

So $y \equiv 23x + 8 \pmod{26}$.

Hence (see Note 16.4)

$$x \equiv 17[y - 8] \pmod{26} \equiv -9[y - 8] \pmod{26} \equiv -9y + 72 \pmod{26} \equiv -9y + 20 \pmod{26}.$$

So

	D	K	D	H	F	M	P	V	H	K	M	N	S	L	A	K	D	P	R	ciphertext
→	3	10	3	7	5	12	15	21	7	10	12	13	18	11	0	10	3	15	17	
→	19	8	19	9	1	16	15	13	9	8	16	7	14	25	20	8	19	15	23	
→	T	I	T	J	B	Q	P	N	J	I	Q	H	O	Z	U	I	T	P	X	plaintext

- (b) We seek $b, c \in \mathbb{N}$ with $1 \leq b, c \leq 25$ and $(b, 26) = 1$ such that

$$y \equiv bx + c \pmod{26}$$

For $I \mapsto D$, we have that $x = 8$ and $y = 3$; and for $T \mapsto K$, we have that $x = 19$ and $y = 10$. So

$$3 \equiv 8b + c \pmod{26}, \quad 10 \equiv 19b + c \pmod{26};$$

i.e.

$$\begin{pmatrix} 19 & 1 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} b \\ c \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 3 \end{pmatrix} \pmod{26}.$$

So again $\Delta = 19 \times 1 - 1 \times 8 = 11$, giving that $(\Delta, 26) = 1$ and $\Delta' = 19$.

Hence Theorem 16.5 gives that

$$\begin{aligned} \begin{pmatrix} b \\ c \end{pmatrix} &\equiv 19 \begin{pmatrix} 1 & -1 \\ -8 & 19 \end{pmatrix} \begin{pmatrix} 10 \\ 3 \end{pmatrix} \pmod{26} \equiv 19 \begin{pmatrix} 7 \\ -23 \end{pmatrix} \pmod{26} \\ &\equiv 19 \begin{pmatrix} 7 \\ 3 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 133 \\ 57 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 3 \\ 5 \end{pmatrix} \pmod{26}. \end{aligned}$$

So $y \equiv 3x + 5 \pmod{26}$.

Hence (see Note 16.4)

$$x \equiv 9[y - 5] \pmod{26} \equiv 9y - 45 \pmod{26} \equiv 9y + 7 \pmod{26}.$$

So

	D	K	D	H	F	M	P	V	H	K	M	N	S	L	A	K	D	P	R	ciphertext			
→	3	10	3	7	5	12	15	21	7	10	12	13	18	11	0	10	3	15	17				
→	8	19	8	18	0	11	12	14	18	19	11	20	13	2	7	19	8	12	4				
→	I	T	I	S	A	L	M	O	S	T	L	U	N	C	H	T	I	M	E				
→	I	T		I	S	A	L	M	O	S	T		L	U	N	C	H		T	I	M	E	plaintext