TOEPASSING OP INVERSE MATRIX: CODEREN EN DECODEREN

Je hebt je misschien al de vraag gesteld: waarom heeft men nu de inverse van een matrix nodig?
Matrices en hun inversen vinden bv. hun toepassingen in het beveiligen van informatie. Wij gaan dat nu illustreren aan de hand van enkele kleine boodschappen.
Bij codering en decodering wordt vaak de volgende methode gebruikt:

- Aan iedere letter van het alfabet wordt op willekeurige wijze een getal gekoppeld. Bv.

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
14	12	22	26	34	31	24	35	15	32	17	28	19

n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*spatie*
13	27	16	21	29	20	30	23	36	11	33	25	18	5

- Er wordt een niet-singuliere (weet je nog wat dit betekent?) **coderingsmatrix** C vastgelegd. Bv.

$$\begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}$$

- De tekst wordt in groepen van vier letters verdeeld. De bij de letters behorende getallen worden in een bepaalde volgorde in een 2×2-matrix geplaatst. Bv. de groep 'in c' wordt voorgesteld door de matrix

$$\begin{bmatrix} 15 & 13 \\ 5 & 22 \end{bmatrix}$$

- De matrix wordt (bv.) rechts vermenigvuldigd met de coderingsmatrix C. Je kan narekenen dat

$$\begin{bmatrix} 15 & 13 \\ 5 & 22 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix} = \begin{bmatrix} 95 & 162 \\ 120 & 213 \end{bmatrix} (*)$$

  De groep 'in c' is nu in code: 95 162 120 213

- Als we beide leden van de vorige uitdrukking $(*)$ aan de rechterkant vermenigvuldigen met de inverse matrix van de coderingsmatrix krijgen we:

$$\begin{bmatrix} 15 & 13 \\ 5 & 22 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1} = \begin{bmatrix} 95 & 162 \\ 120 & 213 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1}$$

$$\Updownarrow$$

$$\begin{bmatrix} 15 & 13 \\ 5 & 22 \end{bmatrix} \cdot \left(\begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1} \right) = \begin{bmatrix} 95 & 162 \\ 120 & 213 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1}$$

$$\Updownarrow$$

$$\begin{bmatrix} 15 & 13 \\ 5 & 22 \end{bmatrix} \cdot \begin{bmatrix} \ldots & \ldots \\ \ldots & \ldots \end{bmatrix} = \begin{bmatrix} 95 & 162 \\ 120 & 213 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1}$$

$$\Updownarrow$$

$$\begin{bmatrix} \ldots & \ldots \\ \ldots & \ldots \end{bmatrix} = \begin{bmatrix} 95 & 162 \\ 120 & 213 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & 9 \end{bmatrix}^{-1}$$

  Dus men kan de oorspronkelijke boodschap terugvinden, door de doorgeseinde code rechts te vermenigvuldigen met de inverse matrix van de ..... Deze inverse matrix zullen we dan ook logischerwijze de **decoderingsmatrix** $D = C^{-1}$ noemen.

- Bereken nu zelf de decoderingsmatrix D en zet dan de volgende doorgeseinde boodschap terug om in mensentaal: 183 315 198 336 100 177 79 126

- Stel nu per twee een korte boodschap (tussen de 8 en 16 letters of spaties) op, zet die om m.b.v. een de coderingsmatrix $C = \begin{bmatrix} 8 & -5 \\ -3 & 2 \end{bmatrix}$. Wissel vervolgens deze boodschap (in code-taal) tesamen met de coderingsmatrix uit met twee collega's. Ontcijfer vervolgens mekaars boodschap. Verdeel het werk!!!

- Decodeer met behulp van het computerprogramma Derive de onderstaande geheime informatie. Hierbij is de gebruikte coderingsmatrix: $C = \begin{bmatrix} 12 & 2 \\ 1 & -6 \end{bmatrix}$.

  454 -134 365 30 166 -182 365 -44 421 -10 79 -104 438 -112 94 -194 421 -10 82 -122 343 -60 215 -106 394 -144 353 28 256 -56 182 -56 378 -122 96 -206 442 -136 341 26 375 -30 410 -92