秋许密码学

~~第一单元~~第一章

1.1. (a) $7503 \bmod 81 = 57$

(b) $-7503 \bmod 81 = -51 + 81 = 30$

(c) $81 \bmod 7503 = 81$

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

1.5. BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIkFUHCQD

~~k=1 addzjexciwtpxqgxi~~
~~addzjexciwtpxqgxi~~

~~2 zcc~~

~~3 ybb~~

~~4 xaa~~

~~5 wzz~~

~~6 vyy~~

~~7 uxx~~ ~~k=17~~

~~8 tww~~

~~9~~

k=1 . addzjexciwtpxqxihpqxgsxihpeapctxihhjetgbpc.

k=2 zcc...

k=3 ybb...

k=4 xaa...

k=5 wzz...

k=6 vyy...

k=7 uxx...

k=8 tww...

k=9 svv...

k=10 ruuqaot...

k=11 qtt...

k=12 pssoytmar...

k=13 orrnxslq...

k=14 nqqmw...

k=15 mpplvq...

k=16 lookupintheair:itssabinditsaplaneitssuperman.

~~k=17~~

∴k=16

1.6. $e_k(x) = (x+k) \bmod 26$

$d_k(y) = (y+k) \bmod 26$

$d_k(e_k(x)) = [(x+k) \bmod 26) + k] \bmod 26 = x$

$(x+26k) \bmod 26 = x$

$x \equiv x + 26k \bmod 26$

k=0 或 13.

1.7. ~~m=30~~. $e_k(x) = (ax+b) \bmod m$

$\gcd(a, m) = 1$

密钥空间为 $\phi(m) \cdot m$.

m=30. ~~$\phi(30)$~~ $30 = 2^1 \times 3^1 \times 5^1$ $\phi(30) = 1 \times 2 \times 4 = 8$ $\phi(30) \cdot 30 = 240$

$m = 100 = 2 \times 50 = 2 \times 2 \times 25 = 2^2 \times 5^2$ $\phi(100) = (4-2)(25-5) = 40$. $\phi(100) \cdot 100 = 4000$

$m = 1375 = 5^2 \times 7^2$ $\phi(1375) = (25-5)(49-7) = 840$ $\phi(1375) \cdot 1375 = 1029000$

∴ m=30. 100. 1375 的密钥量为 240. 4000. 1029000

1.9. $1 \le a \le 28$ $a^{-1} \bmod 29$ ∵ 29为素数

∴ $\gcd(a, 29) = 1$

$1^{-1} = 1$ $6^{-1} = 5$ $11^{-1} = 8$ $16^{-1} = 20$ $21^{-1} = 18$ $26^{-1} = 19$

$2^{-1} = 15$ $7^{-1} = 25$ $12^{-1} = 17$ $17^{-1} = 12$ $22^{-1} = 4$ $27^{-1} = 14$

$3^{-1} = 10$ $8^{-1} = 11$ $13^{-1} = 9$ $18^{-1} = 21$ $23^{-1} = 24$ $28^{-1} = 1$

$4^{-1} = 22$ $9^{-1} = 13$ $14^{-1} = 27$ $19^{-1} = 26$ $24^{-1} = 23$

$5^{-1} = 6$ $10^{-1} = 3$ $15^{-1} = 2$ $20^{-1} = 16$ $25^{-1} = 7$

1.10. $k = (5, 21)$ $\mathbb{Z}_{29}$

(a) $e_k(x) = (5x + 21) \bmod 29$

$a = 5, \ b = 21$

$a^{-1} = 6, \ b$

$d_k(y) = 6(y - 21) \bmod 29 = 6y - 10 = 6y + 19.$

~~$= 12y - 12 + 26 = 12y + 13.$~~

(b) 证: $\forall x \in \mathbb{Z}_{29}, \ d_k(e_k(x)) = x$

$d_k(e_k(x)) = (6((5x + 21) \bmod 29) + 19) \bmod 29$

$= (30x + 126) \bmod 29 + 19$

$= x \bmod 29 + 29 = x$

1.15. (a) $K = \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$ $\det K = (2 \times 5 - 5 \times 9) \bmod 29 = (-35) \bmod 29 = 23$

$K^* = \begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 20 \\ 24 & 2 \end{pmatrix}$

$K^{-1} = (\det K)^{-1} \cdot K^* = 24 \begin{pmatrix} 5 & 20 \\ 24 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 16 \\ 25 & 19 \end{pmatrix}$

1.16. (a)

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

(b) gent/lemen/do/not/read/each/ot/hers/mail.

1.18.

① $(z_1.z_2.z_3.z_4)=(0.0.0.0)$. $z_k=0$. $k\in Z^{+}$

② $(z_1.z_2.z_3.z_4)=(0001)$

0001 1/0011 T=5

∴ 0001. 0011. 0110. 1100. 1000. 周期都为5.

③ $(z_1.z_2.z_3.z_4)=(0010)$

0010 1/0010 T=5

∴ 0010. 0101. 1010. 0100. 1001 周期都为5

④ $z_1.z_2.z_3.z_4=0111$

0111 1/0111 T=5

∴ 0111. 1111. 1110. 1101. 1011 m周期都为5

综上. 当$(z_1z_2z_3z_4)=(0.0.0.0)$时周期为1. 其余均为5.

1.19. $z_{i+4}=(z_i+z_{i+3})\bmod 2$

① 0000 $z_k=0$. T=1

② ~~0001.~~ 0001. 0001.1110.1011.0010/0.0011.1100.~~1/0000.1111~~.

~~0001 0/0001 T=6~~ ~~1111~~ T=15.

~~∴ 0001. 0010. 0101. 1010. 0100. 1000 m周期为6~~ ∴ 0001. 0011. 0111. 1111. 1110. 1101.

1010. 0101. 1011. 0110. 1100. 1001

0010. 0100. 1000 m周期为15.

③ ~~0011~~

~~0011.1/0011 T=6~~

~~∴ 0011. 0111. 1111. 1110. 1100. 1001 T=6~~

④ ~~0110~~

~~0110.1/0110 T=5~~

~~∴ 0110. 1101. 1011. 0110. 1101. 1011. T=5~~

b3.1 安全m密码算法

- 必要条件是有足够大的密钥空间. 以拼穷举算法. (主要基于当前计算能力)
- 密文与密钥之间m关系~~很~~复杂 ~~明文的~~ 使每一位明文影响尽可能多位密文 从而令统计与分析更加困难
- 另外. 作为密码算法m充要条件是令明文与密文之间m对应关系两两相异.