广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):249~251
Vol. 23,No. 4 November 2007

基于中国剩余定理的一种加密算法
An Encryption Algorithm Based on the Chinese Surplus Theorem

张皓翔
ZHANG Hao-xiang

(北京交通大学电子信息工程学院,北京 100044)
(School of Electronics and Information Engineering,Beijing Jiaotong University,Beijing,100044,China)

摘要:在分析论证和推广中国剩余定理的基础上,提出一种新的网络信息加密算法,并用实例说明新算法合理实用.

关键词:信息安全 密钥 算法 中国剩余定理
中图法分类号:TP301.6 **文献标识码**:A **文章编号**:1002-7378(2007)04-0249-03

Abstract: This paper presents the encryption algorithm based on the Chinese surplus theorem,and examples are given to show its rationality and practicability.

Key works: information security, key, algorithm, Chinese surplus theorem

随着互联网的普及,网络安全日益成为困扰互联网发展的瓶颈之一.为了保障信息安全,许多学者在加密算法方面进行了研究.于卫平[1]进行了基于离散 Hopfield 神经网络的数据加密算法研究;张健和周洁敏[2]进行了基于 TMS320C54x DSP 的加密算法研究;陈永强[3]进行了混沌加密算法研究.本文在分析论证和推广中国剩余定理的基础上,根据中国剩余定理提出一种网络信息加密算法.

1 中国剩余定理分析

1.1 定理概述

举世闻名的中国剩余定理最早以"物不知其数"的问题载于《孙子算经》中[4],该问题可以理解为:一个数除以 3 余 2,除以 5 余 3,除以 7 余 2,求适合这些条件的最小的自然数.用现代数学符号表示,即已知

$$N \equiv 2(\mathrm{mod}3) \equiv 3(\mathrm{mod}5) \equiv 2(\mathrm{mod}7).$$

求最小的正整数,答案是 $N = 23$.

《孙子算经》的解法是:"术曰:三三数之剩二,置一百四十;五五数之剩三,置六十三;七七数之剩二,置三十;并之,得二百三十三,以二百一十减之即得.凡三三数之剩一,则置七十;五五数之剩一,则置二十一,七七数之剩一,则置十五.一百六以上,以一百五减之即得."

1.2 定理的数学论证

把"物不知其数"问题推广到一般情况[5]:设 a、b、c、d 为非负整数,且 a 为某个数除以 3 的余数,b 为这个数除以 5 的余数,c 为这个数除以 7 的余数,试求符合条件的最小的数 m.按《孙子算经》的解法有

$$m = 70a + 21b + 15c - 105d.$$

我们可以证明,因为 $m = 70a + 21b + 15c - 105d$ 可改写为 $m = (69a + 21b + 15c - 105d) + a$.又因为 $3|(69a + 21b + 15c - 105d)$ 且 $0 \leqslant a \leqslant 2$,所以 m 除以 3 的余数必为 a,同理可得 m 除以 5 的余数必为 b,m 除以 7 的余数必为 c.又因为 $[3,5,7] = 105$,所以 m 减去 105 的整数倍就能得到符合题意的最小的自然数.

1.3 定理推广

1.3.1 以 3,5,7 为例来总结一般的规律

设 X_1 表示能被 5 和 7 整除的所有整数,Y_1 表示能被 5 和 7 整除且除以 3 余 1 的所有整数,X_2 表示能被 3 和 7 整除的所有整数,Y_2 表示能被 3 和 7 整除且除以 5 余 1 的所有整数,X_3 表示能被 3 和 5 整除的所

收稿日期:2007-08-15
作者简介:张皓翔(1985-),男,主要从事计算机信息安全研究.

有整数，Y_3表示能被3和5整除且除以7余1的所有整数，则可得表1和表2.

表1 满足X_1,X_2,X_3的正整数

条件	正整数	一般表达式*
X_1	35,70,105,140,175,210,245,280…	$35\times n$
X_2	21,42,63,84,105,126,147,168 …	$21\times n$
X_3	15,30,45,60,75,90,105,120 …	$15\times n$

*n表示任意一个正整数.

表2 满足Y_1,Y_2,Y_3的正整数

条件	正整数	一般表达式*
Y_1	70,175,280 …	$70+3\times5\times7\times n$
Y_2	21,126,251 …	$21+3\times5\times7\times n$
Y_3	15,120,245 …	$15+3\times5\times7\times n$

*n表示任意一个正整数.

从表1和表2中可以看出表1中的黑体数字就是Y_1,Y_2,Y_3中的数，其中70,21,15分别是表2中满足条件Y_1,Y_2,Y_3的最小的正整数.若令

$$Y=Y_1+Y_2+Y_3=70+21+15+3\times5\times7\times n=106+105\times n,$$

Y就是《孙子算经》解法的后半部分答案.答案不唯一，106只是其中的一个而已.

1.3.2 将3,5,7推广到n个素数

设$A_1,A_2,A_3,\cdots,A_n$为n个互质的素数.若已知一个整数Y除以$A_1,A_2,A_3,\cdots,A_n$余数分别为$B_1,B_2,B_3,\cdots,B_n$，求Y.

令$M=A_1\times A_2\times A_3\times\cdots\times A_n$，

X_1表示能被$A_2,A_3,\cdots,A_n$整除的所有整数，

Y_1表示能被$A_2,A_3,\cdots,A_n$整除且除以A_1余B_1的所有整数，

X_2表示能被$A_1,A_3,\cdots,A_n$整除的所有整数，

Y_2表示能被$A_1,A_3,\cdots,A_n$整除且除以A_2余B_2的所有整数，

⋮

X_i表示能被$A_1,A_2,A_3,\cdots,A_{i-1},A_{i+1},\cdots,A_n$整除的所有整数，

Y_i表示能被$A_1,A_2,A_3,\cdots,A_{i-1},A_{i+1},\cdots,A_n$整除且除以$A_i$余$B_i$的所有整数，

那么

$X_1=A_2\times A_3\times\cdots\times A_n\times m=M\times m/A_1$，$X_2=A_1\times A_3\times\cdots\times A_n\times m=M\times m/A_2,\cdots,X_n=A_1\times A_2\times\cdots\times A_{n-1}\times m=M_m/A_n$，其中$m$为任意整数.

设F_i满足X_i和Y_i，且令其为Y_i中最小的正整数，其中$1\leqslant i\leqslant n$则$Y_1=F_1+A_1\times A_2\times\cdots\times A_n\times m=F_1+M\times m,\cdots,Y_n=F_n+A_1\times A_2\times\cdots\times A_n\times m=F_n+M\times m$.那么$Y=Y_1+Y_2+Y_3+\cdots+Y_n=F_1+F_2+\cdots F_n+M\times m$.

2 加密算法

根据中国剩余定理，可以得出一种新的网络信息加密算法.以下若无特别说明，所用符号均与前述相同.

2.1 加密和解密分析

用Y表示明文，是所要隐蔽和保护的机要消息.用$B_1,B_2,B_3,\cdots,B_n$表示密文，要把明文转换成一种隐蔽的形式.$A_1,A_2,A_3,\cdots,A_n$和N为密钥.

加密算法的步骤如下.

步骤1：选出n个素数$A_1,A_2,A_3,\cdots,A_n$作为"密钥"；

步骤2：求出这n个素数的乘积M；

步骤3：求出$F_1,F_2,F_3,\cdots,F_n$；

步骤4：由$Y=Y_1+Y_2+Y_3+\cdots+Y_n=F_1+F_2+F_3+\cdots+F_n+M\times m$得出

$$N=[Y-(F_1+F_2+F_3+\cdots+F_n)]/M;$$

步骤5：用Y分别除以$A_1,A_2,A_3,\cdots,A_n$得余数$B_1,B_2,B_3,\cdots,B_n$，并把它们作为密文；

解密算法的步骤如下.

已知密文$B_1,B_2,B_3,\cdots,B_n$和密钥$A_1,A_2,A_3,\cdots,A_n$及N算出$F_1,F_2,F_3,\cdots,F_n$.

由$Y=Y_1+Y_2+Y_3+\cdots+Y_n=F_1+F_2+F_3+\cdots+F_n+M\times m$得出$Y$.

这样就实现了从密文和密钥到明文的整个解密过程.

2.2 加密和解密举例

例1 加密

令明文$X=2001$，密钥为5,7,11，密文为1,6,10可求出$F_1=231,F_2=55,F_3=175$，那么$m=[2001-(231+55+175)]/(5\times7\times11)=4$为另一密钥.

例2 解密

$Y=Y_1+Y_2+Y_3+\cdots+Y_n=F_1+F_2+F_3+\cdots+F_n+M\times m=221+175+55+5\times7\times11\times4=2001.$

3 结束语

基于中国剩余定理的加密算法完全可以用简单的C程序来实现.如果使用的n个素数$A_1,A_2,A_3,\cdots,A_n$足够分散，得到的乘积足够大，那么可以计算这种加密算法复杂度为$O(m^3)$.新加密算法完全合

理、有效.

参考文献:

[1] 于卫平. 基于离散 Hopfield 神经网络的数据加密算法研究[J]. 湖南理工学院学报:自然科学版,2007(3):24-25,94.

[2] 张健,周洁敏. 基于 TMS320C54x DSP 的加密算法设计[J]. 电子元器件应用,2006(3):67-69.

[3] 陈永强. 一种基于混沌加密的自适应图像水印方法[J]. 计算机应用,2007(10):2453-2455.

[4] 潘天骥. 论述中国剩余定理的形成及其影响[J]. 九江师专学报:自然科学版,1987,5(1):1-4.

[5] 曹珍富. 公钥密码学[M]. 哈尔滨:黑龙江出版社,1993:2.

(责任编辑:尹 闯 邓大玉)

(上接第 248 页)

```
        exit(1);
    }
    dict x;
    cout<<"请输入明文字符与密文字符的对应表形成密码本文件,按 Ctrl+z 键结束:"<<endl;
    while (cin>>x.source) {
        cin>>x.secret;
        fout.write((char *)&x,sizeof(x));
    }
    fout.close();
    cout<<"输入结束并已在 F 盘形成密码本文件。"<<endl;
};
void main() {//主程序模块
    readdictionary( );//调用读密码本文件模块
    cout<<"请按下列菜单选择功能:"<<endl;
    cout<<"1——加密    2——解密    3——建立密码本    0—退出"<<endl;
    cout<<"请选择(0————3):";
int i;
    cin>>i;
    switch(i) {
    case 1:
        encryption(diction1,diction2);//加密
        break;
    case 2:
        decryption(diction2,diction1);//解密
        break;
    case 3:
        mimazidian();//生成密码本文件
        break;
    case 0:
        return;
    }
}
```

4 结束语

本文用 C++语言给出了一种加密解密置换算法的具体实现,探讨了西文字符的加密解密问题,但本算法可以扩展到中文甚至其他文字的加密与解密,但是这方面的加密解密问题稍微复杂一些,有待进一步探讨。

参考文献:

[1] WADE TRAPPE, LAWRENCE C WASHINGTON. 密码学概论[M]. 北京:人民邮电出版社,2004.

[2] 范辉,谢青松. 操作系统原理与实训教程[M]. 第 2 版. 北京:高等教育出版社,2006.

[3] 汤子瀛. 计算机操作系统[M]. 西安:西安电子科技大学出版社,2002.

[4] 甘仞初. 信息系统原理与应用[M]. 北京:高等教育出版社,2004.

[5] RICHARCL C LEINECKER, TOM ARCHER. Visual C++6 宝典[M]. 北京:电子工业出版社,2001.

(责任编辑:韦廷宗)