

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

x	0	1	2	3	4	5	6
26x	0	26	52	78	104	130	156

Сообщение: c o n g r a t u l a t e

Key number X: 2 14 13 6 17 0 19 20 11 0 19 4

$ax = 5x$: 10 70 65 30 85 0 95 100 55 0 95 20

$ax + b = 5x + 10$: 20 80 75 40 95 10 105 110 65 10 105 30

$(ax+b) \bmod N =$
 $=(5x+10) \bmod 26$: 20 2 23 14 17 10 1 6 13 10 1 4

Number in key: u c x o r k b g n k b e

Ответ: ucxor kbgnk be



Абрамов
Александр

Berno: x

$\sqrt{2}$

Ciano: $(ax+b) \bmod N = y \Rightarrow y = ax + b \quad b \in \mathbb{Z}_N$

$a = 7 \quad b \in \mathbb{Z}_{26}$

$x = a^{-1}(y - b)$

log(26, 7):

$26 = 7 \cdot 3 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 3 \cdot (26 - 7 \cdot 3) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7$

$1 = 5 - 2 \cdot (7 - 5 \cdot 1) = 3 \cdot 5 - 2 \cdot 7$

$1 = 5 - 2 \cdot 2$

$0 \in \mathbb{Z}_{26}$

$\Rightarrow 1 = -11 \cdot 7$

$1 = 15 \cdot 7$

$7^{-1} = 15$

~~scribbles~~ $\Rightarrow x = 15(y - 9)$

cosignare: 2 d d e e j v
 King canbara y: 25 3 3 4 4 j v

y - 9: 16 -6 -6 -5 -5 0 21
 = -10

15(y - 9): -150 -90 -90 -75 -75 0 180

15(y - 9) mod 26: 6 14 14 3 3 0 24

Other:

goodday