# 第一次作业

# 作业1-习题1-3

① 对于如下方程，求对应的满足方程的最小正整数x:

a. $5x \equiv 4 \pmod 3$

b. $7x \equiv 6 \pmod 5$

② 有多少种仿射密码?

③ 求$Z_5$中各个非零元素的乘法逆元

# 作业1-习题4

④ 《密码编码学与网络安全》P61页，习题3.10

a. 用密钥largest构造一个Playfair矩阵。

b. 用密钥occurrence构造一个Playfair矩阵。对密钥中的冗余字母的处理方法做出合理的假设。

# 作业1-习题5

## ⑤ 《密码编码学与网络安全》P61页，习题3.11

a. 使用Playfair矩阵

| | | | | |
|---|---|---|---|---|
| M | F | H | I / J | K |
| U | N | O | P | Q |
| Z | V | W | X | Y |
| E | L | A | R | G |
| D | S | T | B | C |

加密消息

Must see you over Cadogan West. Coming at once.

b. 用习题3.10(a)中的Playfair矩阵重做习题3.11(a)

c. 对这个习题的结果你如何解释？

# 作业1-习题6~7

⑥

密文为 $c$，明文为 $m$，26 个字母编号为 0~25，加密算法为 $c=7m+11(\mathrm{mod}26)$，当明文为 hello 时，对应的密文是什么？

⑦ 设 π 为集合{1, …, 8}上的置换：

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\pi(x)$ | 4 | 1 | 6 | 2 | 7 | 3 | 8 | 5 |

求出逆置换 $\pi^{-1}$

# 作业1-习题8

⑧

使用穷尽密钥搜索法，破译如下列用移位密码加密的密文：

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

**备注：编程题一般要求给出带注释的源程序及测试样例及结果，以后题目参考此备注**

# 作业1-习题9

⑨ 《密码编码学与网络安全》P63页，编程题3.5

- 编写一个程序，实现2*2Hill密码的加解密算法

# 提交要求

- 通过教学网提交，由助教邹远鑫负责批改
- 如果包含多个文件，压缩为一个文件，提交作业的文件名采用“学号+姓名+第几次作业”
- 例 “1300048400杨帆第1次作业.rar”
- 按时提交截止时间:10月9日23：30前提交