Chinesischer Restesatz

-1

W.H.

$a, b \in \mathbb{Z}$, $n, m \in \mathbb{N}$, $ggT(n,m) = 1$ (teilerfremd)

Löse:
$$x \equiv a \mod n$$
$$x \equiv b \mod m$$

A) Hat eindeutige Lösung $x \in \{0, 1, 2, \dots, n \cdot m - 1\}$ (weitere $\pm\, m \cdot n$)

$$f(\overline{x}_{nm}) = (\overline{x}_n, \overline{x}_m) = (\overline{a}_n, \overline{b}_m)$$

B) Berechnen über Euklid. Alg. $1 = m \cdot \underline{w} + n \cdot \underline{v}$ $\Rightarrow$ Lsg: $x = a \cdot m \cdot w + b \cdot n \cdot v$

Ausrechnen

BSP
$$x \equiv 3 \mod 20$$
$$x \equiv 5 \mod 153$$

$a = 3$, $b = 5$, $n = 20$, $m = 153$

$n \cdot m = 3060$

$1 = 153(-3) + 20 \cdot 23$

$w = -3$, $v = 23$

$x = 3 \cdot 153(-3) + 5 \cdot 20 \cdot 23$
$= 923$

Probe:
$923 = 46 \cdot 20 + 3$
$923 = 6 \cdot 153 + 5$

0

RSA – Verfahren

Beruht auf zahlentheoretische Zusammenhänge

Asymmetrisch: public-key, private-key

A) Einheiten in $(\mathbb{Z}_n, \oplus_n, \odot_n)$ (Restklassen-) Ring mit $\underline{1}$.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\} \qquad ggT(j,n)=1 \iff \overline{j} \text{ invertierbar } (\overline{j} \in \mathbb{Z}_n^*)$$

B) Euler'sche φ-Funktion zählt die Einheiten!

$$\varphi(n) = |\mathbb{Z}_n^*|$$

BSP $\mathbb{Z}_{21}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\}$

$\varphi(n) = 12 = 2 \cdot 6 = \underline{(p-1)(q-1)} \longleftarrow n = 21 = 3 \cdot 7 = \underline{p \cdot q}$ $\underline{\text{kein Zufall!}}$

Wir brauchen Primzahlen: (1)

p, q Prime.

$n = p \cdot q$ $\qquad \varphi(n) \overset{!}{=} (p-1)(q-1) = \varphi(p) \cdot \varphi(q)$

unbekannt!

Welche Zahl $\leq p \cdot q$ ist nicht teilerfremd?

Skizze:

Vielfache von ~~q~~ q: $\quad 1 \cdot q, 2 \cdot q, 3 \cdot q, \ldots, p \cdot q$ $\qquad p$ nicht teilerfremd

gleich

Vielfachen von ~~q~~ p: $\quad 1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p \cdot q$ $\qquad q$

Andere gibt es nicht!

$p + q - 1$ viele

$$\underbrace{p \cdot q}_{\text{Kandidaten für } \varphi(n)} - (p + q - 1) = (p-1)(q-1) = p \cdot q - p - q + 1$$ ✓

<u>Theorem 4.36</u> $\forall\, \underline{n} \in \mathbb{N}, \forall\, a \in \mathbb{Z}$

a, n teilerfremd $\Rightarrow a^{\varphi(n)} \equiv 1 \mod n$

Bsp $\varphi(21) = 12$

$2^{12} \equiv 1 \mod 21$

$2^5 = 32 \equiv 11 \mod 21$

$11 \cdot (11 \cdot 4) \equiv 2 \cdot 11 \mod 21$

$\equiv 1 \mod 21$

(a ist Einheit von $\mathbb{Z}_n$, dann gilt $a^{\varphi(n)} \equiv 1 \mod n$)

<u>Theorem 4.36'</u> Sei $G = \{a_1 = e, a_2, a_3, \ldots, a_m\}$ abelsche Gruppe bzgl. "$\cdot$"

$\Rightarrow \forall g \in G \quad g^m = e.$

Allgemeiner!

$(\mathbb{Z}_n^*, \odot_n)$ Spezialfall Th. 4.36

③

<u>Beweis:</u> Sei $\underline{\underline{g}} \in G$ <u>Betrachte:</u> $\varphi_g : G \to G$

$a \longmapsto a \cdot g$ $(\underline{g} \cdot a)$ geht auch!

<u>Zeige:</u> φ_g ist bijektive <u>Abb.</u>!

<u>φ_g injektiv</u> $a \cdot g = a' \cdot g \overset{\uparrow}{\underset{\text{abelsche Gruppe}}{\Rightarrow}} a \cdot g \cdot g^{-1} = a' \cdot g \cdot g^{-1} \Rightarrow a = a'$

<u>φ_g ist auch surjektiv</u> <u>wg. Kardinalität und Injektivität!</u> $|G|$ viele Elemente auf beiden <u>Seiten</u>

$\Rightarrow \varphi_g$ "permutiert" die Elemente von G

$$\Rightarrow \underline{\left(\prod_{i=1}^{m} a_i\right)} \overset{\downarrow}{\underset{\uparrow\ \underline{\underline{\text{abelsch}}}}{=}} \left(\prod_{i=1}^{m} \varphi_g(a_i)\right) = \prod_{i=1}^{m} (a_i \cdot g) \overset{\underline{\underline{\text{abelsch}}}}{\underset{\downarrow}{=}} \underline{\left(\prod_{i=1}^{m} a_i\right)} g^m$$

von links mit $\left(\prod_{i=1}^{m} a_i\right)^{-1}$ multiplizieren $\Rightarrow e = g^m$ $\square$

RSA Verfahren

Schlüsselerzeugungen

1. **Wähle** zwei "große" Primzahlen p und q $(p \neq q)$

   Setze $n = p \cdot q$ $\varphi(n) = (p-1)(q-1)$

2. **Wähle** $e \in \mathbb{N}$ mit $ggT(e, \varphi(n)) = 1$ Public key (n, e)

3. **Berechne** $d \in \mathbb{N}$ mit Euklid-Alg Private-key (n, d)

   $e \cdot d \equiv 1 \mod \varphi(n)$

Verschlüsseln / Entschlüsseln!

5

Verschlüsseln: Nachricht: $\{0, 1, 2, 3, \dots, n-1\}$

Universum!

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ \sqcup & A & B & C & \end{array}$$

$$E: \{0, 1, 2, \dots, n-1\} \to \{0, 1, 2, \dots, n-1\}$$

$$E(x) = x^e \bmod n \qquad (e, n)$$

$E(x) = y$

$D(y) = x$

Entschlüsseln:

$$D: \{0, 1, \dots, n-1\} \to \{0, 1, 2, \dots, n-1\}$$

$$D(y) = y^d \bmod n \qquad (d, n)$$

BSP **Text:** Folge von Buchstaben $\sqcup = 0 \quad A = 1 \quad B = 2 \quad \dots$

1. Schritt $p = 3, \; q = 11 \quad n = 33 \quad \varphi(n) = 20$

Nachrichtenbereich $\{0, 1, 2, \dots, n-1\}$

2 Schritt $e = 7$ $ggT(7,20) = 1$

public key $(33, 7)$

3. Schritt d Euklid. Alg. $\varphi(n)$ und e

$(-1) \cdot 20 + \underbrace{3}_{d} \cdot 7 = 1$ private-key $(33, 3)$

BSP R S A $R = 18$ $S = 19$ $A = 01$

Verschlüsseln:

$18^7 \bmod 33 = 6$

$19^7 \bmod 33 = 13$

$1^7 \bmod 33 = 1$

Geheimtext: "06 13 01"

Entschlüsselt:

$06^3 \bmod 33 = 18$

$13^3 \bmod 33 = 19$

$01^3 \bmod 33 = 1$

Praktische Anwendung Blöcke übermitteln!

ASCII 256 Zeichen!

Wörter endlicher Länge ~~Länge~~ k! 256^k verschiedene Wörter.

$256^k < n$, n so wählen

$k = 2$ He|iß|er|␣T|ipp: Klausur␣ist␣bald

ASCII $H = 72$ $e = 101$ $i = 105$ $ß = 223$

I. He $72 \cdot 256^0 + 101 \cdot 256^1 = 25928$

II. iß $105 \cdot 256^0 + 223 \cdot 256^1 = 57193$

III. er

IV. ␣T

Diese Zahlen codieren!

(8)'

RSA Verfahren (Korrektheit, Laufzeiten, Sicherheit)

Überblick nochmal

1. 2 große Primzahlen p, q $\quad p \neq q \quad n = p \cdot q$
   wählen/bestimmen $\qquad$ modulo n rechnen
   $\varphi(n) = (p-1)(q-1)$

2. Wähle/bestimme $e \in \mathbb{N}$ mit $ggT(e, \varphi(n)) = 1$ $\qquad (n, e)$ public-key

3. Berechne $d \in \mathbb{N}$ mit $e \cdot d \equiv 1 \mod \varphi(n)$ $\qquad (n, d)$ private-key
   (mult. Inverses in $\mathbb{Z}_{\varphi(n)}$!)

Verschlüsseln: $N' = \{0, 1, 2, \ldots, n-1\}$ Nachrichtenmenge

$E: N' \rightarrow N' \quad E(x) = x^e \mod n$

Entschlüsseln: $D: N' \rightarrow N' \quad D(y) = y^d \mod n$

$$D(E(m)) = m \left(= E(D(m))\right) \quad \forall m \in N'$$

Korrektheit!

Korrektheit: **Theorem 4.35**

Für jedes $n \in \{0, 1, 2, \dots, n-1\}$

gilt: $D(E(m)) = m$.

Beweis: $\overline{(m^e)^d} = \overline{m^{e \cdot d}} \overset{!}{=} \overline{m} \pmod{n}$

$n = p \cdot q$ z.z.: $\underline{n = p \cdot q \mid m^{e \cdot d} - m}$

1. Fall weder p noch q teilt m: $p \nmid m$, $q \nmid m$

2. Fall p (exkl.) oder q teilt m: O.E. $p \mid m$, $q \nmid m$

3. Fall p und q teilen m: $p \mid m$, $q \mid m$

⑨

Γ $\underline{e \cdot d} \equiv 1 \mod \varphi(n)$ $\qquad \varphi(n) = \varphi(p) \cdot \varphi(q)$

$\Rightarrow \quad e \cdot d = 1 + k \cdot \varphi(n) \qquad \underline{\underline{k \in \mathbb{N}}}$ $\lrcorner$

$\underline{1.\ \text{Fall}}$ $\quad \overline{m^{e \cdot d}} = \overline{m \cdot (m^{\varphi(n)})^k} = \overline{m} \odot_n \overline{m^{\varphi(n)}}^{\,k} \underset{\substack{\uparrow \\ p \cdot q \nmid m}}{=} \overline{m} \odot \overline{1}^{\,k} = \overline{m}$ ✓

$\text{Th. } 4.36 \quad ggT(m, \underset{p \cdot q}{\underset{\shortparallel}{n}}) = 1$

$\underline{2.\ \text{Fall}}$ $\quad \underset{n}{\underset{\shortparallel}{p \cdot q}} \mid m^{e \cdot d} - m \qquad p \mid m^{e \cdot d} - m \qquad \underline{\text{zeige}}: \underline{\underline{q \mid m^{e \cdot d} - m}}$

$\underline{(\text{modulo } q)}$ $\quad \overline{m^{e \cdot d}} = \overline{m} \odot_q \overline{m^{\varphi(n)}}^{\,k} = \overline{m} \odot_q \overline{(m^{\varphi(p)})^{\varphi(q)}}^{\,k}$

$\varphi(n) = \varphi(p) \cdot \varphi(q)$

$\underset{\substack{\uparrow \\ \text{Th. } 4.36}}{=} \overline{m} \odot_q \overline{1}^{\,k} = \overline{m} \qquad \Rightarrow \quad p \cdot q \mid m^{e \cdot d} - m$ ✓

(10)

3. Fall $\quad \underbrace{p\cdot q}_{= n} \mid m \quad \overline{m} = \overline{0} = \overline{m^{e\cdot d}} \pmod{n}$ bleibt

also $\quad D(E(m)) = m \quad \overline{m^{e\cdot d}} = \overline{m} \quad n \mid m^{e\cdot d} - m \quad \square$

⌜ $E(D(m)) = m$ ⌟

Implementation / Berechnung / Laufzeiten / Sicherheit?

---

1. p, q finden

- rate ungerade Zahl x
- teste auf Primzahl
- ja: fertig
- nein: $x := x + 2$ usw. usf.

→ Primzahltest

⌜ Primzahldichte ist hoch

\# Primzahlen $< n$

$\sim \frac{n}{\ln n}$

ca. $\ln n$ viele Tests ⌟

11

Laufzeit: $C \log_2(n)^{7.6}$ $k < 8$ polynomieller Alg.
zu hohe Laufzeit

2012 AKS-Test Agrawal, Kayal, Saxena

Praktisch: Miller-Rabin-Test Schnell, randomisiert

Monte-Carlo-Algorithmen $\rightsquigarrow$ mehrfache Ausführung!

---

2. $ggT(e, \varphi(n)) = 1$ finde $e \in \mathbb{N}$

- rate e $\varphi(n) < n$
- teste mit Euklid. Alg

Th. 4.29 $\sim \log_2(n)$ Iterationen

Dichte $< n$

$\sim \frac{n}{\log(\log n)}$

ca. $\log(\log n)$ viele Schritte!

3. Berechne d mit $e \cdot d \equiv 1 \mod \varphi(n)$

$ggT(e, \varphi(n)) = 1 \underset{\text{Euklid. Alg}}{\Longrightarrow} x \cdot e + y \cdot \varphi(n) = 1$

x mult. Inverse.

Verschlüsseln / Entschlüsseln

$x^e \bmod n \rightsquigarrow$ Laufzeit $C \cdot \log(e) \cdot \log(n)$

Sicherheit public key (n, e)

Unbekannt: $n = p \cdot q$

Primfaktorzerlegung: "Schweres" Problem $NP \neq P$