mada Zusammenfassung

Privater Schlüssel: (n, d)

Öffentlicher Schlüssel: (n, e)

$n = p * q \qquad Primzahlen \quad p \neq q, \quad p > 2, \quad q > 2$

$e, d \in \mathbb{Z}^*_{\varphi(n)} \quad mit \;\; e * d \equiv 1(\text{mod}\varphi(n)) \quad \Leftrightarrow \quad e * d \equiv_{\varphi(n)} 1 \quad \Leftrightarrow \quad (e * d) \bmod \varphi(n) = 1$

Zahlentheorie

1) $\forall a \in \mathbb{Z} : 1 \mid a$

2) $\forall a, b \in \mathbb{Z} : a \mid b \Rightarrow (-a) \mid b$

3) $\forall a \in \mathbb{Z} : a \mid 0$

4) $\forall a, b, c \in \mathbb{Z} : (a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$

5) $\forall a, b, c \in \mathbb{Z} : (a \mid b) \wedge (a \mid c) \Rightarrow a \mid (b + c)$

6) $\forall a, b, c, d \in \mathbb{Z} : (a \mid b) \wedge (c \mid d) \Rightarrow (a * b) \mid (b * d)$

Primzahl

Zahl $n \in \mathbb{N}$ heisst Primzahl, wenn sie genau zwei verschiedene Teiler in $\mathbb{N}$ hat.

Die ersten Primzahlen: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101

Primzahlensatz: $\pi(n)$ bezeichnet Anz. Primzahlen $\leq n$. Dann gilt für $n \geq 55$:

$\frac{n}{\ln n+2} < \pi(n) < \frac{n}{\ln n-4}$

grösster gemeinsamer Teiler (ggT)

$ggT(a, b) := \max\{x \in \mathbb{Z} \mid (x \mid a) \wedge (x \mid b)\}$

Für $a, b \in \mathbb{N}$ gilt $a \mid b \Leftrightarrow ggT(a, b) = a$

Falls $ggT(a, b) = 1$ dann heissen *a* und *b* teilerfremd

Für alle $a \in \mathbb{N}$ gilt $ggt(a, 0) = a$

Der ggT kann mit *Primfaktorzerlegung* oder dem *(erweiterten) euklidischen Algorithmus* ermittelt werden.

Primfaktorzerlegung (mit Bsp.)

Der ggT ist das Produkt aller Primfaktoren, die in beiden Zahlen vorkommen, potenziert mit der niedrigeren der beiden Potenzen.

$ggT(2079, 5733) = ? \quad \rightarrow \quad 2079 = 3^3 * 7 * 11 \quad \& \quad 5733 = 3^2 * 7^2 * 13$

3^2 und 7 kommen in beiden Zahlen vor. $\quad \Rightarrow \quad ggT(2079, 5733) = 3^2 * 7 = 63.$

Eulersche φ-Funktion

Es sei $n \geq 2$. Dann ist: $\quad \mathbb{Z}^*_n = \{a \in \{0, 1, \ldots, n-1\} \mid ggT(a, n) = 1\}$

Def.: $\quad \varphi(n) = |\mathbb{Z}^*_n| \qquad$ → Gibt an wie viele zu *n* teilerfremde nat. Zahlen kleiner als *n* existieren.

Bsp.: $\quad \varphi(12) = |\{a \in \{0, 1, \ldots, 11\} \mid ggt(a, 12) = 1\}| \quad = \quad |\{1, 5, 7, 11\}| \quad = \quad 4$

Es sei *p* eine Primzahl, dann gilt: $\quad \varphi(p) = p - 1$

Es sei $n \geq 2$ mit der Primfaktorzerlegung $n = p_1^{e_1} * \cdots * p_k^{e_k}$

Dann gilt: $\quad \varphi(n) = (p_1 - 1) * p_1^{e_1 - 1} * \cdots * (p_k - 1) * p_k^{e_k - 1}$

Bsp.: $\quad \varphi(12) = \varphi(2^2 * 3^1) = (2 - 1) * 2^{2-1} * (3 - 1) * 3^{1-1} = 4$

Modulo

Es seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$.

Es existiert genau ein $q \in \mathbb{Z}$ und ein $r \in \{0, 1, \dots, n-1\}$ mit $a = n * q + r$.

a div n $:= q$ und $a \bmod n$ $:= r$

Bem.: a = (a div n)*n + (a mod n)

Bsp.: 10 div 4 = 2 10 mod 4 = 2
-1 div 4 = 3 -1 mod 4 = 3 (da: -1 = -1 *4 +3)

Rechenregeln Modulo:

Es seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$.

1) $a \bmod n = b \bmod n \quad \Leftrightarrow \quad n \mid (a - b)$

2) $a \bmod n = (a \bmod n) \bmod n$

3) $(a + b) \bmod n = ((a \bmod n) + b) \bmod n$
$(a + b) \bmod n = (a + (b \bmod n)) \bmod n$
$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

4) $(a * b) \bmod n = ((a \bmod n) * b) \bmod n$
$(a * b) \bmod n = (a * (b \bmod n)) \bmod n$
$(a * b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$

.

Definition: Es seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$

Wir schreiben $a \equiv b \pmod{n}$ oder $a \equiv_n b$ falls a mod n = b mod n und sagen: “a ist kongurent zu b modulo n”.

Es sei $n \in \mathbb{Z}$ dann ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$. Das heisst:

1) $\equiv_n$ ist refelxiv, d.h. $\forall a \in \mathbb{Z} : a \equiv_n a$

2) $\equiv_n$ ist symmetrisch, d.h. $\forall a, b \in \mathbb{Z} : a \equiv_n b \Rightarrow b \equiv_n a$

3) $\equiv_n$ ist transitiv, d.h. $\forall a, b, c \in \mathbb{Z} : (a \equiv_n b) \wedge (b \equiv_n c) \Rightarrow (a \equiv_n c)$

Äquivalenzklasse $[a]_n$ enthält alle Elemente, die zu *a* kongrugent modulo *n* sind.

Bsp.: $[7]_3 = \{a \in \mathbb{Z} \mid a \equiv_3 7\} = \{7, 10, 13, \dots\} \cup \{4, 1, -2, -5, \dots\}$

Rechenregeln $\equiv_n$: (Es sei $n \in \mathbb{N}$ und $a, b, c, d \in \mathbb{Z}$)

1) $a \equiv_n b \Leftrightarrow n \mid (a - b)$

2) Aus $a \equiv_n b$ und $c \equiv_n d$ folgt $a + c \equiv_n b + d$ und $a * c \equiv_n b * d$

3) Aus $a * c \equiv_n b * c$ folgt $a \equiv_m b$ mit $m = \frac{n}{ggT(c,n)}$ aber nicht: $a \equiv_n b$

Erweiterter Euklidischer Algorithmus

Einfach:

$18 = 7 \cdot 2 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = \underline{1} \cdot 3 + 0$

$ggT(18, 7) = 1$

Detailliert: Euklid(a,b)

Vorbedingung: $a, b \in \mathbb{Z}, a \geq b \geq 0$

1. Initialisierte Schleife : $a' = a \quad b' = b \quad x_0 = 1 \quad y_0 = 0 \quad x_1 = 0 \quad y_1 = 1$
2. Jeweils : $q = a' \text{ div } b' \quad r = a' \text{ mod } b'$
3. Schleife solange $b' \neq 0$: $a' = b' \quad b' = r \quad x_0 = x_1 \quad y_0 = y_1 \quad x_1 = x_0 - q * x_1 \quad y_1 = y_0 - q * y_1$

	a'	b'	x_0	y_0	x_1	y_1	q	r
INIT:	**a**	**b**	**1**	**0**	**0**	**1**	a' div b'	a' mod b'
Z2:	b'	r	x_1	y_1	$x_0 - q * x_1$	$y_0 - q * y_1$	a' div b'	a' mod b'

Invariante : $ggT(a,b) = ggT(a', b') \quad | \quad a' = x_0 * a + y_0 * b, \quad b' = x_1 * a + y_1 * b \quad | \quad a' \geq b' \geq 0$

Nachbedingung : $\boldsymbol{ggT(a,b) = a' = x_0 * a + y_0 * b}$

falls *d* aus $d * e \equiv_m 1$ bestimmt werdern soll : $d = y_0 \text{ mod } m; \quad a' = m; \quad b' = e; \quad \boldsymbol{ggT = 1}$

> Es sei $m \in \mathbb{N}$ mit $m \geq 2$ und $e \in \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
>
> Dann existiert $d \in \mathbb{Z}_m$ mit $e * d \equiv_m 1$ genau dann, wenn $ggT(m,e) = 1$ also $e \in \mathbb{Z}_m^*$
>
> Dann ist auch $d \in \mathbb{Z}_m^*$
>
> mit Euklid : $1 = ggT(m,e) = x_0 * m + y_0 * e \quad \Rightarrow \quad y_0 * e \equiv_m 1 \quad \Leftrightarrow \quad 1 = (y_0 * e) \text{ mod } m$

Modulare Exponentation

Effizient $\boldsymbol{x^e}$ **mod** $\boldsymbol{m}$ berechnen bei $e, m \in \mathbb{N}, x \in \mathbb{Z}$

Ansatz: *(a*b) mod n = (a mod n * b)* und "zwischendurch" schon *mod m* rechnen. aber besser:

Schnelle Exponation

Idee: Nutze $x^{2^k} = (((x^2)^2)^{2\cdots})^2$

Zerlege den Exponenten in eine Summe von Zweierpotenzen! Bsp : $13 = 2^3 + 2^2 + 2^0 \quad \Rightarrow x^{13} = x^{2^3} * x^{2^2} * x^{2^0}$

Beachte: $13 = (1101)_2 \quad (\rightarrow$ Binärdarstellung)

Wir gehen von hinten nach vorne über die Binärdarstellung, quadrieren jedesmal und multiplizieren, falls das Bit 1 ist.

Algorithmus: Eingabe: x^e mod m $\quad | \quad x \in \mathbb{Z}, \ m \in \mathbb{N}, \ e \in \mathbb{N}$ mit Binärdarstellung $e = (b(0)b(1)\ldots b(l))_2$

1. Initialisierung : $i = l; \ h = 1; \ k = x$
2. iteriertes Quadrieren: solange $i \geq 0$

   falls $b(i) = 1 \quad \rightarrow \quad h = h * k \text{ mod } m$

   $k = k^2 \text{ mod } m$

   $i = i - 1$
3. Ergebnis: *h*

Beispiel: Gesucht: $7^{13} \bmod 11$

$(13)_2 = 1101$

i	h	k
3	1	7
2	7	$49 \bmod 11 = 5$
1	7	3
0	10	9
-1	$\boxed{2}$	

Gruppentheorie

Verknüpfung

Die Verknüpfung ∘ auf (oder in) einer Menge *M* ist eine Vorschrift, die je zwei Elementen *a* und *b* aus *M* (unter Beobachtung der Reihenfolge ein weiteres Element *c* von *M* zuordnet, also eine Abbildung: $M \times M \to M$.

Die Tatsache, dass $a \circ b$ für $a, b \in M$ wieder ein Element von *M* ist, bezeichnet man als Abgeschlossenheit von M bzgl. ∘.

Anstelle von ∘ wird auch $\oplus, \odot, *, +, \cdot, \ldots$ verwendet.

Nachfolgend stets: **Annahme:** $M \neq \mathbf{0}$

Def.: Es sei M eine Menge und f eine Famili von Verknüpfungen auf M. Dann heisst (M, f) algebraische Struktur.

Halbgruppen – Def.: Es sei M eine Menge und ∘ eine Verknüpfung auf M. $(M, \circ)$ heisst Halbgruppe, falls ∘ assiozativ ist,

> d.h. wenn $\forall a, b, c \in M$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

Monoide – Def.: Eine Halbgruppe $(M, \circ)$ heisst Monoid, falls ein Element $e \in M$ existiert mit $e \circ a = a \circ e = a \mid \forall a \in M$.

> e heisst dann neutrales Element und ist eindeutig bestimmt.

Gruppen – Def.: Ein Monoid $(M, \circ)$ heisst Gruppe, falls für alls $a \in M$ ein Element $i \in M$ existiert mit $i \circ a = a \circ i = e$, wobei e das eindeutige neutrale Element ist.

> i heisst dann Inverses von a. Wir schreiben dafür a^{-1} (lediglich Abkürzung!)

Menge M mit einer Verknüpfung ∘ ist also genau dann eine Gruppe, wenn:

1. M ist abgeschlossen bzgl ∘, d.h. $a \circ b \in M \quad \mid \forall a, b \in M$
2. ∘ ist assoziativ, d.h. $(a \circ b) \circ c = a \circ (b \circ c) \quad \mid \forall a, b, c \in M$
3. Es existiert ein neutrales Element $e \in M$, d.h. $a \circ e = e \circ a = a \quad \mid \forall a \in M$
4. Für alle $a \in M$ existiert ein inverses Element $a^{-1} \in M, \quad \text{d.h. } a^{-1} \circ a = a \circ a^{-1} = e$

Kurz

$\text{public key: } (n, e) \quad \text{private key: } (n, d) \quad e * d \equiv 1 \bmod \varphi(n)$

1. $\varphi(n)$ bestimmen
2. *d* mittels erw. eukl.Algo. mit $\varphi(n) = a', \quad e = b'$

3. $d = y_0 \bmod \varphi(n)$
4. entschlüsseln von y mit $y^d \bmod n$ mit schneller Exponation.

ver-, entschlüsseln: $x = y^d \bmod n$; $\quad y = x^e \bmod n$; $\quad (x^e \bmod n)^d \bmod n = x \rightarrow$ schnelle Exponation

Beweise

Zahlentheorie

(1) $\forall a, b \in \mathbb{Z} : a \mid b \Rightarrow (-a) \mid b$

$$a \mid b \rightarrow \exists k \in \mathbb{Z} : b = k * a$$
$$\Rightarrow b = \underbrace{(-k)}_{\in\mathbb{Z}} * (-a)$$
$$\Rightarrow (-a) \mid b$$

(4) $\forall a, b, c \in \mathbb{Z} : (a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$

$$a \mid b \rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 * a$$
$$b \mid c \rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 * b$$
$$\Rightarrow c = \underbrace{(k_1 * k_2)}_{\in\mathbb{Z}} * a$$
$$\Rightarrow a \mid c$$

(5) $\forall a, b, c \in \mathbb{Z} : (a \mid b) \wedge (a \mid c) \Rightarrow a \mid (b + c)$

$$a \mid b \rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 * a$$
$$a \mid c \rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 * a$$
$$\Rightarrow b + c = \underbrace{(k_1 + k_2)}_{\in\mathbb{Z}} * a$$
$$\Rightarrow a \mid (b + c)$$

(6) $\forall a, b, c, d \in \mathbb{Z} : (a \mid b) \wedge (c \mid d) \Rightarrow (a * c) \mid (b * d)$

$$a \mid b \rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 * a$$
$$c \mid d \rightarrow \exists k_2 \in \mathbb{Z} : d = k_2 * c$$
$$\Rightarrow b * d = (k_1 * a * k_2 * c) = \underbrace{(k_1 * k_2)}_{\in\mathbb{Z}} * (a * c)$$
$$\Rightarrow (a * c) \mid (b * d)$$

Rechenregel Modulo

(1) $a \bmod n = b \bmod n \quad \Leftrightarrow \quad n \mid (a - b)$

Zuerst zeigen: $a \bmod n = b \bmod n \Rightarrow n \mid (a - b)$

$$\rightarrowtail a = (a \operatorname{div} n) * n + (a \bmod n)$$
$$\rightarrowtail b = (b \operatorname{div} n) * n + (b \bmod n)$$
$$\Rightarrow a - b = (a \operatorname{div} n - b \operatorname{div} n) * n + \underbrace{a \bmod n - b \bmod n}_{\text{0, nach Voraussetzung}}$$
$$\Rightarrow a - b = \underbrace{(a \operatorname{div} n - b \operatorname{div} n)}_{\in\mathbb{Z}} * n$$
$$\Rightarrow n \mid (a - b)$$

dann: $n \mid (a - b) \Rightarrow a \bmod n = b \bmod n$

$$\rightarrowtail \exists k \in \mathbb{Z} : a - b = k * n$$
$$\Rightarrow a = b + k * n = (b \operatorname{div} n) * n + b \bmod n + k * n$$
$$\Rightarrow a = (b \operatorname{div} n + k) * n + b \bmod n$$
$$\Rightarrow nachDef. : a = (a \operatorname{div} n + a \bmod n)$$

müssen übereinstimmen, da es genau 1 Darstellung von a als Vielfachen von n plus Rest gibt.

(2) $a \bmod n = (a \bmod n) \bmod n$

Gemäss (1) reicht zu zeigen, dass:

$n \mid \underbrace{(a - (a \bmod n))}_{(a \operatorname{div} n) * n}$

Offensichtlich Vielfachen von n