

Thema 5 Benutzerelement M533 - M. 19

$$A = \begin{pmatrix} 3 & 7 & 1 \\ 4 & 11 & 9 \\ 1 & 2 & 3 \end{pmatrix}$$

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

a) Plaintext: STUDENT ii

b) Decrypted: D J S / E V C / Z T N / H L Y / i U M / X W A /

$$a) \begin{pmatrix} 3 & 7 & 1 \\ 4 & 11 & 9 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} S & D & T \\ T & E & i \\ U & N & i \end{pmatrix} = \begin{pmatrix} 3 & 7 & 1 \\ 4 & 11 & 9 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 18 & 3 & 19 \\ 19 & 4 & 8 \\ 20 & 13 & 8 \end{pmatrix} =$$

$$= \begin{pmatrix} 3 \cdot 18 + 7 \cdot 19 + 20 & 3 \cdot 3 + 7 \cdot 4 + 13 & 3 \cdot 19 + 7 \cdot 8 + 8 \\ 4 \cdot 18 + 11 \cdot 19 + 9 \cdot 20 & 4 \cdot 3 + 11 \cdot 4 + 9 \cdot 13 & 4 \cdot 19 + 11 \cdot 8 + 9 \cdot 8 \\ 1 \cdot 18 + 2 \cdot 19 + 3 \cdot 20 & 3 + 2 \cdot 4 + 3 \cdot 13 & 19 + 16 + 24 \end{pmatrix} =$$

$$= \begin{pmatrix} 207 & 50 & 121 \\ 461 & 173 & 236 \\ 116 & 50 & 59 \end{pmatrix} = \begin{pmatrix} 25 & 24 & 17 \\ 19 & 17 & 2 \\ 12 & 24 & 7 \end{pmatrix} = \begin{pmatrix} Z & Y & R \\ T & R & C \\ M & Y & H \end{pmatrix} =$$

$$= Z T M Y R Y R C H$$

b)  $A^{-1} =$

$$\det A = \begin{vmatrix} 3 & 7 & 1 \\ 4 & 11 & 9 \\ 1 & 2 & 3 \end{vmatrix} = 3 \cdot 11 \cdot 3 + 8 + 63 - 11 - 54 - 84 =$$

$$= 99 + 8 + 63 - 11 - 54 - 84 = 21$$

$$A^* = \begin{pmatrix} 3 & -7 & 1 \\ -4 & 11 & -9 \\ 1 & -2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 19 & 1 \\ 22 & 11 & 17 \\ 1 & 24 & 3 \end{pmatrix}$$

$$A^{-1} = \frac{1}{\det A} \cdot A^* = 5 \begin{pmatrix} 3 & 19 & 1 \\ 22 & 11 & 17 \\ 1 & 24 & 3 \end{pmatrix} = \begin{pmatrix} 15 & 17 & 5 \\ 6 & 3 & 7 \\ 5 & 16 & 15 \end{pmatrix}$$

$$\frac{1}{\det A} = \det A = 1^{(\text{mod } 26)} \frac{1}{\det A} = 5$$

DJSEVCZTNHLYIUMXWA

$$\begin{pmatrix} 15 & 17 & 5 \\ 6 & 3 & 7 \\ 5 & 16 & 15 \end{pmatrix} \begin{pmatrix} D & E & Z & H & I & X \\ J & V & T & L & U & M \\ S & C & N & Y & M & A \end{pmatrix} =$$

$$= \begin{pmatrix} 15 & 17 & 5 \\ 6 & 3 & 7 \\ 5 & 16 & 15 \end{pmatrix} \begin{pmatrix} 3 & 4 & 25 & 7 & 8 & 23 \\ 9 & 21 & 19 & 11 & 20 & 12 \\ 18 & 2 & 13 & 24 & 12 & 0 \end{pmatrix} =$$

$$\begin{matrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \end{matrix}$$

$$= \begin{pmatrix} 45 + 17 \cdot 9 + 90 & 15 \cdot 4 + 17 \cdot 21 + 5 \cdot 2 & 15 \cdot 25 + 17 \cdot 19 + 5 \cdot 13 \\ 6 \cdot 3 + 3 \cdot 9 + 7 \cdot 18 & 6 \cdot 4 + 3 \cdot 21 + 7 \cdot 2 & 6 \cdot 25 + 3 \cdot 19 + 7 \cdot 13 \\ 5 \cdot 3 + 16 \cdot 9 + 15 \cdot 18 & 5 \cdot 4 + 16 \cdot 21 + 15 \cdot 2 & 5 \cdot 25 + 16 \cdot 19 + 15 \cdot 13 \end{pmatrix}$$

$$\left. \begin{matrix} 15 \cdot 7 + 17 \cdot 11 + 5 \cdot 24 & 15 \cdot 8 + 17 \cdot 20 + 5 \cdot 12 & 15 \cdot 23 + 17 \cdot 12 + 0 \\ 6 \cdot 7 + 3 \cdot 11 + 7 \cdot 24 & 6 \cdot 8 + 3 \cdot 20 + 7 \cdot 12 & 6 \cdot 23 + 3 \cdot 12 + 0 \\ 5 \cdot 7 + 16 \cdot 11 + 15 \cdot 24 & 5 \cdot 8 + 16 \cdot 20 + 15 \cdot 12 & 5 \cdot 23 + 16 \cdot 12 + 0 \end{matrix} \right\} =$$

$$= \begin{pmatrix} 288 & 427 & 763 & 412 & 520 & 549 \\ 171 & 101 & 298 & 243 & 192 & 174 \\ 429 & 386 & 644 & 571 & 540 & 407 \end{pmatrix} =$$

$$= \begin{pmatrix} 2 & 11 & 9 & 22 & 0 & 3 \\ 15 & 23 & 12 & 9 & 10 & 18 \\ 13 & 22 & 20 & 25 & 20 & 21 \end{pmatrix} =$$

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

$$= \begin{pmatrix} C & L & J & W & A & D \\ P & X & M & J & K & S \\ N & W & V & Z & U & V \end{pmatrix} = \begin{matrix} C P N L X W J M U W J Z \\ - A K U D S V \end{matrix}$$