网络与信息安全概论（10） —— 习题与思考题

**1.使用L函数进行替换：**

（1）{c1000000}变换结果为：C5C20707

（2）{80000000}变换结果为：80820202

**2.证明表一的正确性。**

（1）对每一个用户的输入字，使用程序输出其输出字：

答：此题和第一题是相同题目，所以：

当输入为{c1000000}时，其变换结果为：C5C20707

当输入为{80000000}时，其变换结果为：80820202

（2）对用户的每一个输入模式，输出其可能的输出模式

当输入模式为6=（0110）时，其可能的输出模式为：

* {0111}
* {1011}
* {1101}
* {1110}
* {1111}

**思考题：证明：上的8\*8矩阵的个数为：**

证：该题可以推广为，求有限域上n阶矩阵的可逆矩阵的个数。

设q为质数幂，Fq表示有限域GF(q)。A为Fq上的n阶方阵，其行列式定义为detA。令

显然，非空且有限。对于,于是关于矩阵的乘法是一个有限群。关于群的阶有

定理：群的阶数

证明：令集合

显然为的子群。任取,集合中任一元的第一行均与X的第一行相同，则有，于是有，其中。因此，在中，可用矩阵第一行相同与否交分成陪集，陪集个数为选之总数，并要减去一个的情况，所以有

任取，则

其中，

由共有种取法，所以

从而

反复利用上式，可得：

证毕。

通过群定理，对8阶矩阵而言，，其可逆矩阵个数为：

展开该式得

证毕。

附录：下图为程序运行的结果，表一的验证结果存储于csv文件中。