Cryptography I - Exercise 1 - 2b

Decrypt: "onhldqrttydxtlytojkhqtjxctdc"

Frequencies: t → 6, d → 3, o → 2

We want to find a and b, s.t. $a^{-1}(c_i - b) = m_i$

Alphabet:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

p	q	r	s	t	u	v	w	x	y	z
15	16	17	18	19	20	21	22	23	24	25

We try

m_i	c_i
e	t
t	o

$\Leftrightarrow$ $a^{-1}(19 - b) \equiv 4 \pmod{26}$ and $a^{-1}(14 - b) \equiv 19 \pmod{26}$ (1)

We solve (1):

$$5(a^{-1}) \equiv -15 \pmod{26}$$
$$a^{-1} \equiv 11\,(5^{-1}) \pmod{26}$$
$$a^{-1} \equiv 11 \cdot 21 \pmod{26}$$
$$a^{-1} \equiv 23 \pmod{26}$$

We plug a^{-1} in (1):

$$23(19 - b) \equiv 4 \pmod{26}$$
$$437 - 23b \equiv 4 \pmod{26}$$
$$23b \equiv 433 \pmod{26}$$
$$b \equiv 17 \cdot (23^{-1}) \pmod{26}$$
$$b \equiv 17 \cdot 17 \pmod{26}$$
$$b \equiv 3 \pmod{26}$$

So we have $m_i \equiv 23(c_i - 3) \pmod{26}$

For $o = 14$: $m_i \equiv 23(14 - 3) \equiv 23 \times 11 \equiv 253 \equiv 19 \pmod{26} \rightarrow t$

$n = 13$: $m_i \equiv 23(13 - 3) \equiv 23 \times 10 \equiv 230 \equiv 22 \pmod{26} \rightarrow w$

$h = 7$: $m_i \equiv 23(7 - 3) \equiv 23 \times 4 \equiv 92 \equiv 14 \pmod{26} \rightarrow o$

Solution: two can keep a secret if one is dead