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

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad (ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$M_\varepsilon = \begin{bmatrix} 1 & 3 \\ 3 & -2 \end{bmatrix} \qquad M_D = \underbrace{((1\cdot -2)-(3\cdot 3))^{-1}}_{\text{modulair inverse!}}\begin{bmatrix} -2 & -3 \\ -3 & 1 \end{bmatrix}$$

$$= (-11)^{-1}\begin{bmatrix} -2 & -3 \\ -3 & 1 \end{bmatrix}$$

$$= 11^{-1}\begin{bmatrix} 2 & 3 \\ 3 & -1 \end{bmatrix}$$

eGCD, of de tafels van 11 en 26 opschrijven

$$= 19\begin{bmatrix} 2 & 3 \\ 3 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 12 & 5 \\ 5 & 7 \end{bmatrix}$$

$$c = \text{"OR"} = \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

tafels

x	26
1	26
2	52
3	78
4	104
5	130
6	156
7	182
8	208
9	

x	11
11	121
12	132
13	143
14	154
15	165
16	176
17	187
18	198
19	209

eGCD

$26 = 11\cdot 2 + 4$
$11 = 4\cdot 2 + 3$
$4 = 1\cdot 3 + 1$

	p	q
26	1	0
11	0	1
4	1	-2
3	-2	5
1	3	-7

$-7 = 19$

$$E(m) = M_\varepsilon \cdot m + \begin{bmatrix} -2 \\ 5 \end{bmatrix}, \text{ dus } D(c) = M_D\left(c - \begin{bmatrix} -2 \\ 5 \end{bmatrix}\right)$$

$$D\left(\begin{bmatrix} 14 \\ 17 \end{bmatrix}\right) = M_D\begin{bmatrix} 16 \\ 12 \end{bmatrix} = \begin{bmatrix} 12 & 5 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 12\cdot 16 + 5\cdot 12 \\ 5\cdot 16 + 7\cdot 12 \end{bmatrix} = \begin{bmatrix} 6\cdot 6 + 8 \\ 16 + 4\cdot -2 \end{bmatrix} = \begin{bmatrix} 44 \\ 8 \end{bmatrix} = \begin{bmatrix} 18 \\ 8 \end{bmatrix} = \text{"SI"}$$

$2\cdot 6\cdot 16 = 6\cdot 32 = 6\cdot 6$

$12\cdot 5 = 60 = 52 + 8 = 8$

$16 + 2\cdot 6 + 7\cdot 12$
$= 16 + 8\cdot 12$
$= 16 + 4\cdot 24$
$= 16 + 4\cdot -2$