Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Formelsammlung Security

Sommersemester 2022
(LV 4120, 7240)

1. Nomenklatur

N	Menge der nichtnegativen ganzen Zahlen $\mathbf{N} := \{0, 1, 2, 3, \cdots\}$
N+1	Menge der natürlichen (positiven ganzen) Zahlen $\mathbf{N+1} := \{1, 2, 3, \cdots\} = \mathbf{N} \setminus \{0\}$
Z	Menge der ganzen Zahlen $\mathbf{Z} := \{0, \pm 1, \pm 2, \pm 3, \cdots\}$
P	Menge der Primzahlen $\mathbf{P} := \{2, 3, 5, 7, 11, 13, \cdots\}$
Q	Menge der rationalen Zahlen (abbrechende oder periodisch nicht abbrechende Dezimalbrüche) $\mathbf{Q} := \{a / b \mid a, b \in \mathbf{Z}, b \neq 0, \text{ggT}(a, b) = 1 \text{ (teilerfremd)}\}$
I	Menge der irrationalen Zahlen (nicht-periodisch nicht abbrechende Dezimalbrüche) $\mathbf{I} := \{\sqrt[n]{p} \mid p \in \mathbf{P};\ n = 2, 3, 4, \cdots ; \sin(\pi/4) ; e ; \pi ; \cdots\}$
R	Menge der reellen Zahlen $\mathbf{R} := \mathbf{Q} \cup \mathbf{I}$
C	Menge der komplexen Zahlen $\mathbf{C} := \{a + j\,b \mid a, b \in \mathbf{R};\ j^2 = -1\}$
$\mathbf{Z_m}$	Restklassenring modulo m $\mathbf{Z_m} := \{0, 1, 2, 3, \cdots, m-1\}$
[k:m]	$:= \begin{cases} 0, & \text{falls } k > m \\ \{z \mid z \in \mathbf{Z}, k \leq z \leq m\}, & \text{sonst} \end{cases} \qquad k, m \in \mathbf{Z}$
n | k	n teilt k $\Rightarrow (\exists\, x \in \mathbf{Z})\ k = x \cdot n$
n ∤ k	n teilt k nicht $\Rightarrow (\forall\, x \in \mathbf{Z})\ k \neq x \cdot n$
ggT(n, k)	der größte gemeinsame Teiler von n und k
kgV(n, k)	das kleinste gemeinsame Vielfache von n und k

n mod d	Divisionsrest, wenn man n durch d teilt
ϕ(m)	EULERsche ϕ-Funktion (gibt die Anzahl derjeniger natürlicher Zahlen $n < m$ an, die teilerfremd zu m sind; $m, n \in \mathbf{N}$) a und b teilerfremd heißt: **ggT**(a, b) = 1
$\exists$	Existenzquantor
$\forall$	Allquantor

2. Algebren

<table>
<tr><th colspan="5">Struktur</th><th>Bez.</th><th>Formel (Axiom)</th><th>A</th></tr>
<tr><th colspan="2">Algebra (A, +, •)</th><th colspan="3">Algebra (A, +)</th><th colspan="2"></th><th>N+1 Z Q</th></tr>
<tr><td rowspan="12">Körper</td><td rowspan="9">Ring</td><td rowspan="4">abelsche Gruppe</td><td></td><td>HG</td><td>assoz.</td><td>$a + (b + c) = (a + b) + c$</td><td>x x x</td></tr>
<tr><td colspan="2" rowspan="2">additive Gruppe</td><td>$\exists$ 0</td><td>$0 + a = a$</td><td>- x x</td></tr>
<tr><td>$\exists$ - a</td><td>$a + (- a) = 0$</td><td>- x x</td></tr>
<tr><td colspan="2"></td><td>komm.</td><td>$a + b = b + a$</td><td>x x x</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="3"></td><td>distri.</td><td>$a (b + c) = a b + a c$</td><td>x x x</td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="3">Algebra (A_0, •)</th><td colspan="3"></td></tr>
<tr><td rowspan="4">abelsche Gruppe</td><td></td><td>HG</td><td>assoz.</td><td>$a (b c) = (a b) c$</td><td>x x x</td></tr>
<tr><td>Einselem.</td><td colspan="2" rowspan="2">multipl. Gruppe</td><td>$\exists$ 1</td><td>$1 a = a$</td><td>x x x</td></tr>
<tr><td rowspan="2"></td><td>$\exists a^{-1}$</td><td>$a a^{-1} = 1$</td><td>- - x</td></tr>
<tr><td colspan="2"></td><td>komm.</td><td>$a b = b a$</td><td>x x x</td></tr>
</table>

3. Division mit Rest

$n, d \in \mathbf{N}$ und $d > 0$.

$$n = q \cdot d + r \quad \text{mit} \quad 0 \leq r < d$$
$$(- a) \bmod n = (\alpha \cdot n - a) \bmod n \; (\alpha \in \mathbf{Z})$$
$$(a \circ b) \bmod n = ((a \bmod n) \circ (b \bmod n)) \bmod n$$

4. Kongruenzen

$$r_a = R_n(a) = a \bmod n \text{ und } r_b = R_n(b) = b \bmod n.$$
$$a \equiv b \pmod{n} \quad \text{gdw} \quad r_a = r_b$$
$$a \equiv b \pmod{m} \;\Leftrightarrow\; b \equiv a \pmod{m} \;\Leftrightarrow\; a - b \equiv 0 \pmod{m}$$
$$a \equiv b \pmod{m} \;\Rightarrow\; ggT(a, m) = ggT(b, m)$$

5. Teilbarkeit

$n, d \in \mathbf{N}$ und $d > 0$.

$$d \mid n \quad \text{gdw} \quad (\exists\, q \in \mathbf{Z})\; n = q \cdot d$$
$$0 \mid a \;\Leftrightarrow\; a = 0$$
$$a \mid b \text{ und } b \mid a \;\Rightarrow\; a = \pm b$$
$$(t \mid a \wedge t \mid b) \;\Rightarrow\; (\forall\, x, y \in \mathbf{Z}) \quad t \mid (a \cdot x + b \cdot y)$$
$$a \mid c \text{ und } b \mid c \;\Rightarrow\; a \cdot b \mid c \cdot ggT(a, b)$$
$$b \mid a \text{ und } c \mid b \Rightarrow c \mid a$$
$$c \mid a \text{ und } c \mid b \Rightarrow c \mid (a \pm b)$$
$$a \mid b \;\Leftrightarrow\; ggT(a, b) = \mid a \mid$$
$$a \mid b \cdot c \;\text{ und }\; ggT(a, b) = 1 \;\Rightarrow\; a \mid c$$
$$n \mid (a - b) \;\Leftrightarrow\; a \equiv b \pmod{n}$$

6. **Euklidische Divisions-Theorem**
   $n, d \in \mathbf{N}$ und $d > 0$. $i \in \mathbf{Z}$.

$$R_d(n + i \cdot d) = R_d(n)$$

7. **Größter gemeinsamer Teiler**

$$ggT(n_1, n_2) = ggT(n_1 + i \cdot n_2, n_2) = ggT(n_2, R_{n2}(n_1))$$
$$1 \le ggT(n_1, n_2) \le \min\{ | n_1 | , | n_2 | \}$$
$$ggT(n_1, 0) = | n_1 |$$
$$ggT(a \cdot c, b \cdot c) = | c | \cdot ggT(a, b)$$

8. **Kleinste gemeinsame Vielfache**

$$kgV(a, b) \cdot ggT(a, b) = a \cdot b$$

9. **Restsystem**
   $x \equiv y \pmod m$ und $y \in \mathbf{Z}$. $j \in [1:m]$.

$$y \equiv x_j \pmod m$$
$$\mathbf{Z_m} := \{0, 1, 2, \ldots, m - 1\}$$

10. **Sätze von Fermat und Euler**
    $p \in \mathbf{P}$ und $a \in \mathbf{Z}$ ($a \ne 0$). $ggT(a, p) = 1$.

$$a^{p-1} \equiv 1 \pmod p$$

   $b \in \mathbf{Z}$.

$$b^p \equiv b \pmod p$$

   $a \in \mathbf{Z} \setminus \{0\}$ und $m \in \mathbf{N + 1}$. $ggT(a, m) = 1$.

$$a^{\phi(m)} \equiv 1 \pmod m$$

11. **Quadratische Reste**
    $p \in \mathbf{P}$; $a \in \mathbf{Z}$ mit $ggT(a, p) = 1$ und $a^{(p-1)/2} \equiv 1 \pmod p$.

$x^2 \equiv a \pmod p$ hat 2 Lösungen x_1 <u>und</u> x_2.

   $p, q \in \mathbf{P}$; $m = p \cdot q$, $a \in \mathbf{Z}$ mit $ggT(a, m) = 1$ und $a^{(p-1)/2} \equiv 1 \pmod p$, $a^{(q-1)/2} \equiv 1 \pmod q$.

$x^2 \equiv a \pmod m$ hat 2 oder 4 Lösungen.

12. **Wurzelgleichung**
    $x^2 \equiv a \pmod p$ lösbar, gdw $a^{(p-1)/2} = 1$ bzw. $p \equiv 3 \pmod 4$
    Lösung: $x_1 = a^{(p+1)/4} \bmod p$ und $x_2 = p - x_1$

13. **Diskreter Logarithmus**
    $x, y, g \in \mathbf{Z}$ und $p \in \mathbf{P}$.

$$y = g^x \bmod p$$

14. **Lineare diophantische Gleichung**
    $a, b, d \in \mathbf{Z}$ und $d = ggT(a, b) > 0$.

$$(\exists\, x, y \in \mathbf{Z}) \quad d = a \cdot x + b \cdot y$$
$$| x | \le b / (2 \cdot d) \text{ und } | y | \le a / (2 \cdot d)$$

15. **Modulare Inversion**
    $ggT(a, n) = 1$ und $a \cdot x + n \cdot y = 1$.

$$x = a^{-1} \bmod n \,.$$

   $p \in \mathbf{P}$ und $a \ne 0$.

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

16. Eulersche Phi-Funktion

$n \in \mathbf{N}$ und $p, q \in \mathbf{P}$.

$$\phi(n) = \left|\ 0 \le k < n \mid ggT(k, n) = 1\ \right|$$

$n = p_1^{a1} \cdot p_2^{a2} \cdot \ldots \cdot p_k^{ak}$ mit $p_i \in \mathbf{P}$ und $a_i \in \mathbf{N}$.

$$\phi(n) = n \cdot \prod (1 - 1 / p_i)\ \ ; (i = [1:k])$$

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)\ ; (ggT(m, n) = 1)$$

$$\phi(p) = p - 1$$

$$\phi(p^k) = p^{k-1} \cdot (p - 1)\ )\ ; (k \in \mathbf{N+1})$$

$$\phi(p \cdot q) = (p - 1) \cdot (q - 1)\ ; (p \ne q)$$

17. Entwicklungssatz für modulare Exponentiation

$ggT(a, n) = 1$.

$$a^{b} \bmod n = a^{b \bmod \phi(n)} \bmod n$$

18. Chinesischer Restsatz

$m_i \in \mathbf{N+1}$ und $a_i \in \mathbf{Z}$ sowie $x \equiv a_i \bmod m_i$ $(1 \le i \le n)$.

$m = \prod m_i$ und $M_i = m / m_i$ mit $ggT(m_i, M_i) = 1$.

$$x = (\sum a_i \cdot y_i \cdot M_i) \bmod m \quad \text{und} \quad y_i \cdot M_i \equiv 1 \bmod m_i$$

$n = p \cdot q$ und $p, q \in \mathbf{P}$. $a \bmod q(p) = 0(1)$ und $b \bmod q(p) = 1(0)$ sowie $X \in \mathbf{Z_n}$.

$sig_1 = (X \bmod p)$ und $sig_2 = (X \bmod q)$.

$$sig(m) := X \bmod n = a \cdot sig_1 + b \cdot sig_2$$

$$X \bmod p = (X \bmod n) \bmod p$$

$n = p \cdot q$ und $p, q \in \mathbf{P}$. $x \equiv a \pmod p$ und $x \equiv a \pmod q$.

$$x \equiv a \pmod n$$

19. Linearer Kongruenz- und Pseudozufallszahlengenerator

$$x_{n+1} = (a \cdot x_n + b) \bmod n$$

$$x_{n+1} = a \cdot x_n - \mathrm{int}\,(a \cdot x_n / b) \cdot b$$

$$x_{-1} = s;\ x_{n+1} = (x_n)^2 \bmod n;\ b_i = x_i \bmod 2$$

Schieberegister

LFSR Zustandsfolge $x, x \cdot T, x \cdot T^2, x \cdot T^3, \ldots$

$$T = \begin{pmatrix} z_4 & & & \\ z_3 & & E & \\ z_2 & & & \\ z_1 & 0 & 0 & 0 \end{pmatrix}$$

Max. Periodenlänge $d = 2^n - 1$.

20. Fundamentalsatz der Arithmetik

$a \in \mathbf{N}$ mit $a \ge 2$. $p_1, \ldots, p_k \in \mathbf{P}$ und $a_1, \ldots, a_k \in \mathbf{N}$.

$$a = p_1^{a1} \cdot p_2^{a2} \cdot \ldots \cdot p_k^{ak}$$

21. Primzahlen

$n \in \mathbf{Z}$ und $n > 1$.

$$n \mid a \cdot b \ \Rightarrow\ n \mid a \ \text{oder}\ n \mid b \quad \text{gdw} \quad n \in \mathbf{P}$$

$n \in \mathbf{N}$ sowie $(n - 1) / 2 \in \mathbf{N}$.

$$a_i^{(n-1)/2} = \pm 1 \text{ für } \forall\, a_i \in \mathbf{Z_n} \setminus \{0\} \quad \text{gdw} \quad n \in \mathbf{P}.$$

$$\pi(n) \approx n / (\ln(n) - 1.08366)$$

Sichere Primzahlen $p - 1 = 2\,q$ mit $p, q \in \mathbf{P}$

$n = p \cdot q$ und $\phi = \phi(n)$.

$$p, q = \alpha \pm \sqrt{(\alpha^2 - n)}, \quad \text{wobei } \alpha = (n + 1 - \phi) / 2$$

22. Primzahlentest von Miller und Rabin

n ungerade sowie auch $(n - 1) / 2$ ungerade; $a_i \in \{2, \ldots, n - 2\}$

Falls alle $a_i^{(n-1)/2} \bmod n = \pm 1$ bzw. 1 oder $n - 1$ für $\forall\, a_i$,

entscheide n ist prim, sonst n ist nicht prim.

Fehlerwahrscheinlichkeit $< (1/4)^k$

MRT deterministisch $\Rightarrow$ aus $(\mathbf{Z} / n\mathbf{Z})^*$: $\forall\, a \in \{2, \ldots, \min(n - 1, 2 \cdot \ln^2(n))\}$

n	gleich / ungefähr	Als Zeuge zu testen sind die Zahlen
$< 2^{16}$	65.536	2 und 3
$< 2^{32}$	4.294.967.296	2, 7 und 61
$< 2^{64}$	$\approx 1.844\ 10^{19}$	2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 und 37
< 3.317.044.064.679.887.385.961.981		2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 und 41

23. Verschiebechiffre (Vigenère-Chiffre)

k, z und $z' \in Z_n$.

$$\textbf{E:}\ z \rightarrow (z + k) \bmod n$$

$$\textbf{D:}\ z' \rightarrow (z' - k) \bmod n$$

24. Affine Tauschchiffre

$t \in Z_n \setminus \{0\}$ und $k, n \in Z_n$ mit $ggT(t, n) = 1$.

$$\textbf{E:}\ z \rightarrow (z \cdot t + k) \bmod n$$

$$\textbf{D:}\ z' \rightarrow (b \cdot z' + l) \bmod n$$

$$b \equiv t^{-1} \bmod n \quad \text{und} \quad l = b\,(n - k) \bmod n$$

25. One Time Pad

$\mathbf{A} = \{0, 1\}$ ein Alphabet und $z, r \in \mathbf{A}$.

$$z \rightarrow (z + r) \bmod 2 = z \text{ XOR } r = z \oplus r$$

$$P(M \mid C) = P(M) \quad \Leftrightarrow \quad \text{perfektes Chiffriersystem}$$

26. Diffie-Hellman

$p \in \mathbf{P}$ und $g \in \mathbf{N}$ mit $2 \leq g \leq p - 2$.

$a \in \{0, 1, p - 2\}$ und $b \in \{0, 1, p - 2\}$.

$\alpha = g^a \bmod p$ und $\beta = g^b \bmod p$.

$$K_A = \beta^a \bmod p \text{ und } K_B = \alpha^b \bmod p \text{ mit } K_A = K_B := K$$

27. ElGamal

Schlüsselpaar (PK, SK): Zufallszahl $b \in \{1, ..., p - 1\}$ mit $ggT(b, p) = 1$.

Mit dem Erzeuger g folgt $PK_B := g^b \in \mathbf{G}(\mathbf{Z}p^*)$ und $SK_B := b$.

Verschlüsselung: Zufallszahl $r \in \{1, ..., p - 1\}$ mit $ggT(r, p) = 1$.

Chiffrat $C = (C_1, C_2)$ mit $C_1 = g^r \in \mathbf{G}(\mathbf{Z}p^*)$ und $C_2 = PK_B{}^r \cdot m \in \mathbf{G}(\mathbf{Z}p^*)$

Entschlüsselung: Klartext $m = C_1{}^{p-1-SK} \cdot C_2 \in \mathbf{G}(\mathbf{Z}p^*)$

Signatur: Mit $r = g^k \bmod p$ und $ggT(k, p - 1) = 1$ ist $sig(h(m)) := (r, s)$, wobei

$h(m) = (SK_A \cdot r + k \cdot s) \bmod (p - 1)$ und $s = k^{-1} \cdot (h(m) - SK_A \cdot r) \bmod (p - 1)$

Verifikation: $Verify(h(m), (r, s), PK_A) = true \Leftrightarrow g^{h(m)} \bmod p \ ?{=}?\ PK_A{}^r \cdot r^s \bmod p$

28. RSA

Schlüsselpaar (Pk, Sk): $n = p \cdot q$ und $p, q \in \mathbf{P}$ und $p \neq q$.

$Sk \cdot Pk \bmod \phi(n) = 1$ sowie $ggT(Sk, \phi(n)) = 1$ mit $\phi(n) = (p - 1) \cdot (q - 1)$.

Chiffrat $c = m^{Pk} \bmod n$

Entschlüsselung: Klartext $m = c^{Sk} \bmod n$

Signatur: $sig(m) := h(m)^{Sk} \bmod n$

Verifikation: Verify(h(m), sig(m), Pk) = true $\Leftrightarrow$ $h(m)$?=? $sig(m)^{Pk} \bmod n$

29. Rabin-Verfahren

Schlüsselpaar: geheim (p, q) mit $p \equiv q \equiv 3 \bmod 4$ sowie öffentlich (n) mit $n = p \cdot q$ wobei $p, q \in \mathbf{P}$ und $p \neq q$.

Chiffrat $G = T^2 \bmod n$

Entschlüsselung: Klartext $T \in \{\pm r \bmod n, \pm s \bmod n\}$ mit

$r = (y_p \cdot p \cdot T_q + y_q \cdot q \cdot T_p) \bmod n$, $\quad s = (y_p \cdot p \cdot T_q - y_q \cdot q \cdot T_p) \bmod n$

$T_p = G^{(p+1)/4} \bmod p$, $T_q = G^{(q+1)/4} \bmod q$ sowie

$y_p \cdot p + y_q \cdot q = 1$

30. Hill-Chiffre

Chiffrat $\mathbf{c} = (\mathbf{K} \cdot \mathbf{p}) \bmod m$ mit $ggT(\det \mathbf{K}, m) = 1$, wobei $\mathbf{K}$ = nxn-Schlüsselmatrix.

Klartext $\mathbf{p} = (\mathbf{K}^{-1} \cdot \mathbf{c}) \bmod m$

31. Fiat-Shamir

$n = p \cdot q$ mit $p, q \in \mathbf{P}$ (zufällig)

$Sk = s$ (zufällig) und $Pk := v = s^2 \bmod n$

$x = r^2 \bmod n$ (r zufällig) und $b = \{0, 1\}$ (zufällig)

Vorbereitung:		Prüfung:	
if (b==1) then	$y = r \cdot s \bmod n$	if (b==1) then	y^2 ?=? $x \cdot v \bmod n$
else	$y = r \bmod n$	else	y^2 ?=? $x \bmod n$

32. Hashfunktionen

$y = f(x) = x^k \bmod n$

$h_i = (h_{i-1} + m_i)^2 \bmod n$ für $1 \leq i \leq r$; $h_0 = 0$ und Hashwert $H(m) = h_r$