d_1 = 1 + 6 = 7$, $d_2 = 1 + 2 \times 6 = 13$, $d_3 = 1 + 3 \times 6 = 19$

$D = d_1 \times d_2 \times d_3 = 7 \times 13 \times 19 = 1729$

根据 FFC 算法, 在 0 ~ 1729 中求 c 使　$\mathrm{rm}(c, d_1) = a_1, \mathrm{rm}(c, d_2) = a_2, \mathrm{rm}(c, d_3) = a_3$, 求出 $c = 1645$

发送的密文(d, c)为: (7, 13, 19, 1654)

B 在收到 A 发送的密文后进行解密, 过程如下:

$a_1 = \mathrm{rm}(1654, 7) = 2$; $a_2 = \mathrm{rm}(1654, 13) = 3$; $a_3 = \mathrm{rm}(1654, 19) = 1$

解密后的信息为(2, 3, 1), 与发送的明文一致, 加密与解密过程得到验证.

4　进一步的研究

数据加密是计算机安全领域中重要的研究方面. 本文所描述的数据加密采用的是一种典型的非对称密钥机制, 在加密与解密中采用了不同的算法. 这种数据加密方法存在一定的缺陷, 从本文的例子中可以看出, 所求出的密文在数量级上要比明文得多, 因此在传输大容量源信息时效率偏低, 但其算法相对简单. 要使这种加密方法在实际中得到真正的应用, 还有一些方面需要改进. 我们知道, 通过某种映射关系, 每一个字符都可以用一个唯一的数来表示, 也就是说, 一段字符信息对应了一组数列, 再通过本算法加密, 对方将密文解密后, 再按照这种映射关系将字符表示出来, 这是我们将进一步考虑的问题.

[参考文献]

[1] 龚俭、陆晟、王倩. 计算机安全概论[M]. 南京: 东南大学出版社, 2000, 8.
[2] S C 克林[美]. 元数学导论[M]. 北京: 科学出版社, 1984, 11.

Data Encryption Based on Godel's β Function

Wei Jianxiang[1], Luo Junzhou[2]

(1. Department of Information Science, Nanjing College of Population Programming Management, 210042, Nanjing, PRC;
2. Department of Computer Science and Engineering, Southeast University, 210096, Nanjing, PRC)

Abstract: Data encryption is an important subject of computer security. This paper presents a method of data encryption by the research on Godel's β Function. The encryption process is discribed in detail and an example is also given.

Key words: data encryption, Godel's β Function, encryption Process

[责任编辑: 刘健]

(上接第 13 页)

[参考文献]

[1] Johannes Sametinger. Software Engineering with Resuable Components[M]. New York: Spring-Verlag Berlin Heidelbery. 1997.
[2] 杨芙清. 软件复用及相关技术[J]. 计算机科学, 1999, 26(5).
[3] 徐家福, 王志坚. 对象式程序设计语言[M]. 南京: 南京大学出版社, 1992.
[4] 黄为民, 陈世福. 分布式对象构件及其应用[J]. 计算机应用研究, 2000, (10): 83~ 85.

The Design of Data Base Application System Based on Software Component Technology

Huang Weimin, Bai Xiaodong

(College of Mathematics and Computer Science, Nanjing Normal University, 210097, Nanjing, PRC)

Abstract: Based on the theoretical study on the software component theory, the technology is introduced into the development of the database system. A component-based development model for database system is proposed. An application system has been developed by adopting the proposed technique.

Key words: software, component, database

[责任编辑: 严海琳]