14 Criptați mesajul "incepe_primavara" utilizând o criptare afină pe blocuri de un caracter, cu cheia de criptă. (a=5, b=3), folosind A-Z_.

Tema 5
Volachi Emilie
M532

Criptare afină pe blocuri de un caracter:
Fie (a,b) cheia de criptare
$c = am + b \pmod N$

M	I	N	C	E	P	E	_	P	R	I	M	A	V	A	R	A
m	8	13	2	4	15	4	26	15	17	8	12	0	21	0	17	0
am(mod N)	13	11	10	20	21	20	25	21	4	13	6	0	24	0	4	0
c(mod N)	16	14	13	23	24	23	1	24	4	16	9	3	0	3	4	3
C	Q	O	N	X	Y	X	B	Y	H	Q	J	D	A	D	H	D

⊙ $am \pmod N$ $N = \underline{27}$ caractere (cu tot cu "_"!)

$5 \cdot 8 \pmod{27} = 40 \pmod{27} = 13$
$5 \cdot 13 \pmod{27} = 11$
$5 \cdot 2 \pmod{27} = 10$
$5 \cdot 4 \pmod{27} = 20$
$5 \cdot 15 \pmod{27} = 21$
$5 \cdot 4 \pmod{27} = 20$
$5 \cdot 26 \pmod{27} = 25$
$5 \cdot 17 \pmod{27} = 4$
$5 \cdot 12 \pmod{27} = 6$
$5 \cdot 21 \pmod{27} = 24$

① $e \pmod N \iff (am \pmod N + b) \pmod N$

$13 + 3 \pmod{24} = 16$
$11 + 3 \pmod{24} = 14$
$13 \pmod{24} = 13$
$20 + 3 \pmod{24} = 23$
$24 \pmod{24} = 24$
$25 + 3 \pmod{24} = 1$
$4 \pmod{24} = 4$

$16 \pmod{24} = 16$
$9 \pmod{24} = 9$
$24 \pmod{24} = 0$

Am obținut cifrarea QONXYXBYHOJDADHD.