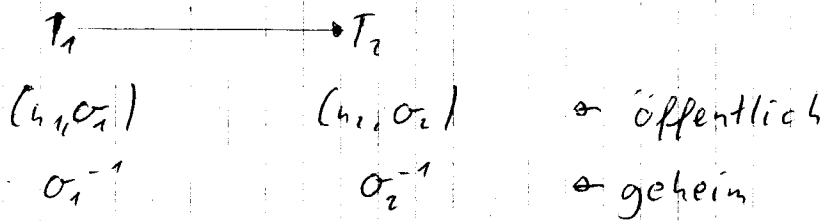


! A1-Vorlesung 21.11.2001



Falls nur T_2 lesen können soll: $\sigma_2(x)$ senden.

Falls nur T_1 lesen können soll: $\sigma_1(x)$ senden.

Falls nur T_1 die Nachricht geschickt haben soll: $\sigma_1^{-1}(x)$ senden
Kombination möglich.

RSA-Algorithmus: (Rivest, Shamir, Adleman 1978)

Wähle $n = p \cdot q$ (p, q große Primzahlen) $\Rightarrow \varphi(n) = (p-1)(q-1)$.

Wahl von e : Wähle $e \in \mathbb{N}$, teilerfremd zu $\varphi(n)$

$\Rightarrow \exists$ Darstellung $e \cdot \tilde{d} + \varphi(n) \cdot \tilde{h} = 1$, $\tilde{d}, \tilde{h} \in \mathbb{Z}$.

$\Rightarrow e \cdot \tilde{d} = 1 + \varphi(n) \cdot (-\tilde{h})$. Setze $d := \tilde{d} + \varphi(n) \cdot m$ $\left\{ \begin{array}{l} m \text{ so groß,} \\ \text{dass } d > 0 \end{array} \right.$

$\Rightarrow \boxed{e \cdot d = 1 + \varphi(n) \cdot r}$ mit $r \in \mathbb{N}$, $r = e \cdot m - \tilde{h}$

$\sigma: \{0, \dots, n-1\} \rightarrow \{0, \dots, n-1\}$, $\tau: \{0, \dots, n-1\} \rightarrow \{0, \dots, n-1\}$
 $\sigma(x) \equiv x^e \pmod{n}$ $\tau(x) \equiv x^d \pmod{n}$

Beh.: Es gilt $\sigma \circ \tau = \tau \circ \sigma = \text{id}$ (und damit sind σ und τ Permutationen).

Bew.: Es gilt $\sigma(\tau(x)) \stackrel{!}{=} \tau(\sigma(x)) \equiv x^{e \cdot d} \pmod{n} = x(x^{\varphi(n)})^r \pmod{n}$

1. Fall: $x = 0 \Rightarrow \sigma(\tau(0)) = 0$

2. Fall: $x \neq 0$, a) x, p teilerfremd

$$\stackrel{\text{Euler-F}}{\Rightarrow} x^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow x \cdot (x^{\varphi(n)})^r = x \cdot (x^{(p-1)r + (q-1)r}) \equiv x \pmod{p}$$

b) p teilt x , also $x = p \cdot m \equiv 0 \pmod{p}$

$$\Rightarrow x \equiv 0 \pmod{p}, x \cdot (x^{\varphi(n)})^r \equiv 0 \pmod{p}.$$

$$\Rightarrow x \cdot (x^{\varphi(n)})^r \equiv x \pmod{p}$$

$$\Rightarrow x \cdot (x^{\varphi(n)})^2 \equiv x \pmod{p} \quad \forall x \in \{0, \dots, n-1\}$$

$$\text{Analog: } x \cdot (x^{\varphi(n)})^2 \equiv x \pmod{q} \quad \forall x \in \{0, \dots, n-1\}$$

$$\text{Sei } y \equiv x \pmod{p}, y \equiv x \pmod{q} \Rightarrow y \cdot x = z \cdot p, y - x = \tilde{z} \cdot q$$

$$\Rightarrow p \mid y - x, q \mid y - x \Rightarrow p \cdot q \mid y - x \Rightarrow y \equiv x \pmod{p \cdot q}$$

$$\Rightarrow x(x^{\varphi(n)})^2 \equiv x \pmod{n}, \text{ d.h. } \sigma(\tau(x)) = x \quad \forall x \Rightarrow \text{Beh.}$$

Prinzip: n, e wird öffentlich gemacht

d wird nur dem Teilnehmer mitgeteilt (geheim)

Um d zu bestimmen (mit Euklid) muss man

$\varphi(n)$ kennen.

§4 Matrizen und Polynome

Sei K ein beliebiger Körper.

Definition:

Eine (m, n) -Matrix A (über K), $m, n \in \mathbb{N}$ ist ein rechteckiges Schema von Elementen aus K .

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Kurzschreibweisen:

$$A = ((a_{ij})) , ((a_{ij}))_{m \times n} , (a_{ij})$$

Speziell heißt $((a_{ij}))_{m \times 1}$ Spalte (Spaltenmatrix)

$((a_{ij}))_{1 \times n}$ Zeile (Zeilenmatrix)

Ist $m = n$, so heißt die Matrix A quadratisch.

Speziell heißt

$$E_n := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \begin{array}{l} \text{Einheitsmatrix.} \\ (\text{geht in } K^{\begin{smallmatrix} \circ & \circ \\ \circ & \circ \end{smallmatrix}}) \end{array}$$

Formale Definition: $E_n = ((\delta_{ij}))_{m \times n}$ mit $\delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

Die Menge aller (m, n) -Matrizen wird mit $\mathbb{K}^{m \times n}$ bezeichnet.

Verknüpfungen für Matrizen:

- Addition wie bei n -Tupeln komponentenweise:

$$A = ((a_{ij})) , B = ((b_{ij})) , A, B \in \mathbb{K}^{m \times n}$$

$$\Rightarrow C := A + B , c_{ij} = a_{ij} + b_{ij} \quad [i=1, \dots, m, j=1, \dots, n]$$

$\Rightarrow (\mathbb{K}^{m \times n}, +)$ ist abelsche Gruppe, Neutralelement ist die Nullmatrix $O = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{m \times n}$

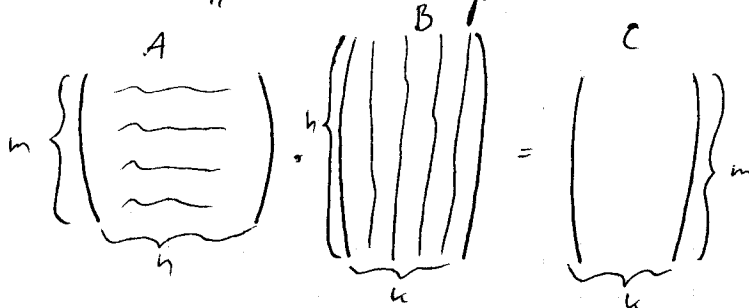
- Multiplikation?

Definition:

Seien $A \in \mathbb{K}^{m \times n}$, $B \in \mathbb{K}^{n \times k}$. Dann wird $C := A \cdot B \in \mathbb{K}^{m \times k}$

durch $c_{ij} := \sum_{r=1}^n a_{ir} b_{rj}$ $i=1, \dots, m, j=1, \dots, k$ definiert.

Merkschema: „Zeile mal Spalte“.



$$" \quad (m \times n) \cdot (n \times k) = m \times k "$$

Beispiel:

a) $\begin{pmatrix} 1 & 0 \\ 2 & 4 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 3 & 1 \end{pmatrix}$ existiert nicht.

$3 \times \textcircled{2} \cdot \textcircled{3} \times 2$

$\begin{pmatrix} 1 & 0 \\ 2 & 4 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 3 & 1 & 1 \end{pmatrix}$ existiert nicht. Aber umgekehrt...

$$b) \quad A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \end{pmatrix} \Rightarrow A \cdot B = \begin{pmatrix} 1 & 5 & 1 \\ 0 & 2 & 0 \\ 1 & 7 & 1 \end{pmatrix}$$

3×2 2×3 3×3

$$B \cdot A = \begin{pmatrix} 2 & 6 \\ 0 & 2 \end{pmatrix}$$

2×3

Satz 1:

Die folgenden Matrizenprodukte und -summen seien erklärt. Dann gelten die folgenden Rechenregeln:

$$(a) \quad (AB)C = A(BC) \quad [A \in K^{m \times n}, B \in K^{n \times k}, C \in K^{k \times g}]$$

$$(b) \quad (A+B)C = AC + BC$$

$$A(B+C) = AB + AC$$

$$(c) \quad E_n \cdot A = A = A \cdot E_n$$

$\begin{matrix} \uparrow \\ A \in K^{k \times k} \end{matrix}$ $\begin{matrix} \uparrow \\ A \in K^{k \times n} \end{matrix}$ \Rightarrow Diese A 's sind u. U. verschieden!