第一次书面作业
参考答案

作业1-习题1

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

解答：

a. x=2

b. x=3

作业1-习题2

② 有多少种仿射密码?

- e(x) = ax + b (mod m)
- a的取值有12个可能(1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25).
- b的取值有 26个可能，从0到25，因此总的仿射变换是 12 × 26 = 312.（包含一个自身映射到自身的变换）

作业1-习题3

③ 求Z_5中各个非零元素的乘法逆元

- $1 \times 1 \equiv 1 \pmod 5$
- $2 \times 3 \equiv 1 \pmod 5$
- $3 \times 2 \equiv 1 \pmod 5$
- $4 \times 4 \equiv 1 \pmod 5$
- $1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$

作业1-习题4

④ 习题3.10《密码编码学与网络安全》P61页

a. 用密钥largest构造一个Playfair矩阵。

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

作业1-习题4

④ 习题3.10《密码编码学与网络安全》P61页

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。

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

作业1-习题5

⑤ 习题3.11《密码编码学与网络安全》P61页

a. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

b. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

c. 行或列的循环移位导致等价的代替，在这一情形中，是对问题3.10a的矩阵按列移一位，按行移三位。

作业1-习题6

- h 7 $7\times7+11 \pmod{26}=8$ i
- e 4 $4\times7+11 \pmod{26}=13$ n
- l 11 $11\times7+11 \pmod{26}=10$ k
- l 11 $11\times7+11 \pmod{26}=10$ k
- o 14 $14\times7+11 \pmod{26}=5$ f

- hello → inkkf

作业1-习题7

设 π 为集合{1,…,8}上的置换:

x	1	2	3	4	5	6	7	8
Π(x)	4	1	6	2	7	3	8	5

逆置换 π^{-1}

x	1	2	3	4	5	6	7	8
Π(x)	2	4	6	1	8	3	5	7

作业1-习题8

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJII KFUHCQD

m=lookup in the air its a bird its a plane its superman

作业1-习题9

⑨　编程题3.5《密码编码学与网络安全》P63页

- 3.5编写一个程序，实现2*2Hill密码的加解密算法