数据加密新方法—人工神经网络方法

张平
(厦门大学 福建厦门 361021)

【摘要】本文主要叙述数据加密的一种新方法。即用人工神经网络的方法。人工神经网络是 2 0 世纪 8 0 年代广为推荐的技术。但把人工神经网络方法用于数据加密,则是一种新思路。本文是我们向大家叙述这个方法的细节。如果站在数学高观点下理解数据加密的观念。我们认为数据加密和人工神经网络都是一种变换。

【关键词】数据加密 人工神经网络 算法 变换
【中图分类号】TP309.7 【文献标识码】A 【文章编号】1673-8209(2010)04-0241-03

因特网(Internet)给人类带来巨大好处。 让信息社会得到迅猛发展。但是黑客的存在和肆意攻击,也给当今社会安定带来许多隐患。如何保护自己,已成为人人关心的首要问题。寻找各种防护方法也引起世界的关注。中国的科学技术人员也极大地关注此课题。数据加密是一种重要的防护方法。我们讲述自己研究结果与大家交流,也将不断改进我们的成果。欢迎大家批评指教。

1 研究数据加密的意义

当今新传媒 Internet 正在风靡全球。尽管 Internet 的发展如此迅猛,但商界对使用电子邮件仍有保留。WWW 目前也主要作为公司扩大影响和进行产品推销的地方。还远未成为一个真正的买卖市场。

为什么呢?只因为商界对 Internet 仍然持有保留态度。这是不无道理的,Internet 的确存在令人担心的一面。就拿电子邮件来说,存在被拆看、误投和伪造的可能性。电子邮件在网络传输中可能轻易地,难于察觉地被阅读,甚至被篡改。

微软公司总裁比尔·盖茨曾不无感慨地说:“每天假借我的名义发出的电子邮件比我自己发出还要多。”

当前,由于信息保护措施不力造成巨大损失,在商业(包括金融,特别是银行系统)、交通、工业、科技、国防、外交等等部门所发生的事例非常之多。仅银行的密码遭他人窃取,美国的银行界每年损失达几十亿美元。

在计算机网络大量普及的今天,信息本身就是时间,就是财富。信息传输,目前通过脆弱的信息通道,信息存储在“不设防”的计算机系统中,如何保护信息安全,使之不被窃取及不被篡改或破坏,已成为当今信息产业界普遍关注的重大问题。采用密码是有效而可行的办法。利用密码技术是“保护自己”的最简单办法。

2 研究数据加密的内容

加密的目的就是把原来看来很明白的“文本”,加工成无法辨认的“乱码”。我们来研究一种工具。它把明文做成乱码。

从历史来看,公元前 4 世纪就有人探索过,应用了。后来又有 DES 算法(数据加密标准,1977 年)。近年来,又有 RSA 加密算法(1984 年)。

最近(1999 年),我们第一次提出用“人工神经网络”方法,解决加密新算法。

加密中还有一个重要的工具,那就是“密钥”。不同的人应当有不同的密钥。才能保证绝对安全。设计“密钥”也是一个重要内容。

随着数据加密不断发展,数据加密在“数字签名”,“身份认证”与“数字标识”等方面获得应用。这些都是我们将要探讨的内容。

3 数据加密模型

什么是密码?简单地说它就是一组含有参数 k 的变换 E。

设已知信息 m,通过变换 Ek 得到密文 c,即

$c=E_k(m)$

这个过程叫做加密,参数 k 叫做密钥。加密算法 E。当密钥 k 不同,所获得的密文也不同。

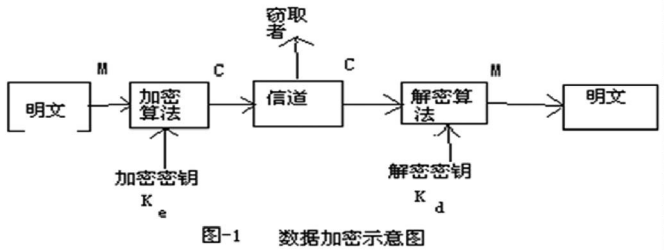


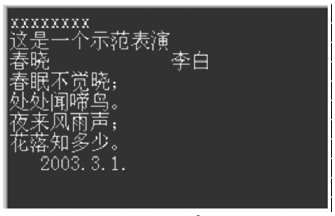
图-1 数据加密示意图

通信双方,一方称为发信方,或简称为发方, 另一方称为收信方,或简称收方。

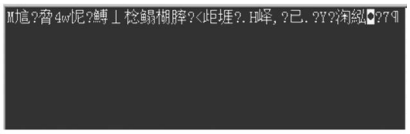
保密通信的传输机理图示如图 1:

注解:明文 M,就是通常看到的文本。 例如 图—明文 所示

经过加密处理后,得到的是密文 C,它是一串乱码,例如 图—密文 所示



图—明文


图—密文

完后,你可以解密,又回到原始的明文。 例如 图—原明文 所示

图—原明文

4 曾经有过的数据加密方法

数据加密研究了几十年,曾有过多种方法。 但有代表性的方法有两个:

其一,DES 方法,Data Encryption Standard —数据加密标准。

其二,RSA 方法,Rivest,Shamir,Adelman 的缩写。

5 DES 方法

1977 年美国国家标准局公布了 IBM 公司的一种数据加密算法,定名为

DES(数据加密标准)——Data Encryption Standard.

DES 是一种分组密码。

假设明文 m 是 0,1 组成的长度为 64 比特的符号串,密钥 k 也是 64 比特的 0,1 符号串。记

$m=m_1m_2m_3\cdots.m_{64}$

$k=k_1k_2k_3\cdots\cdots.k_{64}$

其中

m_i,k_i=0 或 1 I=1,2,……,64

DES 加密过程表达如下

$DES(m)=IP^{-1}.T16.T15\cdots\cdots.T1.IP\ (m)$

IP 是初始变换,IP^{-1} 是它的逆变换,

T16,T15,…….. ,T1 是变换。

DES 解密过程表达如下
DES=IP。T1。T2。。。。。。T16。IP
可以证明
$DES^{-1}(DES(m))=m$
$DES(DES^{-1}(m))=m$
举一例子:
明文: computer
密钥: program
用 ASCII 码表示
m=01100011 01101111 01101101 01110000
01110101 01110100 01100101 01110010
k=01110000 01110010 01101111 01100111
01110010 01100001 01101101
最后结果,密文
01011000 10101000 00000110 10111000
01101001 111111110 10101110 00110011
(* 以上计算过程从略,请看有关书籍)
DES 加密方法最大特点是加密 / 解密的密钥相同。
为了安全,密钥必须通过秘密方式传递。很不方便。
例如,网上有 n 个用户,则需要密钥个数为
C(n,2)=n/2*(n-1)
当 n=1000 时,C(1000,2)约 500000(50 万)。
这么多的密钥,很难管理。

6 RSA 方法

大约 1978 年前后,美国学者 Diffie,Hellman 发表论文“密码学新方向”提出公钥与私钥的思路。1980 年,Rivest,Shamir,Adleman 提出了 RSA 公钥密码系统,同时他们开办了同名的公司。

RSA 算法基于: 密码的安全性依赖于大数的因数分解的困难性。
通俗地说,一个大数要分解成两个因数相乘,是很困难的。
例如:43X59=2539 正向计算很容易
2539=43X59 逆向计算很困难
RSA 加密算法的过程描述如下:
(1)取 2 个素数 p 和 q ---------- 保密
(2)计算 n=pq ---------- 公开
(3)(n)=(p-1)(q-1) ---------- 保密
(4)随机取整数 e,满足 gcd(e, (n))=1---- 公开

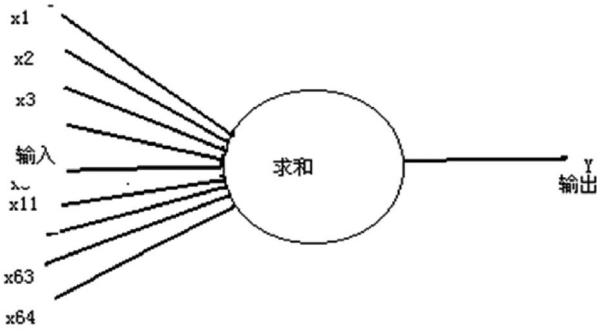


图 2 人工神经元示意图

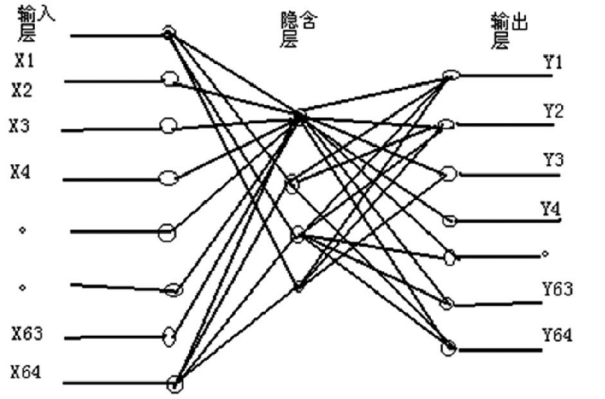


图 3 人工神经网络示意图

(5)计算 d,满足 de=1(mod (n))---------- 保密
加密算法 c=E(m)=m (mod n)
解密算法 m=D(c)=c (mod n)

7 数据加密新方法----人工神经网络方法

(1)人工神经元模型

目前使用的模型是 1943 年由 McCulloch 和 Pitts 提出的, 其模型如下:

神经元是一有 n 个输入和一个输出的元件, 其简图如图 2 所示。
其功能函数为:
y=f(x)=Sgn(W*x - θ)
Sgn(x)是符号函数,W 是权矩阵,θ是域值。
F(x) 理解为非线性变换,因为 sgn(.)非线性。

(2)人工神经网络

由若干个神经元按一定要求连接起来的网络, 称之为神经网络。
目前使用最多的人工神经元网络是三层前向网络。
三层前向神经网络简介
第一层是输入层(有 n 个输入节点, n 是输入向量 x 的维数)
第二层是隐含层(有 p 个神经元)
第三层是输出层(有 m 个神经元, m 是输出 y 的维数)
其结构如图 3 所示。

设计前向网络,主要是确定各层元件的个数, 确定各层的权和阈值,最后得到一个能完成指定变换功能:y=F(x)的转换器。

(3)前向神经网络的性能:

定理:三层前向神经网络具有万有性,即能构成由 Zn 到 Zm 的任一函数。

即任给一个由 $Z^n \rightarrow Z^m$ 的变换 G,则一定存在一个三层前向网络,网络对应的变换为:
y=G(x).
(此定理由张铃提出并验证)。

8 变换的思路

加密技术,无非是对给定明文,进行适当的变换,得到对应的密文,称之为加密。然后,对收到的密文,给出一办法,将密文转变成对应的明文,称之为解密。

一般,对明文都先将它分成若干段(每段长为 n),对每段进行加密…,这样每一段的明文,就是 Zn 上的一个点 x,对它加密,即将它变换成 Zm 上的一个点 y,于是加密过程,就是给出由 Zn —>Zm 的一个变换:y=H(x);解密,就是求其逆变换。
H':x=H'(y)
当然,要使解密后的明文无误,则要求 H 是一一对应的函数.

总之,加密在数学上看,只不过是求 Zn 到 Zm 的一个一一对应的函数而已。

另一方面,如前所述,三层前向神经网络的万有性知,三层前向神经网络能完成任何由 Zn —> Zm 的变换,故得下面的结论。

结论:任何一种(静态)加密技术,都可以用三层神经网络来实现。

这个结论说明用神经网络方法来构造加密技术的能力,远比以往的任何加密技术都强得多。以往的加密技术,如 DES 算法和 RSA 公开密钥体制等, 都只能构成很少一部分的加密技术(即只能构成 Zn 到 Zm 中的很少一部分的变换)。这也是我们提供的方法先进之处。

我们所说的“新型”,即当今世界上,没有人提出过,我们是首创 。

9 几个原理性问题的解释

a)速度问题:人工神经网络是并行计算。由此速度极快。
b)破解问题:人工神经网络方法由于先进,极难破解。
c)特点:
新型数据加密方法有如下几个特点:

(1)覆盖范围大:我们曾用严格的理论证明神经网络实现的数据加密具有“万有性”——可以实现任何的非线性变换。因此可以实现任何需求的加密方案。

(2)灵活性强:由于我们的实现中使用了三层神经网络技术,使得在密锁与密钥选择上有非常大的灵活性。

(3)破解难度高:设计的密锁与密钥具有极高复杂性,极难被破解。初步估算是 10^{260}

关于施工企业合同管理的探讨

杜慧丽[1] 陈龙[2]
(1.上海隧道工程股份有限公司 200082; 2.上海交通建设总承包有限公司 201208)

【摘要】本文针对我国施工企业面临建筑业市场化、工程管理国际化的形势,从合同管理的重要性入手,分析了施工企业合同管理的现状,对树立合同观念,加强合同意识,设立合同管理机构、培养合同管理人才,完善合同管理体系及合同管理制度,建立合同管理信息系统进行了探讨。
【关键词】施工企业 合同管理 现状
【中图分类号】F426.9 【文献标识码】A 【文章编号】1673-8209(2010)04-0243-01

1 引言

随着我国经济体制改革的逐步深入, 建筑市场逐步走向规范与完善。2004 年 11 月 11 日,中国正式加入 WTO 满 3 周年了,这意味着中国加入世贸组织后的 3 年保护过渡期结束,2004 年 12 月 11 日起建筑市场全面对外开放,中资、外资企业都将享受“国民待遇”。全球经济一体化是世界经济发展不可逆转的趋势,逐步对我国国民经济主要支柱的建筑业产生了重大影响,给国内建筑施工企业带来了较大的冲击, 另外,市场经济的一个主要特征就是它的法律强制性,因此在建筑领域逐渐出台了《合同法》、《招投标法》、《建筑法》等以合同为主要内容的法律。合同是联系各合同主体的纽带,任何一方违反合同,必然要受法律的制裁,从建筑市场总体情况来看,目前建筑市场竞争激烈,建筑企业利润减少,合同的风险加大。只有重视合同,重视合同管理,才能有效的降低工程风险,增加企业利润。

2 施工企业合同管理的现状

我国加入 WTO 后,施工企业与国际交往逐渐频繁,到国外承包的工程及在国内承包的国际投资项目也越来越多。严格的合同管理是这些国际工程的惯例,一般都严格使用 FIDIC 合同条件。

就目前国内施工企业合同管理的现状而言,主要存在以下几点问题:

(1)缺乏完全法制化的社会环境。建筑和合同法律体系不够完善,部分法律条文不够严谨,有空子可钻。另外,有法不依、执法不严的现象仍然存在。

(2)缺乏规范化的市场环境。业主利用买方市场的优势地位,提出苛刻的合同条件,施工单位为了生存不得不接受。业主在履行合同过程中随意性太强,存在不按合同、不按规则和惯例办事的现象。

(3)施工企业的合同法律意识和合同管理水平跟不上形势的发展。一般来说,施工企业管理层对投标、签约工作还比较重视,但合同履行过程中的监督、检查、统计、考核、奖惩还缺乏有效的措施和方法。

(4)合同管理人才缺乏,对合同管理人才培养不够重视。我国的合同管理起步较晚,合同管理人才缺乏。另外,由于外部环境不规范的因素太多,企业内部还没有形成重合同的意识和重视合同管理人才培养的环境。

在建筑市场上,不慎签订的一个合同就有可能给企业造成重大损失甚至面临破产的窘境,因此,施工企业必须加强合同管理,以提高企业的生存能力和抗风险能力。

3 加强合同管理的几点建议

3.1 树立合同观念,加强合同意识

企业要对管理人员加强法制教育,特别是企业负责人、项目负责人、合同管理人员,不但要学习《建筑法》,更要学习《招标投标法》、《合同法》,使他们在工程项目管理中处处以合同为依据,以合同管理为中心,只有这样,才能按合同办事,才能拿起法律的武器维护自身的合法权益。在国际工程中,合同管理更是项目管理的核心,尤其对承包商来讲,可以说其合同管理直接关系到项目实施是否顺利,自身的利益能否得到保护。

3.2 设立合同管理机构、培养合同管理人才

一个合理的合同管理机构,以及对合同管理部门的权责及与其它职能部门之间的界面的合理界定,是合同管理成功与否的关键;合同管理人才,需要素质高、学习能力强、知识面广、责任心强,需进行在职培训,组织专题学习和讨论,学习的内容有《合同法》、建设工程施工合同示范文本、《最高法院关于审理建设工程施工合同纠纷案件适用法律若干问题的解释》等;建立有效交流渠道,以达到互相促进、互补不足的目的,明确合同管理人员的责权利,建立完善岗位竞争机制和奖惩机制,以机制促进人,

3.3 建立和完善企业的合同管理体系及合同管理制度

施工企业就合同管理全过程的每个环节建立和健全具体的可操作制度没,这些环节应包括:介绍信的开具、信息的跟踪、合同的草拟、洽谈、评审、用印、交底、责任分解、履约跟踪、变更、索赔、违约、解除、终止等。使合同管理有章可循,规范合同签订程序,减少失误。

3.4 建立合同管理信息系统

信息是合同管理的窗口。为了能及时掌握合同的实施情况,合同文件、变更记录、补充协议、会议纪要、各方的来往函件等文件要及时传递给合同管理人员,在信息技术高速发展的今天,合同管理应建立在信息管理的基础上,施工企业要充分利用网络的优势进行合同管理,可以建立局域网,信息网站等。

4 总结

合同管理是一项高智能的工作,是一个复杂的体系,是项目管理的核心。面对我国建筑领域市场化的推进以及我国建筑业国际化的趋势,没有有效的合同管理,就不能实行有效的工程项目管理,就不能顺利的完成工程预期目标,施工企业必须加强合同意识,只有合同管理规范化,才能在激烈的市场竞争中生存和发展。

参考文献

[1] 金芳,工程量清单计价模式下施工企业的策略研究[D].武汉理工大学硕士论文,2005.
[2] 韩风光,中小施工企业合同管理研究[J].中国科技论文在线.
[3] 朱小林,论如何加强建设工程合同管理[J].经济建筑,2006(9).
[4] 王才旭,试论建筑施工企业面临国际竞争的对策[J].四川建筑,2005(6).

---

(4)易于硬件实现,运行速度快:人工神经网络计算机与当今冯·诺意曼体系计算机最大区别是并行性。并行计算优势为快速。例如 30 个城市的“巡回售货员问题”,用目前计算机算,大约要 3 年,若用 Hopfield 人工神经网络模型计算只要 2 秒钟。可见其速度之差有多大。

(5)应用领域广:数据加密不但在电子邮件可用,其实在非常广泛领域有用。尤其在 Internet 飞速发展的时代,更为重要。在银行、邮电、法院、公安、通信,甚至娱乐业也需要。

(6)发展前景宽广:神经网络有广阔的发展前景,例如反馈网络的应用,可把加密方法做得极其复杂,从而增加破解的难度,使加密技术上更高的层次。

10 示范表演软件

国内的兴趣者可以到网站上,下载表演软件 。

例如:华军网站

http://www.onlinedown.net/soft/19520.htm

也可以在百度搜索—》“数据加密工具 1.0”

即可在许多网站中得到答案。

也可以给作者发邮件:zpxm317@hotmail.com

11 未来的设想

我们想利用硬件实现加密,一是体现人工神经网络的优势,二是加快加密速度。

参考文献

[1] 张铃,张钹:人工神经网络理论及应用,1997,浙江科学技术出版社.
[2] 张平,张铃:电子信封(数据加密)软件,1999.