Detyrë

Përdorni shifrën shtesë me çelësin k=4 për të koduar mesazhin “eljesa”

Emri: eljesa; key = 4

Vlera_enk = ((shkronja - a) + zhvendosja) mod26 + a

V_e=e

V_e ((101 - 97) + 4) mod26 +97

V_e= (4+4) mod26 +97

V_e= 8 mod26 +97

V_e = 8 + 97 = 105

105 = i

V_e = l

V_e = ((108 - 97) + 4) mod26 +97

V_e = (11 + 4) mod26 +97

V_e = 15 mod26 +97

V_e = 15+ 97 = 112

112 = p

V_e = j

V_e = (106-97) + 4) mod26 +97

V_e = (9+4) mod26 +97

V_e = 13 mod26 +97

V_e = 13+97 = 110

110 = n

V_e = e

V_e = ((101 - 97) + 4) mod26 +97

V_e = (4+4) mod26 +97

V_e = 8 mod26 +97

V_e = 8 + 97 = 105

105 = i

V_e=s

V_e = (11597) + 4) mod26 +97

V_e = (18+4) mod26 + 97

V_e = 22 mod26 + 97

V_e = 22 +97 = 119

119 = W

V_e = a

V_e = (97 − 97) + 4) mod26 +97

V_e = (0+4) mod26 +97

V_e = 4 mod26 +97

V_e = 4 + 97 = 101

101 = e

e=i, l=p, j=n, e=i, s=w, a=e

Dekriptimi: Vlera_enk= ((shkronja - a) - zhvendosja) mod26 + a

V_e = i

V_e = ((10597) — 4) mod26 +97

V_e = (8-4) mod26 +97

V_e = 4 mod26 +97

V_e = 4 + 97 = 101

101 = e

V_e =p

V_e = ((112 — 97) – 4) mod26 + 97

V_e = (15 — 4) mod26 +97

V_e = 11 mod26 +97

V_e = 11 + 97 = 108

108 = l

V_e = n

V_e = ((110 - 97) – 4) mod26 +97

V_e = (13-4) mod26 +97

V_e = 9 mod26 +97

V_e = 9+97= 106

106 = j

V_e =i

V_e = ((105-97) - 4) mod26 +97

V_e = (8-4) mod26 +97

V_e = 4 mod26 +97

V_e = 4 + 97 = 101

101 = e

V_e=w

V_e =((119-97) — 4) mod26 +97

V_e= (22-4) mod26 +97

V_e = 18 mod26 + 97

V_e = 18 + 97 = 115

115 = s

V_e = e

V_e = ((101 - 97) - 4) mod26 +97

V_e = (4-4) mod26 +97

V_e = 0 mod 26 +97

V_e = 0 +97= 97

97 = a

i=e, p=l, n =j, i = e, w=s, e=a

Enkriptimi dhe dekriptimi i emrit “Leonora” sipas kodit ASCI k=4, a=97

l) V_e = (108-97) + 4 mod26 + 97= (11+4) mod26 + 97 = 15 mod26 + 97 = 15+97 =112⇒p

e) V_e = (101-97) + 4 mod26 + 97 = (4+4) mod26 + 97 – 8 mod26 + 97= 8 + 97 = 105⇒i

o) V_e = (111-97) + 4 mod26 + 97 = (14+4) mod26 + 97 = 18 mod26 + 97 = 18+97 =115⇒s

n) V_e = (110-97) + 4 mod26 + 97 = (13+4) mod26 + 97 = 17 mod26 + 97 = 17+97 = 114 ⇒r

o) V_e = (111-97) + 4 mod26 + 97 = (14+4) mod26 + 97 = 18 mod26 + 97 = 18+97=115⇒s

r) V_e = (11497) + 4 mod26 + 97= (17+4) mod26 + 97 = 21 mod26 + 97 = 21+97 =118⇒v

a) V_e = (97-97) + 4 mod26 + 97 – 4 mod26 + 97 = 101⇒e

l➜p ; e➜i; o➜s; n➜r; o➜s; r➜v; a➜e

Formula enkriptimit: v_e=((shkronja-a) + zhvendosja) mod26 + a

pisrsve=Leonora

formula dekriptimit : v_d=((shkronja -a) - zhvendosja) mod26 + a

p) V_e = (112-97) – 4 mod26 + 97 = (15-4) mod26 + 97 = 11 mod26 + 97 = 11 + 97 = 108⇒l

i) V_e = (105-97) - 4 mod26 + 97 - (8-4) mod26 + 97 = 4 mod 26 + 97 = 4+97 = 101⇒e

s) V_e = (115-97) - 4 mod26 + 97 = (18-4) mod 26 + 97 – 14 mod 26 + 97 = 111⇒o

r) V_e = (114-97) - 4 mod26 + 97 = (17-4) mod 26 + 97 = 13 mod26 + 97 =110→n

s) V_e = (115-97) - 4 mod26 +97 = (18-4) mod26 + 97 = 14 mod26 + 97 =111⇒o

v) V_e = (118-97) - 4 mod26 + 97 = (21-4) mod26 + 97-17 mod26 + 97 =114⇒r

e) V_e = (101-97) - 4 mod26 + 97 – 0 mod26 + 97 = 97→a

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]