20. Vorlesung 25.11.2020

Notiztitel 25.11.2020

Prinzip der RSA-Verschlüsselung

Empfänger: $N = p \cdot q$ Produkt zweier sehr großer Primzahlen,

er rechnet in $\mathbb{Z}_{\tilde{N}}$ mit $\tilde{N} = (p-1)\cdot(q-1)$ folgendes aus:

er bestimmt e mit $1 < e < \tilde{N}$ und $ggT(e, \tilde{N}) = 1 \Rightarrow$

e hat in $\mathbb{Z}_{\tilde{N}}$ eine Inverse bezüglich der Multiplikation,

er berechnet diese Inverse, d.h. er löst $\overline{e}\cdot\overline{d} = \overline{1}$ in $\mathbb{Z}_{\tilde{N}}$

öffentlicher Schlüssel ist (N, e)

privater Schlüssel ist (N, d)

Sender: Er kennt den öffentlichen Schlüssel (N, e).

Er kodiert den zu verschlüsselnden Text in eine

Zahlenfolge $a_1 a_2 \dots a_k$ mit $ggT(a_i, N) = 1$, $1 \le i \le k$

Für jede Zahl a_i $(1 \le i \le k)$ berechnet er in $\mathbb{Z}_N$

die Zahl $\overline{A_i} = \overline{a_i^e}$;

die Zahlenfolge $A_1 A_2 \dots A_k$ ist dann die verschlüsselte Nachricht!

Empfänger: Er bekommt die Zahlenfolge $A_1 A_2 \dots A_k$ und berechnet mit

dem privaten Schlüssel (N, d) in $\mathbb{Z}_N$ die Zahlen $\overline{A_i^d}$;

es gilt $\overline{A_i^d} = a_i$, d.h. aus $A_1 A_2 \dots A_k$ wird wieder $a_1 a_2 \dots a_k$.

Warum funktioniert das?

Definition: Für $n \in \mathbb{N}$ wird definiert

a) $\Phi(n) = \{k \in \mathbb{N} \mid 1 \le k < n \wedge ggT(k, n) = 1\}$

Das ist die Menge der zu n teilerfremden nat. Zahlen kleiner als n.

b) Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ mit $\varphi(n) = |\Phi(n)| \mathrel{\hat{=}}$ Anzahl der Elemente

in der Menge $\Phi(n)$; diese Funktion heißt Eulersche-phi-Funktion.

Beispiele:

$n = 18 \Rightarrow \Phi(18) = \{1, 5, 7, 11, 13, 17\}$, $\varphi(18) = |\Phi(18)| = 6$

$n = 21 \Rightarrow \Phi(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, $\varphi(21) = 12$

$n = 7 \Rightarrow \Phi(7) = \{1, 2, 3, 4, 5, 6\}$, $\varphi(7) = 6 = 7-1$

$n = 3 \Rightarrow \Phi(3) = \{1, 2\}$, $\varphi(3) = 2 = 3-1$

$\Rightarrow 12 = \varphi(21) = \varphi(3 \cdot 7) = \underbrace{\varphi(3)}_{=2} \cdot \underbrace{\varphi(7)}_{=6}$

Bemerkung:

1) $p \in \mathbb{N}$ Primzahl $\Rightarrow \varphi(p) = p-1$ denn $\Phi(p) = \{1, 2, 3, \dots, p-1\}$

2) $p, q \in \mathbb{N}$ beide Primzahlen $\Rightarrow \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)\cdot(q-1)$

Satz von Euler:

Gegeben sind $a, N \in \mathbb{N}$ mit $ggT(a, N) = 1$, d.h. a und N sind teilerfremd.

Dann gilt

$a^{\varphi(N)} \equiv 1 \bmod N$ anders formuliert: $\overline{a^{\varphi(N)}} = \overline{1}$ in $\mathbb{Z}_N$

Folgerung daraus ist der „Kleine" Satz von Fermat, nämlich:

Für jede Primzahl $p \in \mathbb{N}$ gilt $a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^p \equiv a \bmod p$

(p Primzahl $\Rightarrow \varphi(p) = p-1$, dann ist nach dem Satz von Euler $a^{\varphi(p)} = a^{p-1} \equiv 1 \bmod p$)

Beweisidee zum RSA-Algorithmus

öffentlicher Schlüssel (N, e) mit $N = p \cdot q$ p und q Primzahlen

$\varphi(N) = \varphi(p \cdot q) = (p-1)\cdot(q-1) = \tilde{N}$ und $\underbrace{\overline{e} \cdot \overline{d} = \overline{1}}$ in $\mathbb{Z}_{\tilde{N}} = \mathbb{Z}_{\varphi(N)}$

privater Schlüssel (N, d) mit diesem d

Klartext als Zahl: a mit $ggT(a, N) = 1$, verschlüsselt wird a in

$\overline{a^e} \in \mathbb{Z}_N$ (Rest von a^e beim Teilen durch N): $\overline{A} = \overline{a^e}$, A wird gesendet

Zur Entschlüsselung wird berechnet:

$\overline{A^d} \in \mathbb{Z}_N$ berechnet; es ist

$$\overline{A^d} = \overline{(a^e)^d} = \overline{a^{ed}} \text{ in } \mathbb{Z}_N$$

Es gilt $\bar{e} \cdot \bar{d} = \bar{1}$ in $\mathbb{Z}_{\tilde{N}} = \mathbb{Z}_{\varphi(N)}$, d.h. $e \cdot d$ hat Rest 1 beim Teilen durch $\varphi(N)$; es gibt also ein $i \in \mathbb{N}$ mit $e \cdot d = i \cdot \varphi(N) + 1$

$\Rightarrow$ $\overline{a^{ed}}$ in $\mathbb{Z}_N$ ist $\overline{a^{i\cdot\varphi(N)+1}}$ in $\mathbb{Z}_N$ und damit: $\overline{a^{ed}} = \overline{a^{i\cdot\varphi(N)+1}}$

$$\Rightarrow \underbrace{\overline{a^{e\cdot d}}}_{\overline{A^d}} = \overline{a^{i\cdot\varphi(N)}} \cdot \bar{a} = \bar{a} \cdot \Big(\underbrace{\overline{a^{\varphi(N)}}}_{=\bar{1} \text{ nach Satz von Euler}}\Big)^i = \bar{a} \cdot \bar{1}^i = \bar{a} \cdot \bar{1} = \bar{a}$$

insgesamt gilt: $\overline{A^d} = \bar{a}$ in $\mathbb{Z}_N$.

<u>Beweisidee zum Satz von Euler</u> $\quad a, N \in \mathbb{N}$ mit $ggT(a,N) = 1$

Behauptung $\quad a^{\varphi(N)} \equiv 1 \bmod N \quad \left(\overline{a^{\varphi(N)}} = \bar{1} \text{ in } \mathbb{Z}_N \right)$

Setze $l = \varphi(N)$, dann ist $\Phi(N) = \{k_1, k_2, \dots, k_l\}$ mit $ggT(k_i, N) = 1$ für $1 \le i \le l$; d.h. $\bar{k}_1, \bar{k}_2, \dots, \bar{k}_l$ in $\mathbb{Z}_N$ haben inverse Elemente bezgl. der Multiplikation in $\mathbb{Z}_N$.

Für die Zahlen $a \cdot k_i$ $(1 \le i \le n)$ gilt auch $ggT(a \cdot k_i, N) = 1$, d.h. auch $\overline{a \cdot k_1}, \overline{a \cdot k_2}, \dots, \overline{a \cdot k_l}$ in $\mathbb{Z}_N$ haben inverse Elemente bezgl. der Multiplikation in $\mathbb{Z}_N$.

Für $\mathbb{Z}_N^* = \{\bar{k} \in \mathbb{Z}_N \mid \text{es gibt } \bar{l} \in \mathbb{Z}_N \text{ mit } \bar{k} \cdot \bar{l} = \bar{1}\}$

$$= \{\bar{k} \in \mathbb{Z}_N \mid ggT(k, N) = 1\} = \{\bar{k}_1, \bar{k}_2, \dots, \bar{k}_l\};$$

es ist aber auch $\overline{a \cdot k_1}, \overline{a \cdot k_2}, \dots, \overline{a \cdot k_l} \in \mathbb{Z}_N^* = \{\bar{k}_1, \bar{k}_2, \dots, \bar{k}_l\}$

$\overline{a \cdot k_1}, \overline{a \cdot k_2}, \dots, \overline{a \cdot k_l}$ ist nur eine andere Sortierung (eine Permutation) der Zahlen $\bar{k}_1, \bar{k}_2, \dots, \bar{k}_l$ und damit in $\mathbb{Z}_N$:

$$\overline{k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_e} = (\overline{a k_1}) \cdot (\overline{a k_2}) \cdot \ldots \cdot (\overline{a k_e}) \iff$$

ggT$(k_i, N) = 1$

$$\overline{\cancel{k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_e}} = \overline{a^l \cdot k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_e} = (\overline{a^l}) \cdot (\overline{\cancel{k_1 \cdot k_2 \cdot \ldots \cdot k_e}})$$

nach Kürzen hat man $\overline{1} = \overline{a^l}$ in $\mathbb{Z}_N$ also $\overline{1} = \overline{a^{\varphi(N)}}$ in $\mathbb{Z}_N$

Lineare Gleichungssysteme und Gauß-Algorithmus

Definition: (Wir betrachten nur die Fälle $n \leq k$)

Gegeben sind $n \cdot k$ reelle Zahlen a_{ij} $(1 \leq i \leq n, 1 \leq j \leq k)$ und n reelle Zahlen b_i $(1 \leq i \leq n)$.

(1) Gesucht sind die Werte der k Unbekannten x_j $(1 \leq j \leq k)$ mit

$$\left.\begin{array}{ccccccccc} a_{11} x_1 & + & a_{12} x_2 & + & \cdots & + & a_{1k} \cdot x_k & = & b_1 \\ a_{21} x_1 & + & a_{22} x_2 & + & \cdots & + & a_{2k} \cdot x_k & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1} x_1 & + & a_{n2} x_2 & + & \cdots & + & a_{nk} \cdot x_k & = & b_n \end{array}\right\} \text{ in Kurzform } \sum_{j=1}^{k} a_{ij} \cdot x_j = b_i, \ 1 \leq i \leq n$$

also Lösungen dieses linearen Gleichungssystems mit n Gleichungen für k Unbekannte.

(2) Die Zahlen a_{ij}, $1 \leq i \leq n$, $1 \leq j \leq k$ heißen Koeffizienten des linearen Gleichungssystems; die Zahlen b_i, $1 \leq i \leq n$ heißen rechte Seite des linearen Gleichungssystems und die gesuchten Zahlen x_j, $1 \leq j \leq k$ heißen Unbekannte des linearen Gleichungssystems.

Beispiele:

(1)
$$\left.\begin{array}{l} 3x_1 - 5x_2 + x_3 - x_4 = 1 \\ 2x_2 - x_3 = 0 \\ x_1 + x_2 + x_3 - 5x_4 = -2 \end{array}\right\}$$

$0 \cdot x_1$ $\quad$ $0 \cdot x_4$

lineares Gleichungssystem mit $n = 3$ Gleichungen und $k = 4$ Unbekannten x_1, x_2, x_3, x_4

rechte Seite: $b_1 = 1$, $b_2 = 0$, $b_3 = -2$

Koeffizienten $a_{11}=3,\ a_{12}=-5,\ a_{13}=1,\ a_{14}=-1$

$a_{21}=0,\ a_{22}=2,\ a_{23}=-1,\ a_{24}=0$

$a_{31}=1,\ a_{32}=1,\ a_{33}=1,\ a_{34}=-5$

② $$\left.\begin{aligned} 5x-2y &= 0 \\ -2x+3y &= 0 \end{aligned}\right\}$$ $n=2$ Gleichungen für $k=2$ Unbekannte nämlich x und y, formal

Unbekannte $x_1=x,\ x_2=y$

Koeffizienten: $a_{11}=5,\ a_{12}=-2,\ a_{21}=-2,\ a_{22}=3$

rechte Seite: $b_1=0,\ b_2=0$

Bemerkung: $n\leq k$ heißt: Wir betrachten nur lineare Gleichungssysteme mit weniger Gleichungen als Unbekannte ($n<k$) oder genau soviele Gleichungen wie Unbekannte ($n=k$).

Definition:

① Die $n\cdot k$ Koeffizienten $a_{ij},\ 1\leq i\leq n,\ 1\leq j\leq k$ eines lin. GLS bilden die Koeffizientenmatrix $\underline{\underline{A}}$ des lin. GLS; das ist ein rechteckiges Zahlenschema mit n Zeilen und k Spalten, nämlich

j heißt Spaltenindex ($1\leq j\leq k$)

$$\underline{\underline{A}}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nk}\end{pmatrix}=(a_{ij})_{\substack{1\leq i\leq n\\ 1\leq j\leq k}}$$

i heißt Zeilenindex ($1\leq i\leq n$)

② Die k Unbekannten $x_1, x_2, \ldots, x_k$ bilden den Vektor der Unbekannten, nämlich

$$\vec{x}=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k\end{pmatrix}$$

(Ein solcher Vektor $\vec{x}$ kann auch als Matrix mit k Zeilen und 1 Spalte interpretiert werden)

③ Die n Zahlen $b_1, b_2, \dots, b_n$ bilden den <u>Vektor der rechten Seite</u>, nämlich

$$\vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

(Ein solcher Vektor $\vec{b}$ kann auch als Matrix mit n Zeilen und 1 Spalte interpretiert werden)

<u>Beispiel:</u>

$$\left.\begin{array}{r} 3x_1 - 5x_2 + x_3 - x_4 = 1 \\ 2x_2 - x_3 \qquad = 0 \\ x_1 + x_2 + x_3 - 5x_4 = -2 \end{array}\right\} \Rightarrow$$

$$\underline{\underline{A}} = \begin{pmatrix} 3 & -5 & 1 & -1 \\ 0 & 2 & -1 & 0 \\ 1 & 1 & 1 & -5 \end{pmatrix}, \quad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \quad \vec{b} = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$$