1.1 (a) $7503 \bmod 81 = 51$

(b) $(-7503) \bmod 81 = 30$

(c) $81 \bmod 7503 = 81$

(d) $(-81) \bmod 7503 = 7422$

1.5 经穷尽，可得明文为 lookupintheairitsabirditsaplaneitssuperman

加入标点和空格后为 look up in the air, it's a bird, it's a plane, it's superman.

1.6 $e_K(x) = (x+K) \bmod 26$

$d_K(y) = (y-K) \bmod 26$

若 $e_K(x) = d_K(y)$，则 $e_K(e_K(x)) = x$

$\therefore [((x+K) \bmod 26) + K] \bmod 26 = x$

$\therefore x = 0$ 或 13

1.7 ① $m = 30$

$30 = 2 \times 3 \times 5$ $\therefore \phi(m) = (2^1-2^0) \times (3^1-3^0) \times (5^1-5^0) = 8$

$\therefore$ 量为 $8 \times 30 = 240$

② $m = 100$

$100 = 2^2 \times 5^2$ $\therefore \phi(m) = (2^2-2^1) \times (5^2-5^1) = 40$

$\therefore$ 量为 $40 \times 100 = 4000$

③ $m = 1225$

$1225 = 5^2 \times 7^2$ $\therefore \phi(m) = (5^2-5^1) \times (7^2-7^1) = 840$

$\therefore$ 量为 $840 \times 1225 = 1029000$

1.9

$1^{-1} = 1$
$2^{-1} = 15$
$3^{-1} = 10$
$4^{-1} = 22$
$5^{-1} = 6$
$6^{-1} = 5$
$7^{-1} = 25$
$8^{-1} = 11$
$9^{-1} = 13$
$10^{-1} = 3$
$11^{-1} = 8$
$12^{-1} = 17$
$13^{-1} = 9$
$14^{-1} = 27$
$15^{-1} = 2$
$16^{-1} = 20$
$17^{-1} = 12$
$18^{-1} = 21$
$19^{-1} = 26$
$20^{-1} = 16$
$21^{-1} = 18$
$22^{-1} = 4$
$23^{-1} = 24$
$24^{-1} = 23$
$25^{-1} = 7$
$26^{-1} = 19$
$27^{-1} = 14$
$28^{-1} = 28$

1.10

(1) $a=5 \quad \therefore a^{-1}=6$

$\therefore d_k(y)=6(y-21) \bmod 29=(6y+19) \bmod 29$

$\therefore$ 为 $(6y+19) \bmod 29$

(2) $\forall x \in Z_{29}$

若证 $d_k(e_k(x))=6\times((5x+21) \bmod 29-21) \bmod 29$

$=6\times 5x \bmod 29$

$\because 6=5^{-1}$

$\therefore 6\times 5x \bmod 29=x$

1.15

(a) $A=\begin{pmatrix}2 & 5\\ 9 & 5\end{pmatrix} \qquad A^{-1}=\begin{pmatrix}5 & 17\\ 21 & 2\end{pmatrix}$

1.16

(a)

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

(b) 由密钥 $\pi$ 可得明文为 gentlemen do not read each other's mail

1.18

① (0,0,0,0)

序列：8,0,0,0,0,0…

T=1

② (0,0,0,1)

序列：[0,0,0,1,1],0,0,0,1,1,0…

T=5

③ (0,0,1,0)

序列：[0,0,1,0,1],0,0,1,0,1,…

T=5

④ (0,0,1,1)

序列：[0,0,1,1,0],0,0,1,1,0,0,…

T=5

⑤ (0,1,0,0)

序列：0[1,0,0,1,0],1,0,0,1,0,…

T=5

⑥ (0,1,0,1)

序列：0[1,0,1,0,0],1,0,1,0,0,…

T=5

⑦ (0,1,1,0)
序列 = [0,1,1,0,0],0,1,1,0,0,…
T = 5

⑧ (0,1,1,1)
序列 = [0,1,1,1,1],0,1,1,1,1,0…
T = 5

⑨ (1,0,0,0)
序列 = 1,[0,0,0,1,1],0,0,0,1,1,…
T = 5

⑩ (1,0,0,1)
序列 = 1,[0,0,1,0,1],0,0,1,0,1,…
T = 5

⑪ (1,0,1,0)
序列 = [1,0,1,0,0],1,0,1,0,0,…
T = 5

⑫ (1,0,1,1)
序列 = [1,0,1,1,1],1,0,1,1,1,…
T = 5

⑬ (1,1,0,0)
序列 = [1,1,0,0,0],1,1,0,0,0,…
T = 5

⑭ (1,1,0,1)
序列 = [1,1,0,1,1],1,1,0,1,1,…
T = 5

⑮ (1,1,1,0)
序列 = 1,1[1,0,1,1,1],1,0,1,1,1,…
T = 5

⑯ (1,1,1,1)
序列 = [1,1,1,1,0],1,1,1,1,0,…
T = 5

1.19

① (0,0,0,0)
序列 = 0,0,0,0,0,0,…
T = 1

② (0,0,0,1)
序列 = [0,0,0,1,0,1],0,0,0,1,0,1,…
T = 6

③ (0,0,1,0)
序列 = [0,0,1,0,1,0],0,0,1,0,1,0,…
T = 6

④ (0,0,1,1)
序列 = [0,0,1,1,1,1],0,0,1,1,1,1,…
T = 6

⑤ (0,1,0,0)
序列 = [0,1,0,0,0,1],0,1,0,0,0,1,…
T = 6

⑥ (0,1,0,1)
序列 = [0,1,0,1,0,0],0,1,0,1,0,0,…
T = 6

⑦ (0,1,1,0)
序列 = [0,1,1],0,1,1,0,1,1,0,1,1,…
T = 3

⑧ (0,1,1,1)
序列 = [0,1,1,1,1,0],0,1,1,1,1,0,…
T = 6

⑨ (1,0,0,0)

序列：[1,0,0,0,1,0],1,0,0,0,1,0,...

T=6

⑩ (1,0,0,1)

序列：[1,0,0,1,1,1],1,0,0,1,1,...

T=6

⑪ (1,0,1,0)

序列：[1,0,1,0,0,0],1,0,1,0,0,0,...

T=6

⑫ (1,0,1,1)

序列：[1,0,1],1,0,1,1,0,1,1,0,1,...

T=3

⑬ (1,1,0,0)

序列：[1,1,0,0,1,1],1,1,0,0,1,1,...

T=6

⑭ (1,1,0,1)

序列：[1,1,0],1,1,0,1,1,0,1,1,0,...

T=3

⑮ (1,1,1,0)

序列：[1,1,1,0,0,1],1,1,1,0,0,1,...

T=6

⑯ (1,1,1,1)

序列：[1,1,1,1,0,0],1,1,1,1,0,0,...

T=6

补充题：

1、安全密码算法的关键特征

计算安全性：破解所需计算量超出实际可行范围（如需要数千年计算时间）

数学坚固性：基于经过严格验证的数学难题（如大数分解、离散对数），算法设计没有数学上的弱点或捷径

抵抗已知攻击：能抵抗所有已知类型的密码分析（如差分分析、线性分析、侧信道攻击等），经过密码学界广泛审查和验证

可证明安全性：最好能归约到某个已被证明困难的数学问题或证明破解算法等价于解决某个公认的难解问题

2、实际应用中的安全考量

参数选择安全：密钥长度足够抵抗当前和可预见未来的计算能力，所有参数选择都有明确的安全边界

实现安全性：算法实现不会引入新的弱点，抵抗时序攻击、能量分析等侧信道攻击

协议安全性：在完整协议环境中仍保持安全，不会因为使用方式不当而产生漏洞