

1. HAPPY BIRTHDAY

2. XLYAXLOLAXLYARZVU ;

3. a. E  $\Rightarrow$  Q

T  $\Rightarrow$  J

04  $\Rightarrow$  16

19  $\Rightarrow$  79

Linear cipher:  $C \equiv aP + b \pmod{26}$

$$16 \equiv 4a + b \pmod{24}$$

$$9 \equiv 19a + b \pmod{24} \Rightarrow$$

$$b \equiv 9 - 19a \pmod{24}$$

$$16 \equiv 4a + (9 - 19a) \equiv -15a + 9 \pmod{24}$$

$$7 \equiv -15a \equiv -15(3) \pmod{24}$$

$$\therefore a \equiv 3 \pmod{26}$$

$$16 \equiv 4(3) + b \equiv 12 + b \pmod{26}$$

$$\therefore b \equiv 16 - 12 \equiv 4$$

b. see attached javascript program.

4.

5. TH  $\Rightarrow$  HIO

HE  $\Rightarrow$  PP

19, 7  $\Rightarrow$  7, 14

7, 4  $\Rightarrow$  15, 15

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

a.

solved via Theorem 4.9

$$7 \equiv a \cdot 19 + b \cdot 7 \pmod{24}$$

$$14 \equiv c \cdot 19 + d \cdot 7 \pmod{24}$$

$$15 \equiv a \cdot 7 + b \cdot 4 \pmod{24}$$

$$15 \equiv c \cdot 7 + d \cdot 4 \pmod{24}$$

$$7 \equiv a \cdot 19 + b \cdot 7 \pmod{26} \quad \times 4 \Rightarrow$$

$$15 \equiv a \cdot 7 + b \cdot 4 \pmod{26} \quad \times 7 \Rightarrow$$

$$-77 \equiv 25 \equiv 1 \equiv 27a \equiv a \pmod{24}$$

$$\therefore a \equiv 20 \pmod{26}$$

$$(7 \cdot 7 - 15 \cdot 19) \equiv -236 \equiv -2 \equiv -27b \equiv -b \pmod{26}$$

$$\therefore b \equiv 2 \pmod{26}$$

$$14 \equiv c \cdot 19 + d \cdot 7 \pmod{24} \quad \times 4 \times 7$$

$$-15 \equiv c \cdot 7 + d \cdot 4 \pmod{24} \quad \times 7 \times 19$$

$$-49 \equiv 3 \equiv 27c \equiv c \pmod{24}$$

$$\therefore c \equiv 3 \pmod{26}$$

$$(14 \cdot 7 - 15 \cdot 19) \equiv -187 \equiv -5 \equiv -27d \equiv -d \pmod{24}$$

$$\therefore d \equiv 5 \pmod{26}$$

b.

The expressions

$$P_1 \equiv -5C_1 + 2C_2 \pmod{26}$$

$$P_2 \equiv 3C_1 - C_2 \pmod{26}$$

produce

"HE" "AR" "TH" "EB" "EL" "LS"

or Hear the bells

were put into a javascript function "hill()" see attached files

7. see q7.sage file