1.3.2 Sistemul de criptare afin

$\mathcal{P} = \mathcal{C} = Z_{26}$, $\mathcal{K} = \{(a,b) \mid a, b \in Z_{26},\ cmmdc(a,26) = 1\}$,
iar funcţiile de criptare şi decriptare (pentru o cheie $K = (a,b)$) sunt

$$e_K(x) = ax + b\ (mod\ 26), \qquad d_K(y) = a^{-1}y + a^{-1}(26 - b)\ (mod\ 26)$$

Condiţia ca a să fie prim cu 26 asigură existenţa lui a^{-1} în Z_{26}.

Pentru $a = 3,\ b = 5$ funcţia de criptare este $e_K(x) = 3x + 5$, care poate fi reprezentată prin tabelul:

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
5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2

sau – scris direct pentru caractere

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
F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

PRIMAVARA TARZIE – YEDPFQFEF KDECDR.

Deoarece $3^{-1} = 9\ (mod\ 26)$, decriptarea se realizează matematic folosind funcţia $d_K(x) = 9x + 7$
(sau – practic – inversând cele două linii ale tabelului de mai sus).

Condiţia $cmmdc(a,26) = 1$ asigură injectivitatea aplicaţiei e_K.

De exemplu, pentru $e_K(x) = 10x + 1$, A şi N se transformă ambele în B, iar O nu apare ca imagine în alfabetul substituţiei.

Spaţiul cheilor $\mathcal{K}$: O cheie $K \in \mathcal{K}$ este determinată de valorile întregi (a,b) cu $(a,26) = 1$. Sunt posibile 12 valori pentru a:

$$1, 3, 5, 7, 9, 11, 15, 19, 21, 23, 25$$

Pentru b sunt posibile 26 valori, care se iau independent de a, cu singura excepţie $a = 1,\ b = 0$ (care se exclude deoarece nu conduce la nici o criptare).
Deci $card(\mathcal{K}) = 311$.