华南农业大学学报　19(3)　1998: 126
J. South China Agric. Univ.

三维综合加密算法的设计与分析

王美华
(华南农业大学理学院, 广州, 510642)

DESIGN AND ANALYSIS OF THREE-DIMENSIONAL MULTIENCRYPTICAL ALGORITHM

Wang　Meihua
(College of Sciences, South China Agric. Univ., Guangzhou, 510642)

关键词　数据加密; 棋盘密码; 魔方密码; 转动魔方加密方
Key words　data encryption; square cipher; magic cube cipher; enciphering method of rotating magic cube
中图分类号　O157.4

信息数据加密技术已随计算机技术的迅猛发展, 伸展到交通、工业经济、科学技术、社会安全和公共生活的各个领域, 成为现代社会中保护信息的重要手段和工具. 信息保护的现实需要, 使利用数据加密算法和技术迅速进入了现代社会, 计算机技术和通信领域的专业技术人员和广大用户迫切需要了解并有效使用数据加密技术.

1　三维加密

其主要思想是把字母对照表放入 3×3×3 三维矩阵(魔方)中, 将 26 个字母加上空格" #"放入. 产生密钥表(见表 1).

特别地, 也可以引入以某个字或某个单词作为密钥, 如 china 作为密钥, 则可先将 china 这 5 个字母(重复字母只写 1 个)依次填入表 1, 然后其它字母按顺序依次填充.

表 1　三维密钥对照表

a	000	h	012	o	121	v	201
b	010	i	022	p	102	w	211
c	020	j	100	q	112	x	221
d	001	k	110	r	122	y	202
e	011	l	120	s	200	z	212
f	021	m	101	t	210	#	222
g	002	n	111	u	220		

2　转动魔方加密方法设计

为了进一步增加迷惑性, 笔者将魔方转动. 现将魔方置于一个坐标系上. 每一个字母用其坐标(x, y, z)表示, x, y, z 在{0, 1, 2}上取值. 魔方在 3 个坐标轴的垂直方向上均有 3 个面块魔方是可以转动的, 每次转动, 只能是 1 个面块的转动, 假设 z 不变, 转动后坐标(x', y'), 则可得 $x'=y$, y'取值则由 x 的值不同而不同. 当 $x=2$ 时, 则 $y'=0$; 当 $x=1$ 时, $y'=1$; 当 $x=0$ 时, 则 $y'=2$. 事实上在每个方向上可以转动 90°、180°、270°.

3　魔方转动指令设计

考虑到魔方转动是一个面块接一个面板地转动, 可以设计面板转动, 魔方转动指令由 1 组面板转动指令组成.

于是面转动指令用(d, s, n)向量表示: d—转动轴方向, 取 0、1、2 三个值, 分别表示为垂直 X、Y、Z 轴方向上的面板; s—转动面板, 取 0、1、2 三个值, 分别表示为转动垂直该方向上的 3 个面板中越来越远离原点的面板; n—转动角, 取 0、1、2 三个值分别表示转动 90°、180°、270°三种角度. 于是可得一串由一组转动指令组成的魔方转动指令设计(d_1, s_1, n_1, d_2, s_2, n_2, …, d_m, s_m, n_m)

4　结束语

本文在原先二维加密的基础上, 引申成为三维加密, 将"魔方"采用多种变换, 并已经设计出相应的加密解密软件, 使其加密算法复杂化, 从而提高密文的不可懂性.

1997-09-02 收稿　王美华, 女, 28 岁, 助理实验师, 学士
【责任编辑　张　砺】