Mitschrift der Kryptographievorlesung im Sommersemester 2002 gehalten von N.-P. Skoruppa und G. Illies

Monika Dücker, Caroline Fasel, Lars Fischer, René Six

3. Dezember 2003

Inhaltsverzeichnis

Kapitel 1

Motivation, Problemkreis

Problem Authentifizierung: Kennwort (Password) eingeben
(z.B. einloggen) Pin-Code eingeben
notwendig: Datenbank der Gestalt User: Kennwort
Schutz der Datenbank:

a) geheimhalten - unzureichend

b) Chiffrierung der Kennworte

($\rightsquigarrow$ User: ?!??!?!)
zu b) gesucht: $h : X \to Y$
(z.B. X= Menge der 8-buchstabigen Worte,
Y=alle natürlichen Zahlen $\leq$ gegebener Schranke)

Forderung

i) $\forall\, x :\ h(x)$ „leicht berechenbar“.

ii) zu $y \in Y$ ist es praktisch unmöglich x mit $y = h(x)$ zu bestimmen.

(h mit i) und ii) heißen Einwegfunktionen)
Zu ii) „praktisch unmöglich“

Möglichkeiten:

I) Geheimhaltung von Algorithmus $(x \to h(x))$

II) jeder darf Algorithmus kennen, aber „$y = h(x)$ in x“ zu lösen ist „algorithmisch zu komplex“,als dass man es durchführen kann.

Einwegfunktionen: i) II)

Beispiel (Einwegfunktionen)
p Primzahl (z.b. 150 Stellen)
a Primitivwurzel mod p,
$h : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$, $x \to a^x \; mod \; p$ (h bijektiv)
zu i) Potenzieren: effektiv möglich
zu II) h^{-1} „diskrete Logarithmus“ scheint sehr komplex

Bemerkung 1.1 *Die Berechnung des diskreten Logarithmus entspricht dem Lösen von Gleichungen in einer endlichen abelschen Gruppe (hier $(\mathbb{Z}/_{p\mathbb{Z}})$)*

Problem: Alice und Bob sollen öffentlich eine Geheimzahl vereinbaren.

Lösung:

- Alice und Bob vereinbaren eine große Primzahl p und Primitivwurzel w mod p
- Alice sucht geheimes a und berechnet $C_{AB} = w^a \mod p$ und sendet dieses (öffentlich) an Bob
- Bob sucht seinerseits ein geheimes b und berechnet $C_{BA} = w^b \mod p$ und sendet dieses (öffentlich) an Alice
- Alice rechnet $K := C_{BA}^a \mod p$
- Bob rechnet $K' := C_{AB}^b \mod p$
- Fazit: $K = K'$

praktisch nicht knacken: $a = \log_w C_{AB}, \quad b = \log_w C_{BA}$

Bemerkung 1.2 *„Lösen von $m^2 \equiv c \mod n$“ als Gleichung in m zu gegebenem c ist äquivalent zur Faktorisierung von n.*

1.1 Abelsche Gruppen

1.1.1 Grundbegriffe

Definition 1.1.1 *Eine Menge G zusammen mit einer Abbildung* $\cdot : G \times G \to G$*, so daß gilt*

1. *Für alle* $a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *Assoziativgesetz*
2. *Es existiert ein Element* $n \in G$*, so daß gilt:*
   a) $\forall\, a \in G : a \cdot n = n \cdot a = a$
   b) *zu jedem* $a \in G$ *existiert ein* $b \in G$ *mit* $a \cdot b = b \cdot a = n$

   heißt Gruppe.
   Gilt zusätzlich „$a \cdot b = b \cdot a\ \forall\, a, b \in G$*“ so heißt* $(G, \cdot)$ *eine abelsche Gruppe*

Beispiel

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Z}^n, +)$ Zeilenvektoren
3. ($SO(2, \mathbb{R})$, Matrixmultiplikation)
   $SO(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid 0 \leq \theta \leq 2\pi \right\}$
   Gruppe, weil $m(\theta)m(\phi) = m(\theta + \phi)$
4. $n \in \mathbb{Z}_0 : \mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ n-te Einheitswurzeln
   (μ_n, gew. Multiplikation)

Satz 1.1.2 (Die von „X erzeugte freie abelsche Gruppe“) *Sei X Menge*

$$\mathbb{Z}[X] := \{f :\ X \to \mathbb{Z} :\ f(x) = 0\ für\ fast\ alle\ x\ bis\ auf\ endlich\ viele\}$$

Dann wird durch

$$+ : \mathbb{Z}[X] \times \mathbb{Z}[X] \to \mathbb{Z}[X]$$

$$(f, g) \mapsto f + g,\ wo\ (f + g)(x) = f(x) + g(x)$$

die Struktur einer abelschen Gruppe auf $\mathbb{Z}[X]$ *definiert.*

Elegantere Schreibweisen: Identifiziere $x \in X$ mit dem Element in $\mathbb{Z}[X]$ für das gilt:
$x(y) = \begin{cases} 1 & x = y \\ 0 & sonst \end{cases}$
Damit: Ist $f \in \mathbb{Z}[X]: \ f = \sum_{x \in X} f(x) \cdot x$

Beispiel
Sei Ω Menge, $\mathcal{P}(\Omega) =$ Menge aller Teilmengen von Ω
Operation: $A + B := A \cup B \backslash (A \cap B)$

Satz 1.1.3 *Das Neutralelement ist eindeutig (und wird fortan mit 1 bezeichnet).*

Beweis 1.1 *Sei n' ein weiteres Element, welches auch 2) a) und b) erfüllt. Dann $n' = n' \cdot n = n$.*

Satz 1.1.4 *Das Element b aus 2) b) ist durch a eindeutig bestimmt (und wird mit a^{-1} bezeichnet)*

Beweis 1.2 *Es gelte $ba = b'a = 1$. Dann gilt auch:*

$$b = b \cdot 1 = b(ab') = (ba)b' = 1b' = b'$$

Satz 1.1.5 $(ab)^{-1} = b^{-1}a^{-1}$

Beweis 1.3 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$

Problem
Verschlüsselung von Botschaften
$A \quad B \quad C \mapsto D \quad E \quad F \qquad x \mapsto x + 3$
Manken:

1. Schlüssel „3“ muß übermittelt werden
2. zu simpler Algorithmus

Prototyp für bessere Chiffrierung: **Rivest-Shamir-Adleman** (RSA)
`public-key-Verfahren`, d.h. Verschlüsselungsmethode ist öffentlich
Wähle 2 große Primzahlen p,q jeweils ca. 200 Stellen und berechne deren Produkt $n = p \cdot q$. p und q sind geheim, während n der public key ist, also öffentlich bekannt.
Dazu berechne man noch $e \in \mathbb{Z}_{>0}$ mit $ggT(e, \underbrace{(p-1)(q-1)}_{\varphi(n)}) = 1$
geheim: p,q (und damit auch $\varphi(n)$)
öffentlich: n,e Chiffrierung mittels n und e:

Die Nachricht m soll verschickt werden, c ist das Chiffrat, also der verschlüsselte Text:
$m \to c := m^e \mod n$
Jeder kann mithören und kennt damit c (ich auch).
Dechiffrierung:

Bestimme mittels dem euklidischen Algorithmus ein d, so dass $e \cdot d \equiv 1 \mod (p-1)(q-1)$
damit gilt dann : $c^d \, mod \, n = (m^e)^d \mod n = m^{ed} \mod n = m^1 \mod n = m$
Chiffrieren: $()^e : \underset{\substack{primitive\ Restkl. \mod n \\ endl.\ Gruppe \\ Ordnung: \varphi(n)=(p-1)(q-1)}}{(\mathbb{Z}/_{n\mathbb{Z}})^*} \to (\mathbb{Z}/_{n\mathbb{Z}})^*$ ist Gruppenhomomorphismus.
Ich kann $()^e$ umkehren, weil ich das Geheimnis $\varphi(n)$ kenne.

Satz 1.1.6 *Seien $a, b \in G$. Dann existiert ein und nur ein $x \in G$ mit $a \cdot x = b$*

Beweis 1.4 *Eindeutigkeit:* $ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow x = a^{-1}b$ *Existenz:* $a(a^{-1}b) = b$

Äquivalente Formulierung
Ist $a \in G$, dann ist $m_a : G \to G, \; x \mapsto ax$ bijektiv.
Sei G endlich, also $G = \{a_1, \ldots, a_n\}$
Satz von eben $\Rightarrow$ In jeder Zeile (als auch in jeder Spalte) tritt jedes Gruppenelement nur 1-mal auf.
Falls G abelsch ist $\Rightarrow$ Tafel ist symmetrisch.

Satz 1.1.7 *Sei G eine Menge, sei $\cdot : G \times G \to G$ eine assoziative Operation und für edes $a \in G$ sei $m_a : G \to G, \; x \mapsto ax$ bijektiv. Dann ist $(G, \cdot)$ eine Gruppe.*

1.1.2 Homomorphismen

Definition 1.1.8 *1. Eine Abbildung $h : A \to B$ (A,B abelsche Gruppen) heißt Homomorphismus, falls gilt:* $h(ab) = h(a)\, h(b) \quad \forall\, a, b \in A$

2. (Gruppen-)Isomorphismus = bijektiver Homomorphismus

Satz 1.1.9 $h(1) = 1, \quad h(a^{-1}) = h(a)^{-1}$

Beweis 1.5 $h(1)\, h(1) = h(1 \cdot 1) = h(1) = 1$
$h(a)\, h(a^{-1}) = h(aa^{-1}) = h(1) = 1 \Rightarrow$ *Behauptung*

Beispiel
Sei $a \in A$ (A abelsche Gruppe). Definiere eine Abb. $\mathbb{Z} \to A$ durch

$$x \mapsto a^x := \begin{cases} \underbrace{a \cdot a \ldots a}_{x-mal} & x \in \mathbb{Z}_{>0} \\ 1 & x = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \ldots a^{-1}}_{x-mal} & x \in \mathbb{Z}_{<0} \end{cases}$$

$x \mapsto a^x$ ist ein Homomorphismus.

Definition 1.1.10 *A heißt zyklisch , falls ein $a \in A$ existiert, so daß die Abbildung $\mathbb{Z} \to A$, mit $x \mapsto a^x$ surjektiv ist.*
(äquivalent: $A = \{a^x \mid x \in \mathbb{Z}\}$)

Satz 1.1.11 *μ_n ist zyklisch.*

Beweis 1.6 $\mu_n = \{exp(2\pi\, i\frac{r}{n}) \mid 0 \le r < n\}$,
denn: exp: $(\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$ *ist Gruppenhomomorphismus:*
$exp(w + z) = exp(w)\, exp(z)$ *und* $e^{1\pi i} = 1$ *und* $e^z = 1 \Leftrightarrow z \in 2\pi i\mathbb{Z}$*)*
Also ist die Abbildung $\mathbb{Z} \to \mu_n$ *definiert durch* $x \to exp(2\pi i\frac{r}{n})$ *surjektiv.*

Beispiel
Sei X eine Menge. Betrachte ($\mathcal{P}(X)$, + (sym. Diff.)). Dann gilt für ein $T \in \mathcal{P}(X)$
$T + T(= T \cup T \backslash T \cap T) = \emptyset$, d.h. $2T = 0$
Falls $|X| \ge 2 \Rightarrow |P(X)| > 2$, also kann $\mathbb{Z} \to \mathcal{P}(X)$ mit $x \mapsto xT$ für kein T surjektiv sein.
Beispiel(für Gruppenhomomorphismus)
Seien $a_1, \ldots, a_n \in A$. Dann ist
$\circledast \quad \mathbb{Z}^n \to A, \quad x_1, \ldots, x_n \mapsto a_1^{x_1} \cdot a_2^{x_2} \cdot \ldots \cdot a_n^{x_n}$
ein Homomorphismus.
(nicht wahr für $n > 1$, falls A nicht abelsch wäre)

Definition 1.1.12 *A heißt endlich erzeugt, falls $a_1, \ldots, a_n \in A$ existieren, so daß $\circledast$ surjektiv ist. (d.h. $A = \{a_1^{x_1} \cdots a_n^{x_n} \mid x_1, \ldots, x_n \in \mathbb{Z}\}$)*

Beispiel

1. Jede endliche Gruppe ist endlich erzeugt.
2. $E := \{(x, y) \in \mathbb{Z}^2 \mid |x^2 - 5y^2| = 4$ mit (x,y) zugleich gerade bzw. ungerade $\}$
   $(1, 1),\ (2, 0) \in E$ und die Abbildung $\mathbb{Z}^2 \to E$ definiert durch $(m, n) \mapsto (2, 0)^m\ (1, 1)^n$ ist surjektiv.

Definition 1.1.13 *A heißt frei vom Rang n, falls $a_1, \ldots, a_n \in A$ existieren, so daß $\circledast$ bijektiv ist.*

Satz 1.1.14 *Ist $\mathbb{Z}^m$ isomorph zu $\mathbb{Z}^n$, so folgt $m = n$.*

Beweis 1.7 *Sei $e_1, \ldots, e_m$ kanonische Basis von $\mathbb{Z}^m$.*
Sei $u_1, \ldots, u_n$ kanonische Basis von $\mathbb{Z}^n$.
Sei $h : \mathbb{Z}^m \to \mathbb{Z}^n$ ein Isomorphismus.
Sei $h(e_j) = \sum_{i=1}^{n} u_i\, a_{ij}$ mit $(a_{ij} \in \mathbb{Z}\ geeignet)$.
Setze: $A = (a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le m}}$
Also: $h((x_1, \ldots, x_m)) = (x_1, \ldots, x_m)A^t$
Wäre $m > n$, dann gäbe es ein $0 \neq (x_1, \ldots, x_m) \in \mathbb{Z}^m :\ (x_1, \ldots, x_m)A^t = 0$.
Sei $N \in \mathbb{Z}_{>0}$ mit $Nx_1, \ldots, Nx_m \in \mathbb{Z}$
Also $y := N(x_1, \ldots, x_m) \in \mathbb{Z}^m$ und $h(y) = N(x_1, \ldots, x_m)A^t = 0$ also h kein Isomorphismus (Widerspruch)
Analog: $n > m$ $\Rightarrow$ Widerspruch.

Übung

1. Ist $h : \mathbb{Z}^n \to \mathbb{Z}^n$ ein Isomorphismus, so existiert ein $A \in GL(n, \mathbb{Z})$ mit $h(x) = xA$
2. Umgekehrt gilt für jedes $A \in GL(n, \mathbb{Z})$: Die Abbildung $x \to xA$ ist ein Isomorphismus.

$GL(n, \mathbb{Z}) = \{A \in \mathbb{Z}^{n \times n} \mid A\ invertierbar\ und\ A^{-1} \in \mathbb{Z}^{n \times n}\}$

1.1.3 Untergruppen

Definition 1.1.15 *Eine nichtleere Teilmenge $U \subseteq A$ heißt Untergruppe der abelschen Gruppe, falls:*

1. $ab \in U \quad \forall a, b \in U$
2. $a^{-1} \in U \quad \forall a \in U$

Bemerkung 1.3 *1) + 2) sind äquivalent zu $ab^{-1} \in U \qquad a, b \in U$*

Beispiel

1. triviale Untergruppen: $\{1\}, \quad A \subseteq A$
2. $\mu_3 \subseteq \mu_6$ allgemein $\mu_n \subseteq \mu_{nk} \quad k = 1, 2, \ldots$

Bemerkung 1.4 *Sei $U \subseteq A$, dann definiert $\cdot A \times A \to A$ bei Einschränkung auf $U \times U$ die Struktur einer abelschen Gruppe auf U.*

Satz 1.1.16 *Sind $U, T \subseteq A$ Untergruppen von A, so ist auch $UT := \{ut \mid u \in U,\ t \in T\}$ eine Untergruppe.*
Allgemein: Sind $U_1, \ldots, U_n \subseteq A$ Untergruppen, dann ist auch $U_1 \ldots U_n := \{u_1 \ldots u_n \mid u_i \in U_i\}$ Untergruppe von A.

Bemerkung 1.5 *i.A. für nicht abelsche Gruppen nicht wahr.*

Beispiel

1. $a \in A$, dann ist $< a >:= \{a^x \mid x \in \mathbb{Z}\}$ eine Untergruppe.
2. A zyklisch $\Leftrightarrow \exists\, a \in A :\ A =< a >$.
3. A endlich erzeugt $\Leftrightarrow \exists\, a_1, \ldots, a_n \in A :\ A =< a_1 >< a_2 > \ldots < a_n >$

Satz 1.1.17 *Jede Untergruppe von $\mathbb{Z}$ ist von der Gestalt:*
$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\} =< n >$ *für ein geeignetes n.*

Beweis 1.8 *Sei $U \subseteq \mathbb{Z}$ Untergruppe von $\mathbb{Z}$.*
Ist $U = \{0\}$ ✓
Ist $U \neq \{0\}$, dann existiert ein minimales $x \neq 0,\ x \in U$. Wir können $x > 0$ annehmen.
Zu zeigen: $U = x\mathbb{Z}$
„$\supseteq$“✓
„$\subseteq$“Sei $m \in U$, dann ist $m = qx + r$ mit geeigneten $q, r \in \mathbb{Z}, \quad 0 \leq r < x$
Damit: $r = m - qx$. Wegen der Minimalität von x, muß $r = 0$ gelten.$m = qx \in x\mathbb{Z}$

1.2 Nebenklassen

Definition 1.2.1 *G abelsche Gruppe und $A \subseteq G$ sei eine Untergruppe. Eine A-Nebenklasse in G ist eine Teilmenge $X \subseteq G$ der Gestalt $X = \{ra \mid a \in A\} = rA$ mit geeignetem $r \in G$.*

Satz 1.2.2 *Sei $A \subseteq G$ Untergruppe, G abelsch. Dann gilt:*

1. *Jedes $g \in G$ ist in einer A-Nebenklasse enthalten.*
2. *Sind X,Y zwei A-Nebenklassen, so ist $X \cap Y = \emptyset$ oder aber $X = Y$.*

Beweis 1.9 1. $g \in gA$

2. *Sei $X \cap Y \neq \emptyset$. Sei $r \in X \cap Y$. Sei etwa $X = sA$ mit geeignetem s. Also $r \in X = sA \Rightarrow r = sa$ mit geeignetem $a \in A$. Es gilt: $rA = saA = sA = X$ (denn $aA = A$).*

   Analog folgt $rA = Y$.

Bemerkung 1.6 *Satz besagt: „Die Gruppe G ist disjunkte Vereinigung von A-Nebenklassen.“.*

Satz 1.2.3 *Sei $|G| < \infty$. Ist A eine Untergruppe von G, so ist $|A|$ Teiler von $|G|$.*

Beweis 1.10 *Für $g \in G$ gilt $|gA| = |A|$. Schreibe $G = \bigcup_{i=1}^{r} g_i A$ mit geeigneten $g_1, \ldots, g_r \in G$. Damit $|G| = \sum_{i=1}^{r} |g_i A| = r|A|$*

Bemerkung 1.7 $[G : A] := \frac{|G|}{|A|}$ *= Anzahl der verschiedenen A-Nebenklassen („Index von A in G “).*

Definition 1.2.4 *Für allgemeine G und $A \subseteq G$ setzt man $[G : A]$:= Anzahl der verschiedenen A-Nebenklassen.*

Beispiel

1. A=G
2. $G = \mathbb{Z}, A = 2\mathbb{Z}$. Die Nebenklassen sind dann:
   $A = 2\mathbb{Z}$ und $1 + 2\mathbb{Z} = 1 + A \Rightarrow [\mathbb{Z} : 2\mathbb{Z}] = 2$

Satz 1.2.5 *Sei $|G| < \infty$ und $a \in G$. Dann gilt $a^{|G|} = 1$.*

Beweis 1.11 *Sei* $r = \min\{n \in \mathbb{Z}_{>0} \mid a^n = 1\}$ = *Ordnung von a. r existiert, denn:*
$< a >= \{a^x \mid x \in \mathbb{Z}\}$.
Wähle $x, y > 0$ *mit* $a^x = a^y$ *und* $x > y$. *Dann gilt*
$a^{x-y} = 1, \quad x - y > 0$.
Es gilt also $| < a > | = r$.
($\Rightarrow$*(nach vorigem Satz) r teilt* $|G|$, *also* $a^r = (a^r)^{\frac{|G|}{r}} = 1$)
Denn: $< a >= \{a^x \mid 0 \leq x < r\}$ *und* $a^x \neq a^y$ *für* $0 \leq x < y < r$
(sonst $a^{x-y} = 1$ *und das wäre Widerspruch zu r Minimum)*
gezeigt wird noch: $< a >= \{a^x \mid 0 \leq x < r\}$.
$\supseteq$ *ist klar.*
$\subseteq$*: sei* $y \in \mathbb{Z}$, *dann existieren ein q und ein* $x \in \mathbb{Z}$ *mit* $y = qr + x$, *wobei* $0 \leq x < r$.
Damit $a^y = a^{qr+x} = (a^r)^q a^x = a^x \in$ *rechter Seite.*

1.2.1 Einschub: der Elementarteilersatz

Definition 1.2.6 *Sei F eine endlich erzeugte abelsche Gruppe.* $\{w_1, \ldots, w_n\} \subset F$ *ist Basis von F, falls*

$$\varphi : \mathbb{Z}^n \to F \text{ mit } \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \to \quad \alpha_1 w_1 + \ldots + \alpha_n w_n$$

ein Gruppenhomomorphismus ist.
Eine endl. erzeugte Gruppe F heißt frei, falls eine Basis existiert.

Satz 1.2.7 (Elementarteilersatz) *Sei* $F \neq \{0\}$ *Untergruppe von* $\mathbb{Z}^n$, *dann existiert eine Basis* $b_1, \ldots, b_n$ *von* $\mathbb{Z}^n$ *und* $\alpha_i \in \mathbb{N}, i = 1, \ldots, n : \alpha_1 \neq 0, \alpha_i \mid \alpha_{i+1}$,
$i = 1, \ldots, n-1$, *derart daß* $\{\alpha_1 b_1, \ldots, \alpha_n b_n\}$ *Basis von F ist.*

Korollar 1.2.8 *Jede Untergruppe von* $\mathbb{Z}^n$ *ist frei.*
Jede Untergruppe einer freien Gruppe ist frei.

Bemerkung 1.8 *Kommutative Algebra* $\rightsquigarrow$ *Moduln über kommutativen Ringen (Verallg. des Vektorraums über einem Körper) abelsche Gruppen* $\overset{1:1}{\leftrightarrow}$ *Moduln über* $\mathbb{Z}$
Elementarteilersatz gilt für freie Moduln über Hauptidealringen (statt freie abelsche Gruppen)

Beweis 1.12 *zum Elementarteilersatz per (Induktion über n)*
IA: n=1: $\Rightarrow \exists a_1 \in \mathbb{Z} : F = a_1\mathbb{Z}$ ✓
IS: $n - 1 \to n$:
Seien $u \in F, k_i \in \mathbb{N}$ *und* $w_1, \ldots, w_n$ *Basis von* $\mathbb{Z}^n$ *(und damit auch automatisch Basis des* $\mathbb{Q}^n$*) mit* $u = k_1 w_1 + \ldots + k_n w_n$ *derart,*
daß, falls $u' \in F, 0 < k_1' \in \mathbb{N}$, $w_1', \ldots, w_n'$ *Basis des* $\mathbb{Z}^n$ *mit*

$u' = k_1'w_1' + \ldots + k_n'w_n'$ *und* $k_1 > 0$ *gilt* $k_1' \geq k_1$.
Wähle $\alpha_1 := k_1$ *und weiter* $k_i := q_i\alpha_1 + s_i$, *wobei* $q_i \in \mathbb{N},\ s_i = 0, \ldots, \alpha_1 - 1$ *und* $\{(w_1 + q_iw_i), w_2, \ldots, w_n\}$ *Basis des* $\mathbb{Z}^n$.
$u = \alpha_1(w_1 + q_iw_i) + k_2w_2 + \ldots + s_iw_1 + \ldots + k_nw_n, \quad 0 \leq s_i < \alpha_1$
$\overset{\alpha_1 minimal}{\Rightarrow} s_i = 0 \Rightarrow$ *alle* k_i *sind durch* α_1 *teibar.*
$b_1 := w_1 + q_2w_2 + \ldots + q_nw_n \Rightarrow \alpha_1 b_1 = u \in F.$

Es gilt: $F = \mathbb{Z}(\alpha_1 b_1) \oplus (\underbrace{F \cap \overbrace{(\mathbb{Z}w_2 \oplus \ldots \mathbb{Z}w_n)}^{\cong \mathbb{Z}^{n-1}}}_{=:F' \subset \mathbb{Z}^{n-1}})$
$\Rightarrow$ *nach Induktionsvoraussetzung* $\exists$ *eine Basis* $b_2, \ldots, b_n$ *von* $\mathbb{Z}w_2 \oplus \ldots \oplus \mathbb{Z}w_n$
$\Rightarrow \{b_1, b_2, \ldots, b_n\}$ *ist Basis von* $\mathbb{Z}^n, \alpha_2, \alpha_3, \ldots.$ *wie in Satz*
$\Rightarrow \{\alpha_2w_2, \ldots, \alpha_nw_n\}$ *Basis von F'*
$\Rightarrow \{\alpha_1b_1, \alpha_2b_2, \ldots \alpha_nb_n\}$ *bilden Basis von F, bleibt zu zeigen:* $\alpha_1 | \alpha_2$
$u_1 := \alpha_1b_1 + \alpha_2b_2$, $\alpha_2 = p\alpha_1 + r$, *mit* $0 \leq r < \alpha_1$
$= \alpha_1(b_1 + pb_2) + rb_2 + 0b_3 + \ldots + 0b_n$
$\{b_1, \ldots, b_n\}$ *Basis von* $\mathbb{Z}^n \Rightarrow r = 0$

Korollar 1.2.9 (Übung) *Sei* $M \in Mat(n \times m, \mathbb{Z})$.
Dann $\exists U \in GL(n, \mathbb{Z}), \exists V \in GL(m, \mathbb{Z})$:

$$UMV = \begin{pmatrix} \alpha_1 & 0 & \cdots & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & 0 & 0 \\ \vdots & \cdots & 0 & \alpha_n & 0 \\ \vdots & \cdots & \cdots & 0 & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \qquad \alpha_i \in \mathbb{N}^*, \quad \alpha_i | \alpha_{i+1}, \quad i = 1, 2, \ldots$$

F endl. abelsche Gruppe mit Erzeugenden $a_1, \ldots, a_n$
$\varphi : \mathbb{Z}^n \to F$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \to \alpha_1a_1 + \ldots + \alpha_na_n$$

$\Rightarrow FF \simeq \mathbb{Z}/Kern(\varphi)$

Satz 1.2.10 *Sei* $f : A \to B$ *Homomorphismus, dann sind*
$Kern(f) := \{a \in A \mid f(a) = 1\}$ *und* $Bild(f) := \{f(a) \mid a \in A\}$
Untergruppen.

Definition 1.2.11 *Sei A abelsche Gruppe, dann definiert man:*
$A_n\ (= A[n]) := \{a \in A \mid a^n = 1\} \quad (n \in \mathbb{Z}_{>0})$
$A^n := \{a^n \mid a \in A\}$

Satz 1.2.12 *Ist A abelsch, dann sind* $A_n,\ A^n$ *Untergruppen.*

Beweis 1.13 A_n *und* A^n *sind Kern und Bild des Homomorphismus* $a \to a^n$ *(abelsch* $\Rightarrow (ab)^n = a^n b^n$*).*

Beispiel
$G := (\mathbb{C}^*$, gewöhnliche Multiplikation$)$, $G_n = \mu_n,\ G^n = g$
(hier: $x \to x^n$ surjektiv, nicht injektiv)

Definition 1.2.13 *1. Es existiere ein* $n \in \mathbb{Z}_{>0}$ *mit* $A^n = \{1\}$*. Das kleinste n, so daß* $A^n = \{1\}$ *heißt Exponent von A.*

2. X bel. Menge $(\mathcal{P}(X), symmetrische\ Differenz)$*,* $\mathcal{P}(X)$ *hat Exponent 2 (außer* $X = \{\emptyset\}$*)*

Definition 1.2.14 $A_{tor} := \{a \in A \mid a^n = 1$ *für ein* $n \in \mathbb{Z}_{>0}\}$ *Torsionsuntergruppe von A.*
$A_{tor} = \bigcup\limits_{n \in \mathbb{Z}_{>0}} A[n]$

Satz 1.2.15 *Ist A abelsch, dann ist* A_{tor} *tatsächlich Untergruppe.*

Beweis 1.14 $a, b \in A_{tor}$*, sei* $a^n = 1,\ b^m = 1$ *mit* $m, n \in \mathbb{Z}_{>0}$ *geeignet, dann ist* $(ab)^{mn} = 1$*, denn* $a^{mn} b^{mn}$ *und A abelsch.*

1.2.2 Faktorgruppen

Definition 1.2.16 *Sei* $U \subseteq A$ *Untergruppe. Definiere*
A/U :=*Menge aller U-Nebenklassen.*

Bemerkung 1.9 $A = \dot{\bigcup\limits_{X \in A/U}} X$

Satz 1.2.17 *1. Sind X, Y U-Nebenklassen, so ist auch*

$X \cdot Y := \{x \cdot y \mid x \in X,\ y \in Y\}$ *eine Nebenklasse.*

(Beweis: $X = aU,\ Y = bU$*, dann* $XY = aUbU = abU$*)*

2. Vermöge der Operation $(X, Y) \mapsto X \cdot Y$ *wird die Menge* A/U *zu einer ablschen Gruppe.*

(Beweis: Neutralelement U, $X^{-1} = \{x^{-1} \mid x \in X\}$*,*
$X = aU \ \Rightarrow\ X^{-1} = a^{-1}U$*)*
$(A/U, \cdot)$ *heißt* `Faktorgruppe`*.*

Beispiel
$n \in \mathbb{Z}_{>0}$: $\mathbb{Z}/n\mathbb{Z}$ Gruppe der Restklassen mod n
$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$
Bezeichnung: $a + n\mathbb{Z} =: a \mod n$
Tatsächlich:

a) $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid 0 \leq r < n\}$
(Beweis: „$\supseteq$“: ✓
„$\subseteq$“: Betrachte $a + n\mathbb{Z}$, schreibe $a = qn + r,\ q, n \in \mathbb{Z},\ 0 \leq r < n$, damit $a + n\mathbb{Z} = r + \underbrace{qn + n\mathbb{Z}}_{n\mathbb{Z}})$

b) $0 \leq r,\ s < n \quad r + n\mathbb{Z} = s + n\mathbb{Z} \quad \Rightarrow \quad r = s$
(Beweis: $r - s \in n\mathbb{Z}$, d.h. $n \mid r - s$ aber $|r - s| < n$, daher $r - s = 0$)

$|\mathbb{Z}/n\mathbb{Z}| = n$
$\mathbb{Z}/n\mathbb{Z}$ ist zyklisch: $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x \cdot (1 + n\mathbb{Z})$ ist surjektiv.

Satz 1.2.18 *A/A_{tor} ist torsionsfrei (d.h. $(A/A_{tor})_{tor} = \{1\}$)*

Beweis 1.15 *Sei $X \in A/A_{tor}$ und sei $X^n = 1$ für ein $n > 0$, d.h. mit $X = a \cdot A_{tor}$, daß $a^n\ A_{tor} = A_{tor}$, also $a^n \in A_{tor}$, daher: es existiert $m > 0$ mit $(a^n)^m = 1$. Also $a \in A_{tor}$.*
Fazit: $X = aA_{tor} = A_{tor} (= 1\ in\ A/A_{tor})$

Beispiel
$\mathbb{C}^*/\mu$ ist torsionsfrei $\mu := (\mathbb{C}^*)_{tor} = \bigcup_{n>0} \mu_n$

1.2.3 Homomorphiesatz

$U \subseteq A$ Untergruppe, $\pi : A \to A/U, \quad a \mapsto aU$ „kanonische Projektion“ ist Homomorphismus.

Satz 1.2.19 *Sei $f : A \to B$ ein Homomorphismus.*

1. *Dann existiert ein und nur ein Homomorphismus*
   $\underline{f} : A/Ker(f) \to B$, *so daß das Diagramm:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{\pi} \quad \nearrow_{\underline{f}} & \\ & A/Ker(f) & \end{array}$$

kommutativ ist. (d.h. $\underline{f} \circ \pi = f$)

2. *$\underline{f}$ ist injektiv (insbesondere: Ist f surjektiv, so ist $\underline{f}$ ein Isomorphismus)*

Bemerkung 1.10 $Kern(f) = \{1\}$, $A/Ker(f) = \{\ \{a\}\ |a \in A\} \neq A$

Beispiel
$a \in A, \quad f : \mathbb{Z} \to A, \quad x \mapsto a^x$, sei A zyklisch (f surjektiv)

$$Kern(f) = \begin{cases} \{0\} & \Rightarrow \mathbb{Z} \overset{f}{\approx} A \\ n\mathbb{Z}\ f\ddot{u}r\ ein\ n \in \mathbb{Z}_{>0} & \Rightarrow \mathbb{Z}/n\mathbb{Z} \overset{\bar{f}}{\approx} A \end{cases}$$

Satz 1.2.20 *Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $n\mathbb{Z}$ für ein $n > 0$*

Beweis 1.16 *(Homomorphiesatz)*

Eindeutigkeit *Sei $\underline{f}$ so, daß das Diagramm kommutativ ist, dann $X = aKer(f) = \pi(a)$, dann*
$\underline{f}(X) = \underline{f}(\pi(a)) = f(a)$
$\rightsquigarrow$ *f eindeutig*

Existenz *Definiere $\underline{f}$ via $\underline{f}(X) := f(a)$ für ein $a \in X$*
Wohldefiniertheit: Seien $a, b \in X$, dann $a = bk$ für ein $k \in Ker(f)$
$f(a) = f(bk) = f(b)f(k) = f(b)$
Homomorphie: Übung

1. *Sei $\underline{f}(X) = 1, \quad X = aKer(f)$*
Aber $\underline{f}(X) = f(a)$, also $a \in Ker(f) \quad \Rightarrow \quad X = Ker(f)$

1.2.4 Direkte Produkte

Definition 1.2.21 *Definiere auf $A \times B$ eine Operation:*
$\circledast \quad (a, b) \bullet (a', b') := (aa', bb')$

Satz 1.2.22 *$A \times B$ versehn mit $\circledast$ ist eine abelsche Gruppe (direktes Produkt von A, B)*

Beispiel
Sei X endliche Menge, $X = \{e_1, \ldots, e_n\}$
$\times_{i=1}^{n} P(\{e_i\}) = P(\{e_1\}) \times P(\{e_2\}) \times \ldots \xrightarrow{\varphi} P(X)$
$(T_1, T_2, \ldots, T_n) \mapsto \bigcup_{i=1}^{n} T_i$

Übung
φ ist Gruppenisomorphismus.

Satz 1.2.23 $A \times B/\{1\} \times B \approx A$

Beweis 1.17 *Betrachte* $A \times B \xrightarrow{f} A, \quad (a,b) \mapsto a$
ist Homomorphismus, ist surjektiv, $Ker = \{1\} \times B$,
Homomorphiesatz sagt:
$A \times B/\{1\} \times B \xRightarrow{f} A$ *ist Isomorphismus.*

Satz 1.2.24 $A \times B/U \times V \approx A/U \times B/V$

Beweis 1.18 $A \times B \to A/U \times B/V, \quad (a,b) \mapsto (aU, bV)$ *Homomorphismus, surjektiv,* $Ker = U \times V$. $\Rightarrow$ *Homomorphiesatz anwenden.*

Satz 1.2.25 ***Chinesischer Restsatz***
$\mathbb{Z}/mn\mathbb{Z} \approx \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *falls* $ggT(m,n) = 1$

Beweis 1.19 *Betrachte* $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$a + mn\mathbb{Z} \mapsto (a \mod m, a \mod n)$
Wohldefiniertheit ✓
Homomorphismus ✓
Surjektivität ($\Rightarrow$ *auch injektiv, also Isomorphismus)*
Es gibt $x, y \in \mathbb{Z}$ *mit* $1 = mx + ny$
$m\mathbb{Z} + n\mathbb{Z}$ *ist Untergruppe von* $\mathbb{Z}$*, also* $= t\mathbb{Z}, t > 0$ *geeignet*
$m \in t\mathbb{Z}$*, also* $t \mid m$*;*
$n \in t\mathbb{Z}$*, also* $t \mid n$ *wegen* $(m,n) = 1$*, also* $t = 1$
Sei $(a \mod m, b \mod n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
Setze: $A := any + bmx$*. Dann gilt damit*
$\varphi(A \mod mn) = \varphi(A \mod m, A \mod n)$
$A + m\mathbb{Z} = any + bmx + m\mathbb{Z} = any + m\mathbb{Z} = a(1 - mx)\mathbb{Z} = a + m\mathbb{Z}$
analog: $A + n\mathbb{Z} = b + n\mathbb{Z}$

1.2.5 Untergruppen von $\mathbb{Z}^n$

textbfErinnerung: Untergruppe von $\mathbb{Z}$: $\mathbb{Z}n$ mit $n \in \mathbb{Z}$ und $\mathbb{Z}^n$ Zeilenvektoren

Satz 1.2.26 *Sei* $U \subseteq \mathbb{Z}^n$ *Untergruppe. Dann gibt es ein* $N \in \mathbb{Z}^{r \times n}$, $r \leq n$*, N mit Rang r, so daß* $U = \mathbb{Z}^r N (= \{xN \mid x \in \mathbb{Z}^r\})$
N ist eindeutig bis auf Linksmultiplikation mit Elementen in $GL(r, \mathbb{Z})$.

Bemerkung 1.11 $GL(1, \mathbb{Z}) = \{\pm 1\}$ *(Es kann ein N eindeutig gewählt werden via der Theorie der „Hermite Normal Form“)*

Äquivalente Formulierung
Jede Untergruppe $U \subseteq \mathbb{Z}^n$ besitzt eine $\mathbb{Z}$-Basis der Länge $r \leq n$ (d.h. es gibt Zeilenvektoren $w_1, \ldots, w_r$, so daß die Abbildung $\mathbb{Z}^r \to U$,
$(x_1, \ldots, x_r) \mapsto x_1 w_1 + \ldots + x_r w_r$ ein Isomorphismus ist.

Beweis 1.20 *Induktion über n*
n=1 ✓ ($U = t\mathbb{Z}$, so ist $\mathbb{Z} \to U,\ x \mapsto tx$ Isomorphismus)
Sei jetzt $U \subseteq \mathbb{Z}^n$

Fall 1: $U \subseteq \mathbb{Z}^{n-1} \times \{0\}$ O.K. nach I.V.

Fall 2: Sonst.
Betrachte $\{\alpha \mid \alpha$ ist letzte Komponente eines Vektors in $U\}$ ist Untergruppe von $\mathbb{Z}$, also $= \mu\mathbb{Z}$, mit μ gegeignet.
Sei $w \in U$ mit $w = (*, \mu)$, $U' = U \cap (\mathbb{Z}^{n-1} \times \{0\})$ ist Untergruppe von $\mathbb{Z}^{n-1} \times \{0\}$, nach I.V. existiert ein Isomorphismus $\Phi :\ \mathbb{Z}^s \to U',\ s \leq n-1$.
Dann ist aber $\tilde{\Phi} :\ \mathbb{Z}^{s+1} \to U$ mit $\tilde{\Phi}((x, \alpha)) := \Phi(x) + \alpha(w)$ ein Isomorphismus.

Satz 1.2.27 *(Elementarteilersatz) Sei U eine r-dimensionale Untergruppe von $\mathbb{Z}^n$. Es existiert eine Basis $b_1, \ldots, b_n$ von $\mathbb{Z}^n$, $\quad \gamma_1, \ldots, \gamma_r \in \mathbb{Z}_{>0}$ mit $\gamma_i \mid \gamma_{i+1}$ so daß $\gamma_1 b_1, \ldots, \gamma_r b_r$ Basis von U.*

Bezug zu N: Zeilen von N sind Basis von U. Also existiert $S \in GL(r, \mathbb{Z})$, so daß

$$SN = \left(\begin{array}{cccc|c} \gamma_1 & & & & & \\ & \gamma_2 & & & & 0 \\ & & \ddots & & & \\ & & & \gamma_r & & \end{array}\right) \begin{pmatrix} b_1 \\ \vdots \\ \vdots \\ b_n \end{pmatrix}$$

Also: Es gilt $S \in GL(r, \mathbb{Z}),\ R \in GL(n, \mathbb{Z})$, so daß

$$SNR = \left(\begin{array}{cccc|c} \gamma_1 & & & & & \\ & \gamma_2 & & & & \\ & & \ddots & & & 0 \\ & & & \gamma_r & & \end{array}\right) \gamma_i | \gamma_{i+1}$$

Bemerkung 1.12 $r = n : \det N = \gamma_1 \ldots \gamma_r$

Satz 1.2.28 $\mathbb{Z}^n / U \approx \mathbb{Z}/\gamma_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\gamma_r\mathbb{Z} \times \mathbb{Z}^{n-r}$

Beweis 1.21 $\mathbb{Z}^n \to \mathbb{Z}/\gamma_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\gamma_r\mathbb{Z} \times \mathbb{Z}^{n-r}$
$\sum_{i=1}^{n} x_i\, b_i \mapsto (x_1 \mod \gamma_1,\ x_2 \mod \gamma_2, \ldots, x_r \mod \gamma_r,\ x_{r+1}, \ldots, x_n)$ *ist Gruppenhomomorphismus, surjektiv, Ker=U: Homomorphiesatz $\Rightarrow$ Behauptung*

Korollar 1.2.29 *$\mathbb{Z}^n/U$ ist endlich genau dann, wenn $r = n$ (d.h. wenn $U = \mathbb{Z}N$, $N \in \mathbb{Z}^{n\times n}$ voller Rang) Ist $r = n$, dann gilt $[\mathbb{Z}^n : U]$=$\gamma_1 \dots \gamma_r = \det N$*

Beispiel
Bestimme Untergruppen U vom Index 5 in $\mathbb{Z}^2$.
Ansatz: $U = \mathbb{Z}^2 N$, wobei $N \in \mathbb{Z}^{2\times 2}$ und $\det N \neq 0$
$[\mathbb{Z}^2 : U]$= 5 $\Rightarrow$ $\det N = 5$.
Wir dürfen N von links mit Matrizen in $GL(2, \mathbb{Z})$ multiplizieren.
Uebung
Durch Linksmultiplikation mit geeignetem $R \in GL(2, \mathbb{Z})$ kann man erreichen

$$N' = RN = \begin{cases} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} & N' : \ Hermite\ Normal\ Form \\ \begin{pmatrix} 1 & b \\ 0 & 5 \end{pmatrix} & 0 \leq b < 5 \end{cases}$$

1.2.6 Struktursatz für endlich erzeugte abelsche Gruppen

Satz 1.2.30 *Sei A endlich erzeugte abelsche Gruppe. Dann gibt es einen Gruppenisomorphismus*
$A \approx \mathbb{Z}r \times \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}$
für geeignetes $r \geq 0$ Primzahlpotenzen $p_i^{\alpha_i}$ $(\alpha_i > 0)$. Die Zahl r (heißt Rang von A) und die Primzahlpotenzen $p_i^{\alpha_i}$ (bis auf Reihenfolge) sind durch A eindeutig bestimmt.

Beweis 1.22 *A endlich erzeugt, d.h. es gibt surjektiven Gruppenhomomorphismus $\mathbb{Z}^n \underset{f}{\to}$ A. Sei $U := Ker(f)$, dann haben wir einen Isomorphismus*
$\underline{f} : \mathbb{Z}^n/U \to A$.
Satz von eben: $\mathbb{Z}^n/U \approx \mathbb{Z}/\gamma_1\mathbb{Z} \times \ldots \times \mathbb{Z}/\gamma_k\mathbb{Z} \times \mathbb{Z}^l$ $\gamma_1|\gamma_2| \ldots |\gamma_k$, $l \in \mathbb{Z}_{\geq 0}$ geeignet.
$\mathbb{Z}/\gamma_1\mathbb{Z} \approx \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ falls $ab = \gamma_1$, $(a, b) = 1$.
Iterieren dieser Zerlegung ergibt:
$\mathbb{Z}/\gamma_i\mathbb{Z} \approx$ direktes Produkt von $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, $p_i^{\alpha_i}$ Primpotenzen.

Eindeutigkeit:

Sei $A = \mathbb{Z}^r \times \mathbb{Z}/p_1^{\alpha_1} \times \ldots \times \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}$

1. $A_{tor} = \{0\} \times \mathbb{Z}/p_1^{\alpha_1} \times \ldots \times \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}$
   (denn $n(x_1, \ldots, x_r, y_1 \mod p_1^{\alpha_1}, \ldots, y_s \mod p_s^{\alpha_s}) = 0 \quad (n > 0)$
   $\Rightarrow \quad nx_1 = \ldots = nx_r = 0 \quad \Rightarrow \quad x_1 = \ldots = x_r = 0$)
2. $A/A_{tor} (\approx \mathbb{Z}^r/\{0\}) \approx \mathbb{Z}^r$

3. *Damit r eindeutig bestimmt durch A ($\mathbb{Z}^r \nsim \mathbb{Z}^s$ für $r \neq s$) r:= Rang von A*

4. *Setze $B := A_{tor}$ Betrachte $C := \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ es gilt:*

   Sei p^α irgendeine Primpotenz. $p^{\alpha-1}C/p^\alpha C \approx \begin{cases} \mathbb{Z}/p\mathbb{Z} & p_i | p_i^{\alpha_i} \\ \{0\} & sonst \end{cases}$

5. *Daher* $|p^{\alpha_1}B/p^\alpha B| = p^{\#\{i \mid p^\alpha | p_i^{\alpha_i}\}}$

   Für gegebene (beliebige) Primpotenz p^α gilt also:

   $\#\{i \mid p_i^{\alpha_i} = p^\alpha\} = \log_p |p^{\alpha-1}B/p^\alpha B| - \log_p |p^\alpha B/p^{\alpha+1}B|$

Kapitel 2

Die Gruppe der primen Restklassen

2.1 Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Wir setzen:
$\circledast \qquad (x \mod n) \cdot (y \mod n) := (xy) \mod n$

Satz 2.1.1 *Die Operation $\circledast$ (d.h. die Abbildung $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$) ist wohldefiniert.*
Zusammen mit der Addition wird hierdurch die Struktur eines Ringes auf $\mathbb{Z}/n\mathbb{Z}$ erklärt.
(d.h. es gilt: $\circledast$ ist assoziativ, kommutativ und es gilt:
$a(b+c) = ab + ac \quad \forall\, a, b, c \in \mathbb{Z}/n\mathbb{Z}$*)*

Beweis 2.1 *Sei* $x \mod n = x' \mod n,\ y \mod n = y' \mod n$
Dann: $x - x' \in n\mathbb{Z},\ y - y' \in n\mathbb{Z}$
Also: $y(x - x') \in n\mathbb{Z},\ x'(y - y') \in n\mathbb{Z}$
daher: $y(x - x') + x'(y - y') \in n\mathbb{Z}$
$xy - x'y' \in n\mathbb{Z}$*, d.h.* $xy \mod n = x'y' \mod n$

Schreibweise
$x \equiv y \mod n, \qquad x \equiv_n y \qquad$ für $x \mod n = y \mod n$
(d.h. $x + n\mathbb{Z} = y + n\mathbb{Z}$, d.h. $x - y \in n\mathbb{Z}$)

Rechenregeln
$x \equiv_n x', \quad y \equiv_n y'$
$\Rightarrow \quad x + y \equiv_n x' + y'$ oder $xy \equiv_n x'y'$

Definition 2.1.2 $(\mathbb{Z}/n\mathbb{Z})^* := \{a \in \mathbb{Z}/n\mathbb{Z} \mid \exists\, b \in \mathbb{Z}/n\mathbb{Z} :\ ab = 1\}$
Gruppe der primen (primitiven) Restklassen mod n.

Bezeichnung
Ist R Ring mit 1, dann $R^* = \{a \in R \mid \exists\, b \in R :\ ab = 1\}$
Gruppe der Einheiten

Satz 2.1.3 *$(\mathbb{Z}/n\mathbb{Z})^*$ versehen mit der Multiplikation $\circledast$ bilden eine abelsche Gruppe.*

Definition 2.1.4 $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$ `Eulersche φ-Funktion`

Satz 2.1.5 *Sei $a \in \mathbb{Z}$. Dann gilt: $a \mod n \in (\mathbb{Z}/n\mathbb{Z})^*$ genau dann, wenn $ggT(a,n) = 1$.*

Folgerung 2.1.6 $\varphi(n) = \#\{a \in \mathbb{Z} \mid 0 \le a < n \quad ggT(a,n) = 1\}$

Beweis 2.2 *„⇒“: Es existiere $b \in \mathbb{Z}$ mit $ab \equiv 1 \mod n$*
$\Rightarrow \quad \exists\, x :\ 1 = ab + nx$
$\Rightarrow$ *Ist $t \mid a, n$ dann $t = 1$*
$\Rightarrow \quad ggT(a,n) = 1$
„⇐“: Sei $ggT(a,n) = 1$, dann $\exists\, x, y \in \mathbb{Z} :\ ax + ny = 1$
(denn $a\mathbb{Z} + n\mathbb{Z} = c\mathbb{Z}$ für ein c, also $\exists\, x, y$ mit $ax + ny = c$, aber $c \mid a,\ c \mid n$ daher $c \mid ggT(a,n) = 1$, also $c = \pm 1$, etwa $c = 1$) d.h. $ax \equiv 1 \mod n$

Beispiel
$\varphi(12) = \#A \qquad A := (\mathbb{Z}/12\mathbb{Z})^* \qquad \varphi(12) = 4$
$A = \{1,\ 5 \mod 12, 7 \mod 12, 11 \mod 12\} \approx \{1, 5 \mod 12\} \times \{1, 7 \mod 12\}$
$\approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Satz 2.1.7 *(Euler-Fermat)*
Ist $n \in \mathbb{Z},\ a \in \mathbb{Z},\ ggT(a,n) = 1$, dann $a^{\varphi(n)} \equiv 1 \mod n$
Insbesondere: Ist $n = p$ Primzahl, dann $a^{p-1} \equiv 1 \mod p$

Satz 2.1.8 *Sei p Primzahl, dann ist jedes von 0 verschieden Element von $\mathbb{Z}/p\mathbb{Z}$ (multiplikativ) invertierbar. (d.h. ist $a \in \mathbb{Z},\ p \nmid a$, dann $\exists\, b \in \mathbb{Z}$ mit $ab \equiv 1 \mod p$)*

2.2 Struktur der Gruppen $(\mathbb{Z}/n\mathbb{Z})^*$

Satz 2.2.1 $(\mathbb{Z}/n\mathbb{Z})^* \approx \underset{p^\alpha \| n}{\times} (\mathbb{Z}/p^\alpha\mathbb{Z})^*$

Beispiel
$(\mathbb{Z}/36\mathbb{Z})^* \approx \underset{<7 \mod 9>}{(\mathbb{Z}/4\mathbb{Z})^*} \times \underset{<2 \mod 9>}{(\mathbb{Z}/9\mathbb{Z})^*} \approx (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$
$\approx (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

Beweis 2.3 *Ist* $(a,b)=1$*, dann haben wir den Isomorphismus abelscher Gruppen:*
$\mathbb{Z}/ab\mathbb{Z} \xrightarrow{f} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$
$n \mod ab \to (n \mod a, n \mod b)$ *(chinesischer Restsatz)*
f ist verträglich mit der Restklassenmultiplikation (vornehm: f ist Ringisomorphismus)
Damit erhält man durch Einschränkung einen Isomorphismus:
$(\mathbb{Z}/ab\mathbb{Z})^* \xrightarrow{f'} (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$

Folgerung 2.2.2 $\varphi(n) = \prod\limits_{p^\alpha | n} \varphi(p^\alpha)$

Satz 2.2.3 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1-\frac{1}{p})$

Folgerung 2.2.4 $\varphi(n) = n\prod\limits_{p|n}(1-\frac{1}{p})$

Test:
$\varphi(36) = 36(1-\frac{1}{2})(1-\frac{1}{3}) = 36 \cdot \frac{2}{6} = 12$

Beweis 2.4

0	*1*	*2*	*3*	$\dots$	$p^\alpha - 1$	
0	*p*	*2p*		$\dots$	$p^{\alpha-2}p$	*ausstreichen*
$p^\alpha - p^{\alpha-1}$						*bleiben*

Satz 2.2.5 *Ist* $p \neq 2$ *Primzahl, so ist* $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ *zyklisch.*
Also $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \approx \times\limits_{q^\beta \| p^\alpha(1-\frac{1}{p})} \mathbb{Z}/q^\beta\mathbb{Z}$

Beweis 2.5 $\alpha = 1$ *(*$\alpha > 1$ *war Übungsaufgabe), d.h. zu zeigen:* $(\mathbb{Z}/p\mathbb{Z})^*$ *zyklisch.*
Allgemeiner: Sei K Körper (d.h. ein Ring, in dem jedes von 0 verschiedene Element (multiplikativ) invertierbar ist)
Sei $A \subseteq K^*$ *(*$k\backslash\{0\}$ *versehen mit Multiplikation: abelsche Gruppe) endlich, dann ist A zyklisch: (z.B.* μ_n *ist zyklisch:* $\mu_n =< e^{2\pi i/n} >$*)*
Sei $n := \#A$*. Sei* $A(d) = \#\{a \in A \mid Ordnung\ von\ a\ ist\ gleich\ d\}$
Es gilt:

1. $\sum\limits_{d|n} A(d) = n$ *(klar)*
2. $\sum\limits_{d|n} \varphi(d) = n \quad \big(\frac{0}{n} \quad \frac{1}{n} \quad \frac{2}{n} \dots \frac{n-1}{n} \quad \circledast \quad n\ Br\ddot{u}che\big)$

   kürzen:

a) Es gibt genau $\varphi(d)$ gekürzte Brüche mit Nenner $d > 0$ und in $[0, 1)$

b) Jeder gekürzte Bruch $\in [0, 1]$ und mit Nenner $d \mid n$ kommt unter den Brüchen $\circledast$ vor

3. stets $A(d) \leq \varphi(d)$

1)-3) $\Rightarrow$ $A(d) = \varphi(d)$ *insbesondere* $A(n) = \varphi(n)$, *da* $\varphi(n) > 0$*:* $A(n) > 0$, *d.h. A zyklisch.*
Ist $a \in A(d)$, *dann ist* $a \in E(d) := \{x \in K \mid x^d - 1 = 0\}$
Aber $\#E(d) \leq d$ *(Polynom d-ten Grades hat höchstens d Nullstellen)*
Daher gilt: Ist $A(d) \neq 0$, *dann existiert ein* $a_0 \in A(d)$, *und damit*
$E(d) = \{a_0^\nu \mid 0 \leq \nu < d\}$
Es gilt: a_0^ν *hat Ordnung d* $\Leftrightarrow$ $ggT(\nu, d) = 1$
(Ist $(a_0^\nu)^k = 1$, *so folgt* $d \mid \nu k$, *gilt* $ggT(\nu, d) = 1$, *so gilt:* $d \mid \nu k \Rightarrow d \mid k$*), d.h Ordnung von* $a_0^\nu = d$
Damit $A(d) = \{a_0^\nu \mid 0 \leq \nu < d, \quad (\nu, d) = 1\}$ $\varphi(d)$ *viele* ν*'s.*

Satz 2.2.6 $(\mathbb{Z}/2\mathbb{Z})^* \approx 1$
$(\mathbb{Z}/4\mathbb{Z})^* \approx \mathbb{Z}/2\mathbb{Z}$
$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \underset{\#=2^{\alpha-1}}{\approx} < -1 \underset{\approx \mathbb{Z}/2\mathbb{Z}}{\mod 2^\alpha} > \times < 5 \underset{\mathbb{Z}/2^{\alpha-2}\mathbb{Z}}{\mod 2^\alpha} >$

Beweis 2.6 *Für alle* $\alpha \geq 1 :$ $5^{2^{\alpha-2}} = 1 + n_\alpha 2^\alpha$ *mit ungeradem* n_α
Fixiere α_0. *Sei* $d := ord(5 \mod 2^{\alpha_0})$, *dann gilt wegen*
$5^{2^{\alpha_0-2}} \equiv 1 \mod 2^{\alpha_0}$,
dass $d | 2^{\alpha_0-2}$.
Andererseits gilt auch $5^{2^{\alpha_0-2-1}} = 1 + n_{\alpha_0-1} 2^{\alpha_0-1}$ *mit* n_{α_0-1} *ungerade, daher* $5^{2^{\alpha_0-2-1}} \neq 1 \mod 2^{\alpha_0}$,
und somit $= 2^{\alpha_0-2}$
$(\mathbb{Z}/2^r\mathbb{Z})^* =< \pm 1 > \times < 5 \mod 2^r >$ *für* $r \geq 2$
Es gilt: $\circledast \forall\ \alpha \geq 3$
$5^{2^{\alpha-3}} = 1 + n_\alpha 2^{\alpha-1}$ *(*n_α *ungerade)*
Betrachte: $g :< \pm 1 > \times < 5 \mod 2^r > \xrightarrow{r} (\mathbb{Z}/2^r\mathbb{Z})^*$ *mit* $g(a, b) \to ab$
g injektiv:
Sei $g(a, b) = 1$, *d.h.* $ab = 1$.
Seien $x, y \in \mathbb{Z}$, *so daß* $a = x \mod 2^r$, $\quad b = y \mod 2^r$, *d.h.* $xy \equiv 1 \mod 2^r$
Insbesondere: $xy \equiv 1 \mod 4$.
Da $y \equiv 1 \mod 4$ *folgt* $x \equiv 1 \mod 4$, *d.h.* $a = 1$.
Also $y \equiv 1 \mod 2^r$ *(oder* $b = 1$*)*
g ist Isomorphismus, da Ordnung von $5 \mod 2^r$ *gerade* 2^{r-2} *ist.*
Denn $\circledast$ *mit* $\alpha = r + 1$ *sagt:*
$5^{2^{r-2}} = 1 + n_{r+1} 2^r$

$(5)^{2^{r-2}} \equiv 1 \mod 2^r \quad (5 \mod 2^r)^{2^{r-2}} = 1$
⊛ *mit* $\alpha = r$ *sagt:*
$5^{2^{r-3}} = 1 + n_r 2^{r-1}$ n_r *ungerade*
$(5)^{2^{r-3}} \neq 1 \mod 2^r$, *daher* $(5 \mod 2^r)^{2^{r-3}} \neq 1$
⊛ *mit Induktion:* $\alpha = 3 \qquad 5 = 1 + 1 \cdot 4$
Rest: Übung

Kapitel 3

Endliche Körper

Körper: Ring (kommutativ mit 1), in dem jedes von 0 verschieden Element (multiplikativ) invertierbar ist. z.B.: $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p

Fakten

1. Ist K endlicher Körper, so ist $\#K$ eine Primzahlpotenz.
2. Zu jeder Primzahlpotenz p^α gibt es (bis auf Isomorphie) genau einen Körper mit p^α Elementen.

   Bezeichnung: $\mathbb{F}_{p^\alpha}$, z.B. $\mathbb{F}_p$ für $\mathbb{Z}/p\mathbb{Z}$

(Hinweis zu 2): Zu jedem Körper K existiert ein (bis auf Isomorphie) eindeutiger Körper $\overline{K}$ mit der Eigenschaft:

i) Jedes Element in $\overline{K}$ ist Nullstelle eines Polynoms $\neq 0 \in K[X]$

ii) Ist $L \supseteq \overline{K}$ ein Körper, $\alpha \in L$ Nullstelle eines Polynoms $\neq 0 \in \overline{K}[X]$, dann ist $\alpha \in \overline{K}$

Beispiel
$\overline{\mathbb{R}} = \mathbb{C}, \quad \overline{\mathbb{Q}} \neq \mathbb{C}$
Betrachte: $\overline{\mathbb{F}_p}$.
Nehmen wir an $\mathbb{F}_{p^\alpha} \subseteq \overline{\mathbb{F}_p}$ ist, dann
$x \in \mathbb{F}_{p^\alpha},\ x \neq 0$, so $x^{p^\alpha - 1} = 1$, d.h. $x \in \mathbb{F}_{p^\alpha},\ x^{p^\alpha} = x$
also $\mathbb{F}_{p^\alpha} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^\alpha} = 0\}$
Umgekehrt:
Definieren wir $\mathbb{F}_{p^\alpha} := \{x \in \overline{\mathbb{F}_p} \mid x^{p^\alpha} - x = 0\}$, dann ist das ein Körper.
Tatsächlich: $a, b \in \mathbb{F}_{p^\alpha}$, dann $(a+b)^{p^\alpha} = a+b = \sum_\nu \binom{p^\alpha}{\nu} a^\nu\, b^{p^\alpha - \nu}$, O.K., denn $\binom{p^\alpha}{\nu} = 0$ falls $0 < \nu < p^\alpha$

Explizite Konstruktion von $\mathbb{F}_{p^\alpha}$

1. Wähle ein Polynom f(x) vom Grad α in $\mathbb{F}_p[X] \quad (\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z})$ so daß f irreduzibel ist. (d.h. niemals f=gh mit $g, h \in \mathbb{F}_p[X]$ und Grad von g und h ≥ 1)

   zum Beispiel: $f(x) := x^2 + x + 1 \in \mathbb{F}_p[X]$ ist irreduzibel

2. Setze $\mathbb{F}_{p^\alpha} := \mathbb{F}_p[X]/f \cdot \mathbb{F}_p[X]$

   Beachte: $\mathbb{F}_p[X]$ ist Ring, insbesondere abelsche Gruppe bezüglich +,

   $f\mathbb{F}_p[X] = \{fg \mid g \in \mathbb{F}_p[X]\}$ ist Untergruppe, ist Faktorgruppe

   Definiere eine Multiplikation:

   $(a + f\mathbb{F}_p[X]) \cdot (b + f\mathbb{F}_p[X) = ab + f\mathbb{F}_p[X]$

   (ist wohldefiniert, Beweis analog zu $\mathbb{Z}$ anstelle von $\mathbb{F}_p[X]$)

   Damit jedenfalls $\mathbb{F}_{p^\alpha}$ ist Ring.

   Tatsächlich ist $\mathbb{F}_{p^\alpha} \underbrace{ein\ Körper}_{=:B}\ mit\ \underbrace{p^\alpha - Elemente}_{=:A}$

Zu A:

1. Jede Restklasse $a + f\mathbb{F}_p[X]$ besitzt ein Element vom Grad $\alpha - 1$:

   euklidische Division: $a \neq fq+r \quad q, r \in \mathbb{F}_p[X] \quad deg(r) < deg(f) = \alpha$,

   $a + f\mathbb{F}_p[X] = r + f\mathbb{F}_p[X]$

2. Je zwei verschiedene Polynome vom Grad $\leq \alpha - 1$ liegen in verschiedenen Restklassen

Damit: $\#\mathbb{F}_{p^\alpha} = \#\ Polynome\ in\ \mathbb{F}_p[X]\ vom\ Grad\ \leq \alpha - 1$

Beispiel: $\mathbb{F}_4$

1. Wähle $f = x^2 + x + 1$

2. $\mathbb{F}_4 = \mathbb{F}_2[X]/f\mathbb{F}_2[X]$

   Setze $\gamma := x \mod f = x + f\mathbb{F}_2[X]$.

   Damit $\mathbb{F}_4 = \{0,\ 1,\ \gamma,\ \gamma + 1\}$

   Repräsentanten $0 + f\mathbb{F}_2[X],\ 1 + f\mathbb{F}_2[X],\ x + f\mathbb{F}_2[X],\ x + 1 + f\mathbb{F}_2[X]$

   $\bigoplus$ $\gamma + \gamma + 1 = 1$, etc.

$\odot$	0	1	γ	$\gamma + 1$
0	0	0	0	0
1	0	1	γ	$\gamma + 1$
γ	0	γ	$\gamma + 1$	1
$\gamma + 1$	0	$\gamma + 1$	1	γ

   $\gamma \cdot \gamma = \gamma + 1$, denn $\gamma^2 - \gamma - 1 = 0 \quad x^2 + x + 1 = 0 + f\mathbb{F}_2[X]$
   $\gamma \cdot (\gamma + 1) = 1$

Zu B)
Sei $a + f\mathbb{F}_{p^\alpha}[X] \neq 0$, d.h. $f \nmid a$
Betrachte $I := a\mathbb{F}_p[X] + f\mathbb{F}_p[X]$. I ist Untergruppe von $\mathbb{F}_p[X]$, sogar $\mathbb{F}_p[X] \cdot I = I$
(I ist Ideal), es gilt:
jedes Ideal in $\mathbb{F}_p[X]$ ist von der Gestalt:
$I = c \cdot \mathbb{F}_p[X]$ mit geeignetem $c \in \mathbb{F}_p[X]$ (analog zu $\mathbb{Z}$ mit Grad $\leftrightarrow$ $|.|$)
Es gilt also: $c \mid a, \quad c \mid f$ aber f irreduzibel, daher (bis auf Multiplikation mit Konstanten) gilt: $c = 1$ oder $c = f$
$c = f$ unmöglich, denn $f \nmid a$, also $c = 1$
Also existieren Polynome $u, v \in \mathbb{F}_p[X]$ mit $c = 1 = au + vf$, daher
$(a + f\mathbb{F}_p[X]) \cdot (u + f\mathbb{F}_p[X]) = 1 + f\mathbb{F}_p[X]$

Kapitel 4

Kryptographie

Aufgabe der Kryptographie: Bereitstellung und Untersuchung von Verfahren (Protokollen), die in Spielsituationen
gewährleisten sollen, dass jeder stets genau die für ihn gedachten Informationen erhält und dass Regelverstöße verhindert werden.

4.1 Einführung: Kryptographische Problemstellungen

Beispiel
Münzwerfen am Telefon (Bit-Commitment-Protokoll)

1. A wählt willkürlich einen Namen in einem Telefonbuch und übermittelt die zugehörige Nummer an B:
2. B rät, ob die zweite Ziffer der nächsten Telefonnummer in dem Telefonbuch gerade ist.
3. A übermittelt Namen.
4. A und B überzeugen sich davon, ob B gewonnen hat.

Statt Telefonbuch abstrakt:
$f : N \xrightarrow{\sim} M$ leicht berechenbar
$g : M \to \{0, 1\}$ schwer berechenbar
$h := g \circ f$ leicht berechenbar

(f insbesondere Einwegfunktion, d.h. f leicht, f^{-1} schwer berechenbar)

Beispiel
Merkles Rätsel (rudimentäres Protokoll zum Schlüsselaustausch)

1. A und B vereinbaren ein einfaches symmetrisches Verschlüsselungsverfahren: Entschlüsseln eines Chiffrats (= Finden des Schlüessels) kostet unberufene Entzifferer 2n-mal so viel Zeit, wie Ver- oder Entschlüsseln bei bekanntem Schlüssel.
2. B produziert n zufällige Texte $m_1, \ldots, m_n$ und n zufällige Schlüssel $k_1, \ldots, k_n$ und übermittelt die Schlüsseltexte $E_{k_1}(m_1), \ldots, E_{k_n}(m_n)$ an A (Zeitaufwand n)
3. A wählt zufälliges $i \in \{1, \ldots, n\}$ und findet k_i (Zeitaufwand 2n)
4. A wählt (n-1) zufällige Scheinchiffrate $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n$
5. A setzt $c_i = E_{k_i}(m)$ und übermittelt $c_1, \ldots, c_n$ an B.
6. B berechnet $D_{k_1}(c_1), \ldots, D_{k_n}(c_n)$ (Zeitaufwand n)
7. B hat höchstwahrscheinlich genau einen sinnvollen Text erhalten $m = D_{k_i}(c_i)$

Zeitaufwand für A, B jeweils 2n
unberufener Entzifferer $2n^2 + n$

Beobachtung

1. Protokolle und kryptographische Elemente lassen sich trennen
2. Komplexität von Algorithmen ist entscheidend !

Beispiel
Abstraktes Public Key Protokoll (beschrieben von **Diffie-Hellman** 1976)
kryptographisches Element: $E : P \xrightarrow{\sim} C \quad D : C \to P$
$D \circ E = id_P \quad E \circ D = id_C$

E öffentlich bekannt (public key),
D soll nur einer Person bekannt sein (private key)

- Nachrichtenübermittlung (nur B kennt D)
  - A schickt $E(m)$ an B.
  - B berechnet $m = D(E(m))$
- Signatur von Nachrichten (nur B kennt D)
  - B schickt $D(m)$ an A und ebenfalls m
  - A überprüft $m = E(D(m))$

Erste Realisierung: Rivest, Shamir, Adleman 1978 RSA

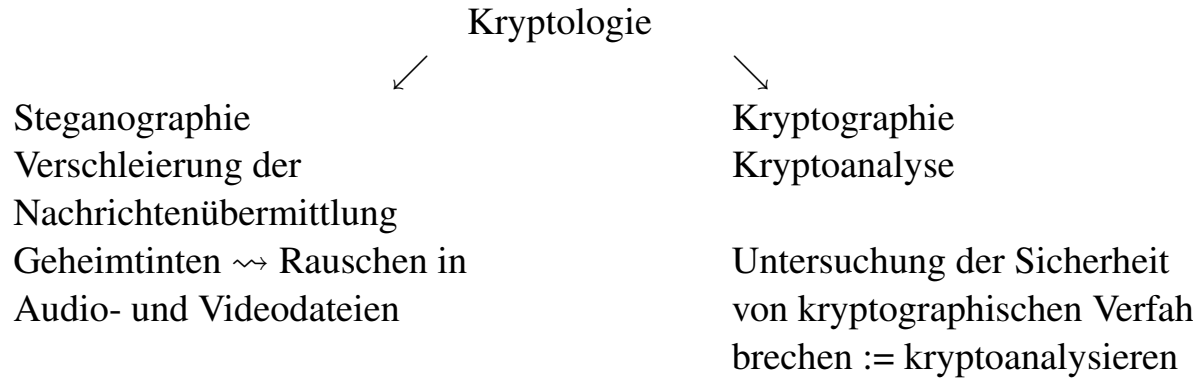
Beispiel
1-2 Oblivious Transfer
A soll entweder die Nachricht m_1 oder die Nachricht m_2 an B übermitteln, aber hinterher nicht wissen, welche von beiden B kennt.
Seien $(E^{(1)}, D^{(1)})$ und $(E^{(2)}, D^{(2)})$ wie im vorigen Beispiel.
Außerdem sei ein klassisches Verschlüsselungssystem $(E_k, D_k),\ k \in K$ (Schlüsselmenge), wobei $E_k,\ D_k$ leicht berechenbar sind, falls k bekannt (alles mit P, C)
A kenne $D^{(1)},\ D^{(2)}$,
B kenne nur $E^{(1)},\ E^{(2)}$.

1. B wählt zufällig $k \in K$ und $E \in \{E^{(1)},\ E^{(2)}\}$ und schickt $E(k)$ an A.
2. A berechnet $c_1 := E_{D^{(1)}(E(k))}(m_1),\ c_2 := E_{D^{(2)}(E(k))}(m_2)$ und schickt diese Werte an B.
3. B berechnet $n_1 := D_k(c_1),\ n_2 := D_k(c_2)$
   Falls $E = E^{(1)} \quad \Rightarrow \quad n_1 = m_1$
   Falls $E = E^{(2)} \quad \Rightarrow \quad n_2 = m_2$

Komplexes Protokoll für gleichzeitige Signatur verwendet (OT).

4.2 Einige klassifizierende Begriffe

- Gliederung:



- Grundprobleme

  α) Geheimhaltung

  β) Identifikation

  γ) Authentifikation

  δ) verbindliche Signatur

  ϵ) Integrität von Daten

- Klassifikation von Angriffen

  α) Ciphertext-only (nur Schlüsseltext vorhanden)

  β) Known-Plaintext (Ein oder mehrere Paare von Klar- und Schlüsseltext bekannt z.B. m̈it freundlichen Grüßen)̈

  γ) Chosen-Plaintext (Klartext/ Schlüsseltext-Paare können erzeugt werden)

  δ) Chosen Cyphertext

- Hilfsmittel

  – Zahlentheorie

- Gruppentheorie
- Kombinatorik
- Komplexitätstheorie
- Informationstheorie / Statistik
- mathematische Logik

4.3 Historischer Abriß

bis 1850	monoalphabetische Substitution
	Transpositionen, Codes, polyalphabetische Substitution mit periodischem Schlüssel (Vigenère)
	Kryptoanalyse: monoalphabetische Substitution mit Buchstabenhäufigkeit
1850 - 1920	Kryptoanalyse: polyalphabetische Substitution (Babbage, Kasiski)
1920 - 1950	One-Time-Pad (Vernam)
	Rotor-Geräte (z.B. Enigma)
	Kryptoanalyse: statistische Parameter, Kappa, Chi (Friedman)
	Bletchley-Park (1940-45)
	Theorie: Informationstheorie (Shannon)
1950 - heute	Moderne Blockschriften (z.B. DES, Rijndalen)
	PKC (1976), Zero-Knowledge (1985) komplexe Protokolle, Elliptische-Kurven-Kryptographie
	Kryptoanalyse: differenzielle und lineare Kryptoanalyse, Computational Number-Theorie, Quantenalgoritmen (Shor)
Zukunft ?	Quantenkryptographie, Quantencomputer

4.4 Kryptographie im Alltag

Internetprotokolle z.B. SSH (Secure Shell), SSL (Secure Socket Layer), IPsec (Virtual Private Network)
Telekommunikationsprotokolle z.B. Handies
benutzen:

- (symmetrische) Blockchiffrieung (z.B. DES, AES)
- Public-Key Verschlüsselung (z.B. RSA, El-Gamal, ECC)
- Hashfunktionen (z.B. MD5, SHA-1)

Kapitel 5

Verschlüsselung

5.1 Public-Key-Verschlüsselung

Ziel: Geheime Kommunikation über einen offenen Kanal
Die Sicherheit der später folgenden Verfahren beruht auf der Härte einiger mathematischer Probleme.

α) diskreter Logarithmus in einer endlichen, zyklischen abelschen Gruppe G:

Finden von $x \in \mathbb{N}$ mit $a^x = b$ für $a, b \in G$ und a primitiv z.B: in $\mathbb{F}_q^*$

β) Faktorisierung großer Zahlen :$n \in \mathbb{N}$ sei Produkt von $p, q \in \mathbb{P}(= Primzahlen)$ groß.

n bekannt, finde p und q

γ) Wurzelziehen in einer endlichen Gruppe: $n \in \mathbb{N}$ sei Produkt von $p, q \in \mathbb{P}$ groß und $a \in \mathbb{Z}_n^*$ sei Quadrat, dann finde $b \in \mathbb{Z}^* : b^2 = a$

δ) Entscheidung über die Frage Q̈uadrat oder Pseudoquadrat ?̈: $n \in \mathbb{N}$ sei Produkt von $p, q \in \mathbb{P}$ groß. Für ein $a \in \mathbb{Z}_n^*$ gelte $\left(\frac{a}{n}\right) = 1$.

Frage: Ist a ein Quadrat in $\mathbb{Z}_n^*$?

ε) K̈nappsackproblem̈: Seien $a_1, \ldots, a_n \in \mathbb{N} \quad \varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n \quad s = \sum_{i=1}^{n} \varepsilon_i \, a_i$.

Gegeben s, finde ε.

5.1.1 Die Verfahren

Diffie-Hellman und El-Gamal

Sei G eine endliche zyklische Gruppe mit

a) Für $\alpha \in G,\ k \in \mathbb{N} \rightsquigarrow \alpha^k$ leicht berechenbar

b) Für $\alpha,\ \beta \in G,\ \alpha$ primitiv $\rightsquigarrow$ diskreter Logarithmus x (d.h. $\alpha^x = \beta$) schwer berechenbar.

5.1.2 Diffie-Hellman Schlüsselaustausch (1976)

1. A wählt $k_a \in \mathbb{N}$, B wählt $k_b \in \mathbb{N}$ (geheim)
2. A und B einigen sich auf ein primitives Element $\alpha \in G$
3. A sendet $a := \alpha^{k_a}$ an B.
   B sendet $b := \alpha^{k_b}$ an A
4. A und B berechnen den Schlüssel
   $K := \alpha^{k_a\ k_b} = b^{k_a} = (\alpha^{k_b})^{k_a} = a^{k_b} = (\alpha^{k_a})^{k_b}$

Bemerkung
Unberufene Entzifferer kennen $\alpha,\ a,\ b$, aber weder k_a noch k_b (da diskreter Logarithmus schwer zu berechnen ist).
Es gibt kein bekanntes Verfahren K zu berechnen.

5.1.3 El-Gamal-Verfahren für $\mathbb{F}_p^*$

(asynchrones Diffie-Hellman)

1. B wählt großes $p \in \mathbb{P}$ und $\alpha \in \mathbb{F}_p^*$ primitiv, $k_b \in \mathbb{N}$
2. B gibt $(p,\ \alpha,\ \underset{=:b}{\alpha^{k_b}})$ bekannt (public key)

3. A wählt ein $k_a \in \mathbb{N}$

4. A schickt das Paar $(c,\ \alpha^{k_a})$ an B, wobei $c := k \cdot m$, $k = b^{k_a}$, $\quad m \in \mathbb{F}_p^*$ die Nachricht ist.

5. B berechnet $k^{-1} \in \mathbb{F}_p^*$ (er kennt $k = a^{k_b}$ und findet k^{-1} mit dem euklidischen Algorithmus) und $m = k^{-1} \cdot c$

Bemerkung

1. nicht ohne weiteres für Signatur brauchbar

2. Vorteil: Gruppe G ersetzbar $\mathbb{F}_{p^n}^*$ oder $G = E(\mathbb{F}_{p^n})$ Punkte einer elliptischen Kurve über $\mathbb{F}_{p^n}$

Beispiel für Diffie-Hellman
$G = \mathbb{F}_p^*,\ p = 101,\ \alpha = 2 \mod 101$
A wählt $k_a = 31, \quad \alpha^{31} = 34 \mod 101$
B wählt $k_b = 78, \quad \alpha^{78} = 21 \mod 101$
B berechnet $34^{78} \equiv 49 \mod 101$
A berechnet $21^{31} \equiv 49 \mod 101$

5.1.4 RSA (Rivest-Shamir-Adleman 1978)

1. B wählt große $p, q \in \mathbb{P}$ (etwa 100 bis 200-stellig) sowie $e \in \mathbb{N}$ mit $ggT(e,\ \varphi(n)) = 1$, wobei $n := p \cdot q \quad (\varphi(n) = (p-1)(q-1) = \#\mathbb{Z}_n^*)$

2. B gibt das Paar (n, e) bekannt (public key)

3. A schickt $c := m^e \in \mathbb{Z}_n^*$, wobei $m \in \mathbb{Z}_n^*$ die Nachricht ist.

4. B berechnet ein $d \in \mathbb{N}$ mit $ed \equiv 1 \mod \varphi(n)$ (euklidischer Algorithmus) und errechnet $m = c^d \in \mathbb{Z}_n^*$ (d ist private key)

Bemerkung

1. **Satz von Euler-Fermat** $m^{\varphi(n)} = 1 \; \forall \; m \in \mathbb{Z}_n^*$
   $de = l \cdot \varphi(n) + 1$ mit $l \in \mathbb{N}$ und $m^{l \cdot \varphi(n)} = 1$
   $\Rightarrow \quad c^d = m^{de} = m^{l \cdot \varphi(n)} \cdot m = m$

2. Unberufene Entzifferer benötigen $\varphi(n)$ um d zu berechnen und das ist gleichwertig zur Kenntnis von p, q.

Beispiel
$p = 101, \; q = 103, \; n = 10403, \; \varphi(n) = 10200 = 2^3 \cdot 3 \cdot 5^2 \cdot 17$
$e = 7219, \; ggT(e, \; \varphi(n)) = 1$
$d = 7579, \; ed \equiv 1 \mod 10200$
$m = 4812 \mod 10403 \in \mathbb{Z}_n^*$
A schickt $c = 4812^{7219} \mod 10403 = 8700 \mod 10403$
B berechnet $m = 8700^{7579} \mod 10403 = 4812$

5.1.5 Merkle-Hellman-Verfahren (Rucksack-Verfahren)

1. B wählt $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ und $M > \alpha_1 + \ldots + \alpha_n$ mit
   $\circledast \quad \alpha_{i+1} > \alpha_1 + \ldots + \alpha_i, \quad i = 1, \ldots, n-1$ und $ggT(\alpha_i, M) = 1$,
   sowie $a \in \mathbb{N}$ mit $ggT(a, M) = 1$

2. B gibt $(M, a_1, \ldots, a_n)$ bekannt (public key), wobei $a_i =$ Rest von $alpha_i \mod M$

3. Sei $m \in \{0, 1\}^n$ eine Nachricht $m = (m_1, \ldots, m_n)$
   A schickt $s := \sum_{i=1}^{n} m_i \, a_i$ an B

4. B berechnet ein $b \in \mathbb{N}$ mit $ab \equiv 1 \mod M$ und berechnet $s' = s \cdot b \mod M$. Er findet die m_i leicht, wegen $s' = \sum_{i=1}^{n} m_i \, \alpha_i$ (da $b \cdot a_i \equiv \alpha_i \mod M$)

Bemerkung

1. Wegen $\circledast$ findet B die m_i, indem er mit dem größten α_i beginnt.

2. System schon seit 20 Jahren geknackt!!!

Beispiel
$(\alpha_1, \ldots, \alpha_5) = (3, 5, 11, 24, 49)$,
$M = 103$ $(prim \quad \Rightarrow \quad ggT(\alpha_i, M) = 1)$
$a = 73 \quad (prim \quad \Rightarrow \quad ggT(a, M) = 1)$
$b = 24 \quad (24 \cdot 73 \equiv 1 \mod 103)$
$m = 01001$
B schickt $(a_1, \ldots, a_5) = (13, 56, 82, 1, 75)$
$s = (56 + 75)\%103 = 28$
A schickt s und B rechnet $s' = (28 \cdot 24)\%103 = 54$
$\alpha_5 \leq 54 \Rightarrow m_5 = 1 \quad s' - \alpha_5 = 5$
$\alpha_4 > 5 \Rightarrow m_4 = 0$
$\alpha_3 > 5 \Rightarrow m_3 = 0$
$\alpha_2 = 5 \Rightarrow m_2 = 1,\ m_1 = 0$

Bemerkung

1. Protokollangriffe:
   (a) „Man in the middle“
   (b) „Replay“
2. Diffie-Hellman / El-Gamal:
   Gruppen:
   (a) $\mathbb{F}_q^*$
   (b) $E(\mathbb{F}_q)$ elliptische oder hyperelliptische Kurve
   (c) $Cl(K)$ Idealklassengruppe eines Zahlkörpers K
3. Beim RSA-Verfahren:
   m kann aus $\mathbb{Z}_n$ statt nur $\mathbb{Z}_n^*$ gewählt werden (Blatt 7)
4. Korrektur zu Merkle-Hellman
   $\alpha_i \in \mathbb{N},\ \pi$ Permutation der n Indizes geheim $i = 1, \ldots, n$
   $\circledast \quad \alpha_{\pi(i+1)} > \alpha_{\pi(1)} + \ldots + \alpha_{\pi(i)}$ (Blatt 7)

5.1.6 Rabin-Verfahren

1. B wählt p,q $p \neq q$ prim, groß, $p \equiv 3 \mod 4,\ q \equiv 3 \mod 4$ er gibt $n = pq$ bekannt

2. Für $m \in \mathbb{Z}_n^*$ schickt A $c = m^2$ an B

3. B berechnet (chinesischer Restsatz) m mittels

   $\ominus \quad m \equiv \pm c^{\frac{p+1}{4}} \mod p,\ m \equiv \pm c^{\frac{q+1}{4}} \mod q$

   (Er bekommt 4 Werte $m_1, \ldots, m_4$ von denen wahrscheinlich nur eine sinnvoll ist)

Beweis zu $\ominus$
$c^{\frac{p+1}{4}} \equiv (m^2)^{\frac{p+1}{4}} \equiv (m^{\frac{p-1}{2}})m \mod p \equiv \pm m$
$(m^{\frac{p-1}{2}})^2 \equiv m^{p-1} \equiv 1 \mod p \Rightarrow m^{\frac{p-1}{2}} \equiv \pm 1 \mod p$
genauso für q

Rechnung von $m_1, \ldots, m_4$
Euklidischer Algorithmus $u, v \in \mathbb{Z} : up + vq = 1$
$m_{1,\ldots,4} = \pm upc^{\frac{q+1}{4}} \pm vqc^{\frac{p+1}{4}} \equiv m \mod p \equiv m \mod q \Rightarrow \equiv m \mod n$

Beispiel
$p = 31,\ q = 43,\ n = 1333,\ m = 17 \mod 1333$
$c \equiv 289 \mod 1333 \equiv 10 \mod p \equiv 31 \mod q$
$c^{\frac{p+1}{4}} = c^8 \equiv 14 \mod p$
$c^{\frac{q+1}{4}} = c^{11} \equiv 17 \mod q$
$-18p + 13q = 1$
$m_{1,2,3,4} \equiv \pm 18 \cdot 31 \cdot 17 \pm 13 \cdot 43 \cdot 14 \mod n \equiv 1316,\ 327,\ 17,\ 1006$

5.1.7 Goldwasser-Micali-Verfahren

Definition 5.1.1 *1. Legendre-Symbol:*

Sei p prim, ungerade, $a \in \mathbb{N},\ ggT(a, p) = 1$

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a\ quadratischer\ Rest \mod p \\ -1 & a\ kein\ quadratischer\ Rest \mod p \end{cases}$$

2. *Jacobi-Symbol:*

   $m \in \mathbb{N}$ ***ungerade,*** $a \in \mathbb{N},\ ggT(a,m) = 1,\ m = p_1 \cdot \ldots \cdot p_r, \quad p_i$ ***prim***

   $$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

Regeln

m, m_1, m_2 ungerade, $a, b \in \mathbb{Z}$ teilerfremd zu m, m_1, m_2

1. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$
2. $\left(\frac{a}{m_1 m_2}\right) = \left(\frac{a}{m_1}\right)\left(\frac{a}{m_2}\right)$
3. $a \equiv b \mod m \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$
4. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$
5. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$
6. $\left(\frac{m_1}{m_2}\right)\left(\frac{m_2}{m_1}\right) = (-1)^{\frac{(m_1-1)(m_2-1)}{4}}$ Gaußsches Reziprozitätsgesetz

$\Rightarrow$ effektiver Algorithmus für Berechnung von $\left(\frac{a}{m}\right)$

Spezialfall

$n = pq$ p,q prim ungerade

$\left(\frac{x}{p}\right) = 1$ für die Hälfte aller $x \in \mathbb{Z}_p^*$ andere Hälfte $\left(\frac{x}{p}\right) = -1$

entsprechend für q

$\Rightarrow$(chinesischer Restsatz) $\left(\frac{a}{n}\right) = 1$ für die Hälfte aller $a \in \mathbb{Z}_n^*$ andere Hälfte $\left(\frac{a}{n}\right) = -1$

davon die Hälfte hat $\left(\frac{a}{p}\right) = 1,\ \left(\frac{a}{q}\right) = 1$, d.h. a quadratischer Rest mod n davon die Hälfte hat $\left(\frac{a}{p}\right) = -1,\ \left(\frac{a}{q}\right) = -1$ nicht quadratischer Rest mod n (Pseudoquadrate)

Goldwasser-Micali

1. b wählt p,q prim, groß $n = pq$ und ein Pseudoquadrat $y \in \mathbb{Z}_n^*$
   (d.h. $\left(\frac{y}{n}\right) = 1$, y Nichtquadrat mod n)
   (n, y) wird bekannt gegeben.
2. Die Nachricht sei $m \in \{0,1\}^l$.
   A wählt zufällige $\alpha_i \in \mathbb{Z}_n^*,\ i = 1, \ldots, l$
   A sendet $c_i := \begin{cases} \alpha_i^2 & falls m_i = 0 \\ y\alpha_i^2 & falls m_i = 1 \end{cases}$ an B
3. B überprüft, ob c_i Quadrat mod n ist ($\Leftrightarrow$ Quadrat mod p $\Leftrightarrow$ $\left(\frac{c_i}{p}\right) = 1$) da $\left(\frac{c_i}{n}\right) = 1 = \left(\frac{c_i}{p}\right)\left(\frac{c_i}{q}\right)$
   falls ja $m_i = 0$, falls nein $m_i = 1$

Beispiel

$m = 01,\ p = 31,\ q = 43,\ n = 1333$

Es gilt: $\left(\frac{6}{31}\right) = -1, \left(\frac{3}{43}\right) = -1$

$-18 \cdot 31 + 13 \cdot 43 = 1$

$-18 \cdot 31 \cdot 3 + 13 \cdot 43 \cdot 6 \equiv 347 \mod n \equiv 6 \mod 31 \equiv 3 \mod 43$

$\Rightarrow \underset{=-1}{\left(\frac{347}{n}\right)} = \underset{=-1}{\left(\frac{347}{31}\right)} = \underset{=-1}{\left(\frac{347}{43}\right)} = -1$

Aber 347 ist kein Quadrat mod n, da kein Quadrat mod p, mod q
$\Rightarrow\ y = 347$ ist Pseudoquadrat
$\alpha_1 = 291 \mod n,\ \alpha_2 = 832 \mod n$
$c_1 = 291^2 \mod n \equiv 702 \mod n$
$c_2 = 832^2 \cdot 347 \mod n \equiv 460 \mod n$
B berechnet: $\left(\frac{702}{31}\right) = 1 \ \Rightarrow\ m_1 = 0$
$\left(\frac{460}{31}\right) = -1 \ \Rightarrow\ m_2 = 1$

5.2 Analyse der Verfahren

Effektiven Algorithmus für Problem

$\alpha \rightsquigarrow$ Diffie-Hellman / El-Gamal unsicher

$\beta \rightsquigarrow$ RSA, Rabin, Goldwasser-Micali unsicher

$\gamma \rightsquigarrow$ Rabin unsicher

$\delta \rightsquigarrow$ Goldwasser-Micali unsicher

$\varepsilon \rightsquigarrow$ Merkle-Hellman

Hier: Sicherheitsbeurteilung unter der Annahme, daß keine effektiven Algorithmen für $\alpha - \varepsilon$ existieren.

Proposition 5.2.1 *Kenntnis von $d \in \mathbb{N}$ (Entschlüsselungsexponent) mit $ed \equiv 1 \mod \varphi(n)$ $\Leftrightarrow$ Faktorisierung von m.*

Angriffe auf RSA bei Nachlässigkeit

- zu kleiner Klartext $\rightsquigarrow$ Durchprobieren
- „Message Consiling“:
  Es gibt stets Klartext $m \in \mathbb{Z}_n$, $c = m^e = m$ (Fixpunkt vgl. Blatt 8)

- „Cycling Attack“:

  Es gibt stets $k \in \mathbb{N}$ mit $c^{(e^k)} = c \Rightarrow c^{e^{k-1}} = m$

  (dafür sorgen, daß k in der Regel groß ist, z.B. $p-1,\ q-1$ enthalten große Primfaktoren)

- Kleines e: Bsp.: $e = 3$

  m sei für 3 verschiedene m_1, m_2, m_3 paarweise teilerfremd verschlüsselt

  $c_1, c_2, c_3\ c_i \equiv m^3 \mod n_i$

  chinesischer Restsatz $\rightsquigarrow \exists\,!\ c \in \{0, \ldots, m_1 m_2 m_3 - 1\},\ c \equiv c_i \mod n_1 n_2 n_3$

  $\Rightarrow\ c \equiv m^3 \mod {}^{n}_{1} n_2 n_3$

  $m < n_i \Rightarrow m^3 < n_1 n_2 n_3 \Rightarrow c = m^3 \Rightarrow m = c^{\frac{1}{3}}$

  (Auch Angriffe mit kleinem d)

- „Common Modulus“

  - benutzt $B_1\ (n, e_1)$ benutzt $B_2\ (n, e_2)$ so kann $B_1\ d_2$ berechnen und $B_2\ d_1$, da Faktorisierung von n bekannt
  - kennt C, $c_1 \equiv m^{e_1} \mod n,\ c_2 \equiv m^{e_2} \mod n \qquad ggT(n, m) = 1$ und $ggT(e_1, e_2) = 1$

    $\rightsquigarrow\ \exists\, u, v \in \mathbb{Z} :\ u\, e_1 + v\, e_2 = 1$

    $\Rightarrow\ m \equiv c_1^u\, c_2^v$

- algebraische Abhängigkeiten

  Bsp.: $e = 3,\ c_1 \equiv m^3 \mod n,\ c_2 \equiv (m+1)^3 \mod n$

  $$\frac{c_2 + 2c_1 - 1}{c_2 - c_1 + 2} \equiv \frac{3m^3 + 3m^2 + 3m}{3m^2 + 3m + 3} = m \mod n$$

Proposition 5.2.2 *(zu RSA)*
Kenntnis von $d \in \mathbb{N}$ mit $ed \equiv 1 \mod \varphi(n)$ ist algorithmisch gleichwertig zur Faktorisierung von $n = pq$

Beweis
Faktorisierung $\rightsquigarrow d$ klar (eukl. Alg.)
$\underline{d \rightsquigarrow p,q}$ $ed-1=2^s u$, u ungerade

Lemma 5.2.3 $\#\{\bar{a} \in \mathbb{Z}_n^* \mid ord_{\mathbb{Z}_p^*}(\bar{a}^u) \neq ord_{\mathbb{Z}_q^*}(\bar{a}^u)\} \geq \frac{(p-1)(q-1}{2}$
Man wähle zufällig $a \in \{2,\ldots,n-2\}$
Falls $ggT(a,n) \neq 1 \quad \Rightarrow$ *Faktorisierung*
Falls $ggT(a,n)=1$*, d.h.* $\bar{a} \in \mathbb{Z}_n^*$*, berechne* $ggT(a^{2^t u},n) t=0,\ldots,s-1$
Falls $ord_{\mathbb{Z}_p^*}(\bar{a}^u) \neq ord_{\mathbb{Z}_q^*}(\bar{a}^u) \quad \Rightarrow \exists\, A=0,\ldots,s-1$
$ggT(a^{2^t u},n)=p,q$

Beweis (Lemma)
Wähle prim. Element $g \in \mathbb{Z}_n^*$
1. Fall: $ord_{\mathbb{Z}_p^*}(g^u) > ord_{\mathbb{Z}_q^*}(g^u)$
Falls $a \equiv g^x \mod p \quad a \equiv g^y \mod q; \quad x=1,3,5,\ldots,p-2,\ y=0,1,\ldots,q-2$
$\Rightarrow\ ord_{\mathbb{Z}_p^*}(\bar{a}^u)=ord_{\mathbb{Z}_q^*}(g^u),\ ord_{\mathbb{Z}_q^*}(\bar{a}^u) \leq ord_{\mathbb{Z}_q^*}(g^u)$
$\Rightarrow ord_{\mathbb{Z}_p^*}(\bar{a}^u) > ord_{\mathbb{Z}_q^*}(\bar{a}^u)$
Chinesischer Restsatz: $\frac{p-1}{2}(q-1)$ Werte für $\bar{a}$
2. Fall: $ord_{\mathbb{Z}_p^*}(g^u) < ord_{\mathbb{Z}_q^*}(g^u) \quad \rightsquigarrow$ genauso
3. Fall: $ord_{\mathbb{Z}_p^*}(g^u) = ord_{\mathbb{Z}_q^*}(g^u)$
Falls $a \equiv g^x \mod p \quad a \equiv g^y \mod q$ mit entweder x gerade, y ungerade oder x ungerade y gerade
$\Rightarrow \quad ord_{\mathbb{Z}_p^*}(\bar{a}^u) \neq ord_{\mathbb{Z}_q^*}(\bar{a}^u)$

Diffie-Hellman / El-Gamal

Vermutung Berechnen von Diffie-Hellman / El-Gamal $\Leftrightarrow$ diskreter Logarithmus

Rabin

Proposition 5.2.4 *Quadratwurzel ziehen in* $\mathbb{Z}_n^*,\ n=pq,\ p,q$ *prim*
$p \equiv 3 \mod 4\ q \equiv 3 \mod 4$
$\Leftrightarrow$ *Faktorisieren von n*

Beweis
Faktorisierung von n
$\rightarrow$ Quadratwurzel
$\leftarrow$ Wähle $m \in \mathbb{Z}_n^*$ beliebig $c := m^2$
Finde Quadratwurzel $m^{'}$ von c
Wahrscheinlichkeit $\frac{1}{2}$ $m^{'} = m$ oder $m^{'} = n - m$ 1. Fall
Wahrscheinlichkeit $\frac{1}{2}$ $m^{'} - m \not\equiv 0$ und $m^{'} + m \not\equiv 0 \mod n$ 2. Fall
Im 2. Fall gilt: $m^2 - m^{'2} = 0 \equiv 0 \mod n$
$\Rightarrow\ n|(m - m^{'})(m + m^{'})$
$\Rightarrow\ 1 < ggT((m - m^{'}), n) < n$
$\Rightarrow$ Rabin genauso schwer wie Faktorisierung von n.

Merkle-Hellman
Gebrochen mit LLL-Algorithmus (Lenstra, Lenstra, Lorasc)
Zum Finden „kurzer“ Vektoren in Gittern

Goldwasser-Micali
Keine Information über den Klartext außer man löst das Problem δ

Kapitel 6

Klassische Verschlüsselungsverfahren

6.0.1 Polyalphabetische Substitution (allg. Vigenère)

Sei $m \in \mathbb{N}^*, \mathbb{Z}_n$ Alphabet.
Seien $\pi_i : \mathbb{Z}_n \to \mathbb{Z}_n, i = 1, \ldots, l$ Permutationen von $\mathbb{Z}_n \quad ((\pi_1, \ldots, \pi_l)$ sind der Schlüssel),
$m \in \mathbb{Z}_n^r, m = (m_1, \ldots, m_r)$ eine Nachricht. m wird verschlüsselt durch $c = (c_1, \ldots, c_r), c \in \mathbb{Z}_n^*$, mit $c_i = \pi_{\tilde{i}}(m_i), \tilde{i} \in \{1, \ldots, l\}, \tilde{i} \equiv i$ mod l (d.h. periodische Verschlüsselung).

Spezialfall:
$n = 26, \mathbb{Z}_n \cong$ Buchstaben A,. . .,Z
Für $\alpha \in \mathbb{Z}_n$ definiert $\pi^{(\alpha)} : \mathbb{Z}_n \to \mathbb{Z}_n, a \to a + \alpha$ eine spezielle Verschiebung
(„shift “) $\hookrightarrow$ Vigenère
Für $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_n^l$, setze $\pi_i = \pi^{\alpha_i}, i = 1, \ldots, l$

Beispiel
Schlüsselwort: „KEY“$\triangleq (10, 4, 24)$
Nachricht: „Hallo“$\triangleq (7, 0, 11, 11, 14)$
$c_1 = m_1 + \alpha_1 = 10 + 7 = 17, c_2 = 4, c_3 = 9, c_4 = 21, c_5 = 18$
$\Rightarrow c = (17, 4, 9, 21, 18) \triangleq$ REJVS

Beispiel
Rotormaschinen (z.B. Enigma)(allg. Vigenère), sehr lange Periode, Per-

mutationen π_i fixpunktfrei und involutiv

Spezialfall:
l=1 (monoalphabetische Substitution) z.B. n=26, nur shifts $\rightarrow$ Cäsarverfahren

Beispiel
Schlüssel: k=10, Nachricht: Hallo =$(10, 0, 11, 11, 14)$
$c = (17, 10, 21, 21, 24)$ =RKVVY

Beispiel(Playfair)
$n = 25^2$ = Paare von Buchtaben$\neq$ J, l=1: Schlüssel: „KEY“$\rightarrow$ Schlüsselmatrix

K	E	Y	A	B
C	D	F	G	H
I	L	M	N	O
P	Q	R	S	T
U	V	W	X	Z

$YI \leftrightarrow KM, HZ \leftrightarrow OB, QS \leftrightarrow RT$

Buchstabenverdopplung durch Einfügen (meist X) vermeiden,
konkret: Hallo $\rightarrow$ Halxlo $\rightarrow$ GBNVMI =c

Spezialfall
r=l One-Time-Pad (Vernam)
Schlüssellänge=Textlänge, absolut sicher gegen Ciphertext-only, falls der Schlüssel eine Zufallsfolge ist! (vgl. 3.3)

Beispiel
Schlüssel: DVMZI = (3,21,12,25,8), Hallo $\rightsquigarrow$ KVXKW

6.0.2 Lineare Blockchiffren

$n \in \mathbb{N}^*, r \in \mathbb{N}^*, A \in GL(r, \mathbb{Z}_n)$,d.h. $A \in Mat(r \times r, \mathbb{Z}_n)$,
$\det A \in \mathbb{Z}_n^* \overset{Cramer}{\Rightarrow} \exists A^{-1} \in GL(r, \mathbb{Z}_n) : AA^{-1} = E$
Nachricht $m \in \mathbb{Z}n^r$ wird durch $\boxed{c = Am} \in \mathbb{Z}_n^*$ verschlüsselt.
(Kombination mit Vigenère: affine Chiffren)

Beispiel

$n = 26, r = 2, A = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}, \det A = -5 \in \mathbb{Z}_{26}^*,$

$(-5) * 5 \equiv 1 \mod 26,$

$A^{-1} = (\det A)^{-1} \cdot \begin{pmatrix} 4 & -3 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 20 & 11 \\ 11 & 5 \end{pmatrix}$

„HALLOX“= (7,0,11,11,14,23)$\hookleftarrow$ (7,21,18,25,5,4) = AVSZFE

Verschlüsselung der ersten beiden Zeichen:$A \cdot \begin{pmatrix} 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 \\ 21 \end{pmatrix},$

Entschlüsselung der letzten beiden Zeichen Chiffre:

$\begin{pmatrix} 20 & 11 \\ 11 & 5 \end{pmatrix} \begin{pmatrix} 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 144 \\ 75 \end{pmatrix} = \begin{pmatrix} 14 \\ 23 \end{pmatrix}$

Spezialfall: Permutationschiffren
Die Matrix A enthält nur 0en und 1en. In jeder Zeile genau eine 1 und in jeder Spalte genau eine 1.

Beispiel

$r = 3, A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, n = 26$

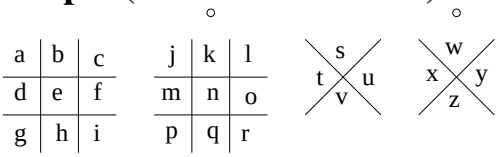
HALLOX$\rightarrow$ ALHOXL, $A^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

6.0.3 Sonstiges

- Homophone: Mehrere mögliche Verschlüsselungen für das gleiche Zeichen
- Spreizen: Klartextzeichen durch Schlüsseltextketten mit verschiedener Länge verschlüsseln
- Blender: Füllzeichen

- Codes, Codebücher, Stichworte: Semantische Verschlüsselung, d.h. keine Zeichen, sondern linguistische Einheiten werden verschlüsselt
- exotische Symbole: Beispiel Freimaurerchiffren

Beispiel(Freimaurerchiffren)



6.1 Kryptoanalyse–Methoden

Bei „**Chiphertext-only**“: statistische Verfahren, Grundlage: Redundanz der Sprache.

- Häufigkeitsanalyse:
  - Buchstaben: enirstaduhl (engl. etaoiskrdlu)
  - Bi- und Trigramme: en, em, de, ei (engl. th, he, as, in)
  - Worte: die, der, und (engl. the, of, and)
  - Muster
- Länge des Vigenère-Schlüssels
- Kasiski-Methode (Blatt 8, A3)
- Index of Coincidence (Friedman)(Blatt 8, A4), Formel von Sinkov (1935)
- Kappa-Verlaufsanalyse: (Kullback): Zahl der Übereinstimmungen zwischen c und dem um n geshifteten Chiffrat $\tilde{c}$ ist groß, falls n

Vielfaches der Blocklänge l ist. (übrigens Mittel aller dieser Werte: Index of Coincidence)

- allg. trickreiche kombinatorische Methoden

„Known-plaintext“häufig einfacher

Beispiel

1. Hill: r linear unabhängige Paare von Klartext/Schlüsseltext

   $(m_i, c_i), i = 1 \ldots, r$

   $A \cdot \underbrace{(m_1\ m_2\ \ m_r)}_{M} = \underbrace{(c_1\ c_2\ \ c_r)}_{C} \Rightarrow A = CM^{-1}$

2. Bekanntes Wort im Klartex für ein Enigma-Chiffrat (fixpunktfrei, involutiv). Nur wenige mögliche Positionen für das Wort.

6.2 Shannon-Theorie

- Entropie: als Informationsmaß H(P)=Unsicherheit über den Klartext

- bedingte Entropie: Unsicherhit über den Klartext bei bekanntem Schlüsseltext

- perfekte Sicherheit: $H(P) = H_C(P)$ erfüllt vom One-Time-Pad, notwendig dafür H(P)$\leq$ H(K), Schlüssel muss mindestens so groß wie der Klartext sein!

  Shannons pessimistische Ungleichung

- Redundanz: $\log_2 26 \approx 4,7$ Bit/Buchstabe Information in Zufallsfolgen von $A, \ldots, Z$

  $\approx 1,2$ Bit/Buchstabe in deutschen Texten

  $\approx 3,5$ Bit/Buchstabe Redundanz

Beispiel
zufällig gewählte Klartexte addieren $\rightsquigarrow$ brauchbares One-Time-Pad

- Unizitätslänge im random-cipher-model: Falls H(C)≥H(P)+H(K)
  $\rightsquigarrow$ findet man Klartext,
  Klartext- und Schlüsseltextlänge: $H(C) = k \cdot \underbrace{4,7Bit/Buchstabe}_{\log_2 26}$,
  $H(P) = k \cdot 1,2Bit/Bst.$,
  $H(K) = \log_2 z, \quad z =$Anzahl der möglichen Schlüssel des Systems
  $k \geq \frac{\log_2 z}{4,7 \cdot 1,2} = \frac{\log_2 z}{3,5}$ Unizitätslänge

Beispiel
monoalphabetische Sustitution $n = 26$
$\Rightarrow z = 26, \quad \frac{\log_2 z}{3,5} \approx 25$

Kapitel 7

Moderne Block- und Stromchiffren

7.1 Blockchiffre

Definition 7.1.1 *Eine Blockchiffre der Länge n ist ein Verschlüsselungsverfahren mit $\mathcal{P} = \mathcal{C} = \Sigma^n$ über dem Alphabet Σ ist.*

Bemerkung
Die Verschlüsselungsfunktion $E_k : \mathcal{P} \to \mathcal{C}$ ist notwendigerweise bijektiv.

7.1.1 DES = Data Encryption Standard

seit 1981: ANSI-Standard

Beschreibung
$\mathcal{P} = \mathcal{C} = \mathbb{F}_2^{64}$ (je 8 Byte)
$K = \{(b_1, \ldots, b_8) \in \mathbb{F}_2^{64} | \sum_{i=1}^{8} b_{8k+1} = 1, k = 0, \ldots, 7\}$ d.h. jedes achte Bit ist ein Prüfbit, also nur 56 Bit Schlüssellänge.

Bemerkung
$|K|$ zu klein für heutige Verhältnisse, man nimmt heute Tripel-DES (3DES)
Wir schreiben Elemente von $\mathbb{F}_2^{64}$ als (L,R), L erste 32 Bit, R letzte 32 Bit.

1. Festlegung der Rundenzahl, Standard r=16

2. Aus Schlüssel $k \in 8k$ eine Folge $k_1, \ldots, k_r$ von Rundenschlüsseln $k_i \in \mathbb{F}_2^{48}$ berechnet, wie folgt:

   - PC1: $\mathbb{F}_2^{64} \to \mathbb{F}_2^{28} \times \mathbb{F}_2^{28}$
   - PC2: $\mathbb{F}_2^{28} \times \mathbb{F}_2^{28} \to \mathbb{F}_2^{48}$

   Details, insbesondere Tabellen im „Handbook of applied Cryptography "ab S. 250, Kapitel 6.

   - $(C_0, D_0) = PC1(k)$
   - $v_i = \begin{cases} 1 & i = 1, 2, 9, 16 \\ 2 & \text{sonst} \end{cases}$
   - rekursiv C_i aus C_{i-1} durch zyklisches Linksshiften um v_i
   - $k_i = PC2(C_i, D_i)\ i = 1, \ldots, r(= 16)$

3. Verschlüsseln einer Nachricht $m \in \mathbb{F}_2^{64}$

   - Anwenden einer festgelegten Funktion $\mathbb{P} : \mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$ (initial permutation) $(L_0, R_0) = \mathbb{P}(m)$
   - Festgelegte Funktionen:
     $E : \mathbb{F}_2^{32} \to \mathbb{F}_2^{48}$ (expanding)
     $P : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$
     $S_i : \mathbb{F}_2^{6} \to \mathbb{F}_2^{6}\ i = 1, \ldots, 8$ (s-Boxen)
     die s-Boxen bilden den Kern von DES,
     jahrelange Arbeit für Konstruktion der s-Boxen
   - Für $k_i \in \mathbb{F}_2^{48}$ hat man die Funktionen $f_{k_i} : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ folgendermaßen: $R \in \mathbb{F}_2^{32}$
     $E(R) + k_i = B_1, \ldots, B_8 \in \mathbb{F}_2^8\ c = c_1, \ldots, c_8$ mit $c_i = s_i(B_i)$
     $f_{k_i}(R) := P(C)$
   - $(L_i, R_i) := (R_{i-1}, L_{i-1} + f_k(R_{i-1}))$
   - $c := \mathbb{P}^{-1}(R_r, L_r)\ (r = 16)$

4. Verschlüsselung mit umgekehrter Rundenschlüsselfolge $k_{16}, \ldots, k_1$

7.1.2 Rijndal AES

AES= Advanced Encryption Standard (NIST-Ausschreibung für DES-Nachfolge)
Gewinner: Rijndael
Beschreibung: $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^{128}$ $(auch\ für\ \mathbb{F}_2^{160}, \mathbb{F}_2^{192}, \mathbb{F}_2^{224}, \mathbb{F}_2^{256})$

- Identifiziere $\mathbb{F}_2^8$ mit $\{f \in \mathbb{F}_2[] \mid \deg f < 8\}$
  $(b_7, \ldots, b_1) \mapsto \sum_{k=0}^{7} b_k x^k$
  $\lambda : \mathbb{F}_2^8 \to \mathbb{F}_2^8$
  $\lambda(f) \equiv (x^4 + x^3 + x^2 + x + 1)f + x^6 + x^5 + x + 1 \mod (x^8 + 1)$

- Identifiziere $\mathbb{F}_2^8$ mit $\mathbb{F}_{256} = \mathbb{F}_2[X] \setminus m$
  $m = x^8 + x^4 + x^3 + x^2 + 1$ (irred.)
  $\sigma : \mathbb{F}_{256} \to \mathbb{F}_{256}$
  $a \mapsto \lambda(a^{-1}) = \lambda(a^{254})$

- $\xi : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4,\ \xi((a_i)_{i=0}^3) := (\sigma(a_{i+1})_{i=0}^3)$

- Identifiziere $\mathbb{F}_{256}^4$ mit $\{g \in \mathbb{F}_{256}[G] \mid \deg g < 4\}$
  $(a_0, \ldots, a_3) \mapsto \sum_{k=0}^{3} a_k G^k$
  $C := (X, 1, !, X + 1) \in \mathbb{F}_{256}^4,\ \mu : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$
  $\mu(g) \equiv C \cdot g \mod (G^4 + 1)$

- Wie oben und $D := (X^3 + X^2 + X, X^3 + 1, X^3 + X^2 + 1, X + 1) \in \mathbb{F}_{256}^4$ $\nu : \mathbb{F}_{2556}^4 \to \mathbb{F}_{256}^4$
  $\nu(g) \equiv D \cdot g \text{mod}(G^4 * 1),\ \nu = \mu^{-1}$
  $\rho : (\mathbb{F}_{256}^4)^4 \to (\mathbb{F}_{256}^4)^4\ \ (\mathbb{F}_{256}^4)^4 = \mathbb{F}_2^{128}$
  $\rho(((a_{i,j})_{i=0}^3)_{j=0}^3) = ((a_{i,j+i})_{i=0}^3)_{j=0}^3$
  als Matrix: Zeile i wird zyklisch um i Stellen nach links geshiftet

- für $s \in \mathbb{F}_2^{128}$ definiere $\tau_s : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$ $\tau_s(x) = x + s$

- Sei $k \in K = \mathbb{F}_2^{128}$ Schlüssel, $k = (w_j)_{j=0}^3,\ w_j \in \mathbb{F}_{256}^4$, wobei rekursiv

  $w_4, w_5, \ldots, w_43 \in \mathbb{F}_{256}^4$ definiert werden durch:

  $$W_j = \begin{cases} w_{j-1} + w_{j-4} & j \equiv 0 \bmod 4 \\ \xi(w_{j-1}) + w_{j-4} + (x^{\frac{j-4}{4}}, 0, 0, 0) & \text{sonst} \end{cases}$$

  $k_l = (w_{4l}, \ldots, w_{4l+3}),\ l = 0, \ldots, 10$

  Verschlüsselung: $E_k : \mathbb{F}_2^{128} \longrightarrow \mathbb{F}_2^{128}$,
  $E_k = \tau_{k_1 0}\rho\sigma\tau_{k_9}\mu\rho\sigma \ldots \tau_{k_1}\mu\rho\sigma\tau_{k_0}$

7.1.3 Verwendung von Blockchiffren

1. ECB: Electronic Code Book

   Klartext $m = m_1, \ldots, m_r,\ m_i \in \Sigma^n$

   (eventuell mit Zeichen auffüllen, um Vielfaches von n zu erhalten)

   Schlüsseltext: $C = c_1, \ldots, c_r,\ c_i \in E_k(m_i)$

   Nachteil: Gleiche Klartextblöcke geben gleiche Schlüsseltextblöcke

2. CBC: Cipher Block Feedback

   $\Sigma = \mathbb{F}_2,\ IV \in \Sigma^n$ fest gewählt, $m = m_1, \ldots, m_r,\ m_i \in \Sigma^n$

   Schlüsseltext: $c = c_1, \ldots, c_r$ mit $c_0 = IV,\ c_i = E_k(m_i + c_{i-1})$

   Entschlüsselung: $m_j = D_k(c_j) + c_{j-1}$

3. CFB Cipher Feedback

4. OFB Output Feedback

Bemerkung
CFB und OFB erlauben Entschlüsseln schon während der Übertragung des Schlüsseltextes

7.2 Kryptoanalyse

- differentielle Kryptoanalyse (Biham, Shamir, 1990) chosen chiphertext-Angriff, sehr allgemein
- lineare Kryptoanalyse (Matsui, 1994) Known Plaintext, spezieller

Beide beruhen auf Korrelationen im Chiffrat. 16 Runden DES und Rijndael sind gut konstruiert gegen diese Angriffe. Nicht viel besser als brute force.

7.3 Stromchiffren

„Klartextstrom“ in Schlüsseltextstrom

Beispiel
ECB, CBC, CFB, OFB angewandt auf Blockchiffre

7.3.1 LSFR

Lineare Feedback Shift Register= Lineares Schieberegister mit Rückkopplung
$a_1, \ldots, a_n \in \mathbb{F}_2$ fest gewählt, $k = (k_1, \ldots, k_n) \in \mathbb{F}_2^n$ Schlüssel
$$z_i = \begin{cases} k_i & i = 1, \ldots, n \\ \sum_{j=1}^{n} a_j z_{i-j} & \text{sonst} \end{cases}$$
wird durch Schieberegister realisiert;
Klartextstrom: $(m_1, m_2, \ldots)$
Schlüsseltextstrom: $(c_1, c_2, \ldots)$ $c_i = m_i + z_i$

Bemerkung
Algorithmische Eigenschaften von $p = 1 + a_i x + \ldots + a_m x^m$ liefern Eigenschaften von LFSR.

Bemerkung
Allgemeine Riemannsche Vermutung:

$=>$ $\forall n \in \mathbb{N}^*$ ungerade, nicht prim $\exists$ ein Zeuge a gegen die Primalität von n mit $1 < a \leq 2 \log n$ mit Primzahlbeweis in $O(\log^5 n)$ Bit-Operatoen.

Kapitel 8

Analytische Zahlentheorie

Viel präzisere Aussagen über die Verteilung von Primzahlen. Hauptmethode:
$\zeta -$ und $L-$Funktion
$\rightarrow$ Riemannsche $\zeta-$Funktion

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (Realteil\ von\ s > 1)$$

$\rightarrow$ Dirichletsche L-Reihen

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\chi(\bar{n})}{n^s} \quad (Re(s) > 1)$$

wobei $\tilde{\chi} : \mathbb{Z}_n^* \rightarrow S^1$ und

$$\chi(\bar{n}) := \begin{cases} \tilde{\chi}(\bar{n}) & falls\ \bar{n} \in \mathbb{Z}_n^* \\ 0 & sonst \end{cases}$$

$\zeta(s),\ L(s, \chi)$ sind meromorph fortsetzbar für $s \in \mathbb{C}$
Untersuchung der Nullstellen von ζ bzw L mit $0 \leq Re(s) \leq 1$ (kritischer Streifen)
$\rightsquigarrow$ Aussagen über die Primzahlzerlegung $\pi(x) := \#\{p \in \mathbb{P} | p \leq x\}$

Satz 8.0.1 (Primzahlsatz:(von de la Vallee-Poussin und Hadamard 1896))

$$\frac{\pi(x)}{\left(\frac{x}{\log x}\right)} \to 1(x \to \infty)$$

Satz 8.0.2 (Dirichletsche Primzahlsatz:(1837)) $n \in \mathbb{N}^*,\ a \in \mathbb{Z}_n^*$ *dann*
$\pi_{a,n}(x) := \#\{p \in \mathbb{P} \mid p \equiv a\ in\ \mathbb{Z}_n^*\} = \infty$
Es gilt sogar: $\dfrac{\pi_{a,n}(x)}{\left(\frac{x}{\log(x)}\right)} \to \varphi(n)(x \to \infty)$

wesentlich genauere Aussagen sind bewiesen worden

Allgemeine Riemannsche Vermutung:
$\zeta(s)$ und $L(s, X)$ haben eine Nullstelle mit $0 < Re(s) \leq 1$ ARV
$\rightsquigarrow$„optimale“ Resultate über $\pi(X), \pi_{a,n}(X)$

8.1 Probedivision, Sieb des Erathostenes

Proposition
$n \in \mathbb{N}^*$ nicht prim
$\Rightarrow \exists\ p$ prim $p \mid n$ und $p \leq \sqrt{n}$

Beweis
q prim $q \mid n$
falls $q \leq \sqrt{n}$ ✓
falls $q > \sqrt{n},\ n' := \dfrac{n}{q}$
$\Rightarrow\ n' < \sqrt{n}$
$\Rightarrow\ \exists\ p$ prim $p \mid n'$
$\Rightarrow p < \sqrt{n},\ p \mid n$ □

$\rightsquigarrow$**Möglicher Primzahltest:**
$n \in \mathbb{N}^*$, teste $p \mid n\ \forall\ p \in P,\ p \leq \sqrt{n}$

Problem:
etwa $\sqrt{n}\log(\sqrt{n})$ solche p für $n \approx 10^{100}$ zu viele!
außerdem alle $p \leq \sqrt{n}$ müssen erst berechnet werden.

Bemerkung
Alternative Betrachtungsweisen als „Sieb“ des Erathostenes

8.2 Fermat Test

p prim, $a \in \mathbb{Z}_p^* \Rightarrow a^{p-1} \equiv 1 \mod p$ nach dem Satz von Fermat.
$\rightsquigarrow$ **Fermat Test:**
$n \in \mathbb{N}^*$, wähle zufälliges $a \in \mathbb{Z}_n^*$ falls $a^{n-1} \neq \bar{1} \mod n \Rightarrow n$ nicht prim. Falls n nicht prim ist, aber $a^{n-1} = \bar{1} \mod n$, so heißt n Pseudoprimzahl zur Basis a.

Beispiel
$2^{208} \equiv 36 \mod 209 \Rightarrow 209$ nicht prim.

Problem
Es gibt n , die pseudoprim sind für viele $a \in \mathbb{Z}_n^*$

Beispiel
$n = 341 = 11 \cdot 31$ pseudoprim zu 99 Basen a , z.B. $\bar{2}, \bar{4}, \bar{8}, \bar{15}$

Definition 8.2.1 *1. $n \in \mathbb{N}^*$ nicht prim, mit n ist Pseudoprimzahl für alle Basen $a \in \mathbb{Z}_n^*$ heißt Carmichaelzahl*

2. $\psi : \mathbb{N}^* \to \mathbb{N}^*$
$n \mapsto \min\{m \in \mathbb{N}^* \mid a^m = \bar{1} \; \forall \, a \in \mathbb{Z}_n^*\}$ heißt Carmichaelfunktion.
Insbesondere gilt $\psi(n) \mid \varphi(n)$

Blatt 4 Aufg. 4 + 2) b) $n \in \mathbb{N}^*$ ungerade , $n = \prod_{i=1}^{r} p_i^{e_i}$
$\psi(n) = kgV\{\underbrace{(p_1 - 1)p_1^{e_1 - 1}}_{\#\mathbb{Z}^*_{p_1^{e_1}}}, \ldots, (p_r - 1)(p_r)^{e_r - 1}\}$

Folgerung
$n \in \mathbb{N}^*$ nicht prim. n Carmichaelzahl $\Leftrightarrow \ \psi(n) \mid n-1$ (da $a^{\psi(n)} = \bar{1} \ \forall \ a \in \mathbb{Z}_n^*$)

Folgerung
$n \in \mathbb{N}^*$ ungerade und nicht prim
n Carmichaelzahl $\Leftrightarrow$ n quadratfrei und $p-1 \mid n-1 \ \forall \ p \mid n$

Folgerung
$n \in \mathbb{N}^*$ ungerade und nicht prim. n Carmichaelzahl
$\Rightarrow$ mindestens 3 Primfaktoren.
($n = pq, \ q < p \ : q(p-1) = n - q < n - 1 < n + p - q - 1 = (q+1)(p-1)$)

Bemerkung
Es gibt unendliche viele Carmichaelzahlen ($\sim X^{\frac{2}{7}} < X$) (Alford, Granville, Pomerance 1993)

Beispiel
$561 = 3 \cdot 11 \cdot 17, \ 1105 = 5 \cdot 13 \cdot 17, \ 1729 = 7 \cdot 13 \cdot 19$ (Carmichael 1910)

8.3 Miller Rabin Test

Satz 8.3.1 $n \in \mathbb{N}^*$ *ungerade* $n - 1 = 2^s \cdot d$, *d ungerade. Dann gilt:*

1. *n prim,* $a \in \mathbb{Z}_n^*$
   $\Rightarrow \ a^d = \bar{1} \circledast$
   oder $\exists \ r = 0, 1, \ldots, s-1 \ : \ a^{2^r d} = -\bar{1} \ \circledast\circledast$

2. *n nicht prim*
   $\Rightarrow \#\{a \in \mathbb{Z}_n^* \mid \ \circledast \ oder \ \circledast \ \circledast\} \leq \dfrac{n-1}{4}$

Ein $a \in \mathbb{Z}_n^*$ *heißt Zeuge für die Primalität von n, Nichtprimalität von n*

Das führt zum Miller Rabin Test $n \in \mathbb{N}^*$,
Wähle ein zufälliges $a \in \mathbb{Z}_n^*$
Prüfe $\circledast und \circledast \circledast$, falls nicht erfüllt
$\Rightarrow$ n nicht prim

Beispiel
$n = 561,\ s = 4,\ d = 35\ (560 = 2^4 \cdot 35)$
$\bar{2}^{35} \equiv 2\bar{6}3,\ \bar{2}^{2\cdot 35} \equiv 1\bar{6}6,\ \bar{2}^{4\cdot 35} \equiv 6\bar{7},\ \bar{2}^{8\cdot 35} \equiv \bar{1}$
$\Rightarrow\ \bar{2}$ ist Zeuge für n nicht prim.
$\Rightarrow$ n ist zusammengesetzt.

Beweis

1. $n = p$ prim
   $\Rightarrow\ \mathbb{Z}_p^*$ zyklisch von Ordnung $p-1$
   $a \in \mathbb{Z}_p^*$
   $\Rightarrow\ a^{p-1} = \bar{1}$
   Sei m Ordnung von a^d
   $\Rightarrow\ m^{2^l}\ (d \mid p-1)$
   Falls $l = 0\ \Rightarrow\ a^d = \bar{1}$ ✓ $\circledast$
   Falls $l > 0\ \Rightarrow\ (a^{2^{l-1}d})^2 = a^{2^l d} = \bar{1}$
   $\Rightarrow\ a^{2^{l-1}d} = -\bar{1}$, da $a^{2^{l-1}d} \neq \bar{1}$

2. Sei $k := \max\{r = 0, \ldots, s-1 \mid \exists\, a \in \mathbb{Z}_n^*\ :\ a^{2^r d} = -\bar{1}\}$
   (Falls $a^{2^r d} \neq -1\ \forall a, r$
   $\Rightarrow\ a^d \neq \bar{1}\ \forall a, r$ da $(-a)^d = -a^d$
   $\Rightarrow$ keine Nichtzeugen)
   Sei $= \prod_{i=1}^{n} p_i^{e_i},\ m := 2^k d \quad (m \mid n-1)$
   $J := \{a \in \mathbb{Z}_n^* \mid a^{n-1} = \bar{1}\}$
   $K := \{a \in \mathbb{Z}_n^* \mid \varphi_{p_i^{e_i}}(a^m) = \pm\bar{1}\ \forall\ p_i\}$

$\varphi_{p_i^{e_i}} : \mathbb{Z}_n^* \to \mathbb{Z}_{p_i^{e_i}}^*$

$L := \{a \in \mathbb{Z}_n^* \mid a^m = \pm\bar{1}\}$

$M := \{a \in \mathbb{Z}_n^* \mid a^m = \bar{1}\}$

Per Definition (und chinesischer Restsat): $M \subset L \subset K \subset J \subset \mathbb{Z}_n^*$ Kette von Untergruppen

genügt zu zeigen: $\#(\mathbb{Z}_n^*/L) \geq 4 \ominus$ (da Nichtzeugen ?? von L sein müssen)

$a \in K \underset{chinRestsatz}{\Rightarrow} a^2 \in M$

$\Rightarrow \#(K/M) = 2^{j'}$

$\Rightarrow \#(K/L) = 2^j \quad (j \leq j')$

(da $\#(K/M) = \#(K/L) \cdot \#(L/M)$)

1. Fall: $j \geq 2$ ✓

2. Fall: j=1 $\exists\, a \in K : a^m = -1$

$\Rightarrow \varphi_{p_i^{e_i}}(a^m) = -1$

$\forall a \in K$

$\Rightarrow a^{2m} = \bar{1}$

$\Rightarrow \varphi_{p_1^{e_1}}((a^m)^2) = \bar{1}$

$\Rightarrow$ Hälfte der Elemente $\tilde{a} \in \mathbb{Z}_{p_1^{e_1}}^*$ hat $\tilde{a}^m = \bar{1}$

Hälfte der Elemente $\tilde{a} \in \mathbb{Z}_{p_1^{e_1}}^*$ hat $\tilde{a}^m = -\bar{1}$

j=1 $\underset{chin.\ Restsatz}{\Rightarrow}$ n hat 2 Primfaktoren

$\underset{Folg\ 3\ aus\ 5.2}{\Rightarrow}$ n keine Carmichaelzahl

$\Rightarrow \#(\mathbb{Z}_n^*/J) \geq 2$

$\Rightarrow \ominus$

j=0 $\underset{wie\ oben}{\Rightarrow} n = p^l$ Primzahlpotenz, $\mathbb{Z}_n^*$ zyklisch

von $Ord(p-1)p^{e-1}$

$\Rightarrow (p-1)$ Elemente $a \in \mathbb{Z}_n^*$ mit $a^{n-a} = \bar{1}$

(da $ggT(p^{e-1}, n-1) = 1$ und $(p-1)(n-1) = p^l - 1$

$\Rightarrow \ \#J = p-1$

$\Rightarrow \ \#(\mathbb{Z}_n^+/J) = p^{l-1} \geq 4$

außer für $n = 9$ (leicht zu überprüfen)

Kapitel 9

Primfaktorzerlegung

Aufgabe: $n \in \mathbb{N}$, finde Primfaktorzerlegung.

9.1 Probedivision

Nachprüfen in welcher Ordnung kleine Primzahlen p in n aufgehen, sehr schnell untauglich.

9.2 Pollard's (p-1)-Methode

Beobachtung

(a) Gelte $p \mid n$ und $p-1 \mid k$; mit Fermat
$\Rightarrow p \mid (a^k - 1) \forall\, a \in \mathbb{N}, \quad ggT(a,p) = 1$
$\Rightarrow p \mid ggT(a^k - 1, n)$, d.h. falls $n \nmid (a^k - 1)$
$\Rightarrow ggT(a^k - 1, n)$ ist echter Teiler von n.

(b) Falls $p-1$ nur Primzahlpotenzen $q^e < B$ enthält,
so ist $k := \prod_{q,e: q^e \leq B} q^e \quad (\Rightarrow p-1 \mid k)$

($p-1$)-Methode

(a) für $n \in \mathbb{N}$, wähle man $B \in \mathbb{N}$, $\quad k := \prod_{q,e:q^e \leq B} q^e$

(b) Berechne $ggT(a^k - 1, n)$ für verschiedene $a \in \mathbb{N}$

(c) Falls so kein echter Teiler von n gefunden wird, wähle größeres B

Beispiel

$n = 36719, B = 10, k = 8 \cdot 9 \cdot 5 \cdot 7 = 2520, a = 2$
$2^{2520} \equiv 33216(n),\ ggT(33215, n) = 73\ \ 36719 : 73 = 503$

$\Rightarrow 36719 = 73 \cdot 503$ ist Primfaktorzerlegung.(503,73 beide prim)

Bemerkung

Die $(p-1)$-Methode ist nur geeignet für n, das einen Primfaktor p enthält, derart dass $(p-1)$ nur kleinere Primfaktoren enthält.

9.3 Pollards ρ-Methode

Beobachtung

(a) Geburtstagsparadoxon: k zufällige Elemente aus $\{0, 1, \ldots, m-1\}$, diese sind paarweise verschieden mit $P = \prod_{i=1}^{k-1}(1 - \frac{i}{m})$

$\Rightarrow p \approx e^{-\frac{k^2}{2m}}$ für $k \gg 0$
$\Rightarrow$ für $k \approx \sqrt{2 \log 2} \cdot \sqrt{m}$ gilt $p \approx \frac{1}{2}$

(b) $f : \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$ Funktion
$x_0 \in \{0, 1, \ldots, m-1\}, x_{i+1} = f(x_i), i \geq 0$
$\Rightarrow \exists i_0, j_0 \in \mathbb{N}, j_0 \geq 1$ mit

i. $x_0, x_1, \ldots, x_{i_0+j_0-1}$ paarweise verschieden

ii. $x_i = x_{i+j_0}\ \forall\ i \geq i_0$ $\quad i_0$ ist Vorperiodenlänge, j_0 Periodenlänge

Sei $k_0 = l \cdot j_0$ das kleinste Vielfache von j_0 mit $k_0 \geq i_0$
$\Rightarrow x_{k_0} = x_{2k_0}$ $(x_{2k_0} = x_{k_0+l \cdot j_0})$

ρ -Methode

(a) Sei $n \in \mathbb{N}$. Wähle ganzzahliges Polynom $f(z)$, üblicherweise $x^2 + a, a \in \mathbb{Z}^*$

(b) Wähle zufälligen Startwert $x_0 \in \mathbb{N}_0$ und $y_0 = x_0$

(c) $x_{i+1} = f(x_i)$ mod n, $y_{i+1} = f(f(y_i))$ mod n $(\Rightarrow y_i = x_{2i})$

(d) Prüfe, ob $1 < d_i = ggT(x_i - y_i, n) < n$, falls ja d Teiler von n. (Obige Zahl m ist hier die Zahl der Restklassen mod d_i, also d_i)

(e) falls erfolglos, neues x_0

Beispiel

$n = 1387, f(x) = x^2 - 1, x_0 = y_0 = 2$
$x_1 = 3,\ y_1 = x_2 = 8,\ ggT((x_1 - y_1), n) = ggT(5, 1387) = 1$
$x_2 = 8,\ y_2 = x_4 = 1194 \mod n,\ ggT(x_2 - y_2, n) = 1$
$x_3 = 63,\ y_3 = x_6 = (1194^2 - 1)^2 - 1 \equiv 177$ mod n,
$ggT(63 - 177, 1387) = 19(\leftarrow$ prim), $1387 : 19 = 73(\leftarrow$ prim)

Bemerkung

Die ρ-Methode funktioniert nur gut, falls n einen relativ kleinen Teiler d hat.

9.4 Quadratisches Sieb QS (Pomerance 1982)

Beobachtung

(a) $n \in \mathbb{N},\ 0 \leq x, y < n,\ x \not\equiv \pm y \mod n,\ x^2 \equiv y^2 \mod n$
$\Rightarrow (x - y)(x + y) = l \cdot n$
$\Rightarrow ggT(x \pm y, n)$ echte Teiler von n

(b) Hat man mehrere Kongruenzen
$(A_i = \prod p_k^{e_k}) \equiv (B_i = \prod p_j^{e_j})$ mod n mit kleinen Primzahlen $p_k,\ p_j$, so kann man versuchen einige von ihnen zu multiplizieren, um auf beiden Seiten verschiedene Quadrate zu haben.

Beispiel

Hat man gefunden, dass $2^4 \cdot 5 \equiv 3$ mod 77 und $2^6 \cdot 5 \equiv 243 = 3^5 \mod 77$

$\Rightarrow (\underbrace{2^5 \cdot 5}_{260})^2 \equiv (\underbrace{3^3}_{27})^2 \mod 77$

$\Rightarrow 260 \equiv 27 \mod 77,\ ggT(260 \pm 27, 77) = 7$ bzw. 11

QS, systematische Erzeugung solcher Kongruenzen

Quadratisches Sieb, vereinfachte Variante

(a) $n \in \mathbb{N},\ m = \lfloor \sqrt{n} \rfloor,\ f(x) = (x+m)^2 - n.$
Wähle $P > 0,\ B := \{2\} \cup \{p \in \mathbb{P} \mid p < P,\ (\frac{n}{p}) = 1\} = \{p_1, \ldots, p_l\}$
sowie $c > 0$ und $S := \{-c, -(c-1), \ldots, 0, 1, \ldots, c\}$
(In der Praxis $c,\ P \sim e^{\sqrt{\log n \log\log n}},\ P < 2c < P^2$)

(b) Für alle $s \in S$ zerlege $f(s) = (s+m)^2 - n = (-1)^{\varepsilon_0(s)} \cdot \prod_{i=1}^{l} p_i^{e_i(s)} \cdot t$
$\varepsilon_0 \in \{0, 1\}$

(c) $\forall s \in S$ mit $t = 1$ betrachte den Vektor $(\varepsilon_0(s), \varepsilon_1(s), \ldots, \varepsilon_l(s)) \in \mathbb{Z}_2^{l+1}$
$\varepsilon_i(s) = \overline{\varepsilon_i(s)}$ in $\mathbb{Z}_2$

(d) Finde einige solcher $s_1, \ldots, s_w$ mit
$\sum_{j=1}^{w} \varepsilon(s_j) = 0 \in \mathbb{Z}_2^{l+1}$ (Gauß-Verfahren über $\mathbb{K} = \mathbb{F}_2$)

(e) Berechne $ggT\left(\left(\prod_{j=1}^{w}(s_j+m)-\prod_{i=1}^{l}p_i^{f_i}\right),n\right)$ ist Kandidat für Teiler von n.

Beispiel

$n=2041, m=45, P=5, c=2, B=\{2,3,5\}$

$$\begin{array}{lllll} f(-2)= & 43^2-2041= & -192= & -2^6\cdot 3 & \rightsquigarrow \quad (1,0,1,0) \\ f(-1)= & 44^2-2041= & -105= & -3\cdot 5\cdot 7 & \rightsquigarrow \quad t=7\neq 1 \\ f(0)= & 45^2-2041= & -16= & -2^4 & \rightsquigarrow \quad (1,0,0,0) \\ f(1)= & 46^2-2041= & 75= & 3\cdot 5^2 & \rightsquigarrow \quad (0,0,1,0) \\ f(2)= & 47^2-2041= & 168= & 2^3\cdot 3\cdot 7 & \rightsquigarrow \quad t=7\neq 1 \end{array}$$

$(1,0,1,0)+(0,0,1,0)+(1,0,0,0)=(0,0,0,0)$

$ggT(43{\cdot}45{\cdot}46{+}2^5{\cdot}3{\cdot}5,n)=157\,(43{\cdot}45{\cdot}46)^2\equiv(-1)^2{\cdot}2^1 0{\cdot}3^2{\cdot}5^2=(2^5\cdot 3\cdot 5)^2)$

$ggT(43\cdot 45\cdot 46-2^5\cdot 3\cdot 5,n)=13\;2041=13\cdot 157$

Bemerkung

$\forall\, p\ \exists$ höchstens 2 Restklassen α_1,α_2 mod p mit $p\mid(\alpha+m)^2-n$, alle anderen Restklassen werden ausgesiebt.

9.5 Laufzeiten

$L_n[u,v]:=e^{v\cdot(\log n)^u\cdot(\log\log n)^{1-u}}\ , u,v\leq 0$

$L_n[0,v]=(\log n)^v \triangleq$ polynomiale Laufzeit

$L_n[1,v]=e^{v\log n}\triangleq$ exponentielle Laufzeit

Unter heuristischen Annahmen $\rightsquigarrow$ QS hat Laufzeit $L_n[\frac{1}{2},c], c>1$

Variante mit quadratischen Formen $\overset{streng}{\rightsquigarrow}$ Laufzeit $L_n[\frac{1}{2},c]$

Elliptische Kurven-Faktorisierung $\rightsquigarrow$ gleiche Laufzeit, aber besser, falls „kleiner“ Teiler existiert.

Zahlkörpersieb $\rightsquigarrow$ Laufzeit $L_n[\frac{1}{3}, (\frac{64}{9})^{\frac{1}{3}}] \leftarrow$ beste Methode (Pollard 1988)

9.6 Primzahl-Erzeugung-Test-Beweis-Zertifikat

Primzahltest: Test auf Zusammengesetztheit

Primzahlerzeugung: Algorithmus zur Erzeugung (wahrscheinlicher) Primzahlen

(a) wähle zufälliges n

(b) Probedivision durch viele kleine p

(c) k-mal Miller-Rabin

(d) falls bestanden, Wahrscheinlichkeit für n prim $> 1 - (\frac{1}{4})^k$

(e) falls nicht neues n probieren

Varianten:

a) Algorithmus zur Erzeugung sicherer Primzahlen („cycling attack “)

b) Erzeugung beweisbarer Primzahlen (Maurer)

Primzahlbeweis: $n \in \mathbb{N}$ vorgegeben, Entscheidungsalgorithmus, ob n prim

- APR, Adleman, Pomerance, Rumely in $O((\log n)^{c \cdot \log\log\log n})$
- ECPP „Elliptic curve primality proving “, Erwartungswert $O(\log^6 n)$

Primzahlzertifikat: (Pratt), Nachprüfbarer Beweis für die Primalität n in $O(\log^2 n)$ überprüfbar. (um den Beweis zu konstruieren, benötigt man die Zerlegung von (n-1))

Kapitel 10

Diskreter Logarithmus

Problem

G zyklische Gruppe, $n = |G|$ bekannt, $\gamma \in G$ Erzeuger, $\alpha \in G$.

Finde $z \in \mathbb{N} : \gamma^z = \alpha$

Bemerkung

Hängt von der Darstellung von G ab.

Diskreter Logarithmus in $(\mathbb{Z}_n, +)$ leicht! (Euklidischer Algorithmus)

Diskrete Logarithmen in G ist gleichwertig zu Bijektion $G \to (\mathbb{Z}_n, +)$ explizit berechnen zu können.

Schon $G = \mathbb{Z}_p^*$ ist schwer (d.h. explizite Bijektion $\mathbb{Z}_p^* \to (\mathbb{Z}_{p-1}, +)$)

10.1 Enumeration

Berechne γ^z für alle $z = 0, 1, 2, 3, \ldots, p-1$

Vergleiche mit α. Laufzeit O(n) $\rightsquigarrow$ schlecht!

10.2 Shanks Baby-Step-Giant-Step-Algorithmus

$m := [\sqrt{n}]$. Berechne und speichere (Aufwand $\sim \sqrt{n}$)

$R := \{((\gamma^m)^q, q) \mid q = 0, 1, \ldots, [\frac{n}{m}\} \leftarrow$ Giant steps

$B := \{(\alpha\gamma^{-r}, r) \mid r = 0, 1, \ldots, m-1\} \leftarrow$ Baby steps

Suche nach $q \in \{0, 1, 2, \ldots, [\frac{n}{m}]\}, r \in \{0, 1, \ldots, m-1\}$ mit

$(\gamma^m)^q = \alpha\gamma^{-r}$

$\Rightarrow \gamma^{qm+r} = \alpha$

$\Rightarrow \ z = qm + r$ ist Lösung.

Beispiel

$2^z \equiv 6 \mod 19$ (2 Erzeuger von $\mathbb{Z}_{19}$)

$m = [\sqrt{n}] = 4, 2^m \equiv 16 \mod 19$,

$2^{-1} \equiv 10 \mod 19$

$R := \{(16^0, 0), (16^1, 1), (16^2, 2), (16^3, 3), (16^4, 4)\}$
$= \{(1, 0), (16, 1), (9, 2), \underline{(11, 3)}, (5, 4)\}$

$B := \{(6 \cdot 10^0, 0), (6 \cdot 10^1, 1, (6 \cdot 10^2, 2), (6 \cdot 16^3, 3)\}$
$= \{(6, 0), (3, 1), \underline{(11, 2)}, (15, 3)\}$

Wähle also $q = 3, r = 2$

$\Rightarrow z = 3 \cdot 4 + 2 = 14, \ 2^{14} \equiv 6(19)$

10.3 Pollards ρ-Methode

Idee: Ähnlich wie beim Faktorisieren definiert man rekursiv die Folge

$x_i, \ x_{i+1} = f(x_i)$, wobei die $x_i = (\gamma^{u_i}\alpha^{v_i}, u_i, v_i)$ Tripel sind.

Falls $x_i^{(1)} = x_j^{(1)}$

$\Rightarrow \gamma^{u_i}\alpha^{v_i} = \gamma^{u_j}\alpha^{v_j}$

$\Rightarrow \gamma^{u_i-u_j} = \alpha^{v_j-v_i} = \gamma^{z(v_j-v_i)}$

$\Rightarrow u_i - u_j \equiv z(v_j - v_i) \mod n$ (da $\gamma^n = e$ und $\gamma^m = e \Rightarrow n \mid m$)

Berechne die möglichen Werte für z (eukl. Algorithmus).

Oft nur wenige mögliche $\rightarrow$ ausprobieren.

Falls viele Werte $\rightsquigarrow$ neuer Startwert x_0.

Konkret:

benutzt Funktion f, die gut durchmischt

$\rightsquigarrow$ Geburtstagsparadoxon ist gutes Modell

$\rightsquigarrow\sim \sqrt{n}$ Schritte bis Erfolg $\rightsquigarrow$ Laufzeit O($\sqrt{n}$)

Konstuktion:

$G_1,\ G_2,\ G_3 \subset G$ disjunkte Teilmengen, nicht notwendig Gruppen,

$G_1 \cup G_2 \cup G_3 = G,\ u_0 \in \{0, 1, \ldots, n-1\}$ zufällig.

$v_0 = 0,\ x_0 = (\gamma^{u_0}, u_0, 0),\ \beta_i := \gamma^{u_i}\alpha^{v_i},\ x_{i+1} = f(x_i)$ definiert durch

$$u_{i+1} = \begin{cases} u_i + 1 & , \beta_i \in G_1 \\ 2u_i & , \beta_i \in G_2 \\ u_i & , \beta_i \in G_3 \end{cases}$$

$$v_{i+1} = \begin{cases} v_i & , \beta_i \in G_1 \\ 2v_i & , \beta_i \in G_2 \\ v_i + 1 & , \beta_i \in G_3 \end{cases}$$

$$\Rightarrow \beta_i = \begin{cases} \gamma\beta_i & , \beta_i \in G_1 \\ \beta_i^2 & , \beta_i \in G_2 \\ \beta_i\alpha & , \beta_i \in G_3 \end{cases}$$

Durchführung:

Wie beim Faktorisieren, berechne parallel x_i und $y_i := x_{2i}$ und überprüfe:

$x_i^{(1)} = y_i^{(1)}, i > 0$

Alternative:

Für $j = 0, 1, 2, 3, \ldots$ berechne man und speichere x_{2^j} für $i = 2^j + 1, \ldots, 2^{j+1}$ berechne x_i und prüfe, ob $x_i^{(1)} = x_{2^j}^{(1)}$

Beispiel

$3^z \equiv 8 \mod 1697$, (3 Erzeugendes von $\mathbb{Z}_{1697}^*$)

$G_1 := \{x \in \mathbb{Z}_{1697}^* \mid x \equiv 1 \mod 3\}$

$G_2 := \{x \in \mathbb{Z}_{1697}^* \mid x \equiv 2 \mod 3\}$

$G_3 := \{x \in \mathbb{Z}_{1697}^* \mid x \equiv 3 \mod 3\}$,

$u_0 = 123,\ \gamma = 3,\ \alpha = 8$

i	$x_i^{(1)}$	$y_i^{(1)}$	u_i	v_i	u_{2i}	v_{2i}
0	1504	1504	123	0	123	0
1	1118	459	124	0	124	1
2	459	759	124	1	249	2
3	253	429	248	2	996	8
4	759	1457	249	2	592	32
5	789	1028	498	4	593	33
6	425	1306	996	8	593	35
7	765	798	296	16	594	36
8	1457	765	592	32	680	144
9	1474	1474	592	33	1360	289

$u_i - u_{2i} \equiv 2(v_{2i} - v_i) \mod 1697$,

$n = |\mathbb{Z}_{1697}^*| = 1696, \quad ggT(289 - 33, 1696) = 32$

$z' \frac{289-33}{32} \equiv \frac{592-1360}{32} \mod \frac{1696}{32} = 53$

$\Rightarrow z' \equiv 50 \mod 53$

$\Rightarrow z = l \cdot 53 + 50 \rightarrow$ ausprobieren liefert $z = 1110$

10.4 Pohlig-Hellmann-Algorithmus

Sei die Primfaktorzerlegung von $n = \prod p_i^{e_i}$ bekannt (sehr optimistisch!)

(a) **Reduktion auf Primzahlpotenzordnung**

Sei $z \equiv z_i \bmod p_i, z_i \in \{0, 1, \ldots, p_i - 1\}$

Definiere $\gamma_i = \gamma^{\frac{n}{p_i^{e_i}}}, \alpha_i = \alpha^{\frac{n}{p_i^{e_i}}}, \gamma^z = \alpha$

$\Rightarrow \gamma_i^z = \alpha_i^z$

$\Rightarrow \gamma_i^{z_i} = \alpha_i$ (da $\gamma_i^{ep_i^{e_i}} = e$)

$G_i := \{g^{\frac{n}{p_i^{e_i}}} | g \in G\} => G_i$ ist zyklisch von Ordnung $p_i^{e_i}$ und γ_i Erzeugendes von G_i, $\alpha_i \in G_i$, d.h. z_i ist Lösung des diskreten Logarithmusproblems für Basis α_i in der Gruppe G_i.

(b) **Reduktion auf Primzahlordnung**

Sei $z_i = z_i^{(0)} + z_i^{(1)} \cdot p_i + \ldots + z_i^{(e_i+1)} p_i^{e_i-1}, p_i-$ adische Darstellung.

Mit $z_i^{(j)} \in \{0, 1, \ldots, p_i - 1\}$.

$\gamma_i^{z_i} = \alpha_i$

$\Rightarrow (\underbrace{\gamma_i^{p_i^{e_i-1}}}_{\gamma_i^{(0)}})^{z_i} = \underbrace{\alpha^{p_i^{e_i-1}}}_{\alpha_i^{(0)}}$

$\Rightarrow \boxed{\gamma_i^{(0)^{z_i^{(0)}}} = \alpha_i^{(0)}}$, da $(\gamma_i^{(0)})^{lp_i^{e_i}} = e$ ist.

d.h. $z_i^{(0)}$ ist Lösung des diskreten Logarithmusproblems zur Basis $\gamma_i^{(0)}$ von $\alpha_i^{(0)}$ in $G_i^{(0)} := \{g^{p_i^{e_i}} | g \in G_i\}$.

G_i ist zyklisch von Ordnung $p_i, \gamma_i^{(0)}$ ist Erzeuger.

Sei $z_i' = z_i^{(1)} + z_i^{(2)} p_i + \ldots + z_i^{(e_i-1)} p_i^{e_i-2} \equiv \frac{z_i - z_i^{(0)}}{p_i}$

$\Rightarrow (\underbrace{\gamma^{p_i}}_{\gamma_i'})^{z_i'} = \alpha\gamma^{-z_i^{(0)}} =: \alpha_i'$

d.h. z_i' ist Lösung des dikreten Logarithmusproblems zur Basis γ_i' von α_i' in $G_i' = \{g^{p_i} | g \in G_i\}$, G_i ist zyklisch von der Ordnung $p_i^{e_i-1}$

$\rightsquigarrow$ iterativ fortfahren und $z_i^{(1)}, \ldots, z_i^{(e_i-1)}$ bestimmen.

Beispiel

$3^z \equiv 8 \mod 1697, n = \#\mathbb{Z}_{1697}^* = 1696$

$n = 53 \cdot 2^5,\ p_1 = 2,\ e_1 = 5,\ p_2 = 53,\ p_2 = 1$

$\gamma_1 \equiv 3^{53} \equiv 69 \mod 1697$

$\alpha_1 \equiv 8^{53} \equiv 1328 \mod 1697$

Löse $69^{z_1} \equiv 1328 \mod 1697$

$z_1 = z_1^{(0)} + z_1^{(1)} \cdot 2 + z_1^{(2)} \cdot 4 + \ldots + z_1^{(4)} \cdot 16$

$\gamma_1^{(0)} = \gamma_1^{16} = 1,\ \alpha_1^{(0)} = \alpha_1^{16} = 1$

$\Rightarrow z_1^{(0)} = 0$

$\Rightarrow 69^{2z_1^{(1)}+\ldots+16z_1^{(4)}} \equiv 1328 \quad |^8$

$\Rightarrow (69^{16})^{z_1^{(1)}} \equiv 1328^8$

$\Rightarrow (-1)^{z_1^{(1)}} \equiv -1$

$\Rightarrow z_1^{(1)} = 1$

$\Rightarrow 69^{z_1^{(2)}\cdot 4+\ldots+16z_1^{(4)}} \equiv 1328 \cdot 69^{-2} \quad |^4$

$(69^{16})^{z_1^{(2)}} \equiv (1405)^4$

$\Rightarrow z_1^{(2)} = 1$

$\rightsquigarrow z_1^{(3)} = 0,\ z_1^{(4)} = 1$

$\Rightarrow z_1 = 22$

$\Rightarrow z \equiv 22(32),\ z = 50(53)$

BabyStepGiantStep liefert $z_2 \equiv 50(53) \overset{chin.Restsatz}{\Rightarrow} z = 1110$

3. **Laufzeit:**
   $o\left(\sum e_i(logn + \sqrt{p_i} + log^2 n)\right)$
   $|G| = n = \prod p_i^{e_i}$ (falls Baby-Step-Giant-Step bzw. ρ-Methode für zyklisches G verwendet wird), d.h. Laufzeit dominiert durch $\sqrt{p_i}$ mit p_i größter Primfaktor von n.

10.5 Index Calculus

G zyklische Gruppe, γ Erzeuger, $\alpha \in G$, gesucht $z : \gamma^z = \alpha$

(a) **Idee:**
Sei $B = \{b_1, b_2, ..., b_r\} \subset G$;
B heißt Faktorbasis.
$b \in G$ heißt B-Element, falls $\exists\ x_1, x_2, ..., x_r \mid b = b_1^{x_1} * b_2^{x_2} * ... * b_r^{x_r}$.

(a) **Schritt:**
Bestimme diskreten Logarithmus: l_i von b_i zur Basis γ, d.h. $\gamma^{l_i} = b_i$
Dazu: Wähle zufälliges $k \in \{0, 1, ..., n-1\}$.
Prüfe, ob γ^k ein B-Element ist, falls ja bestimme $k_1, k_2, ..., k_r$ mit
$\gamma^k = b_1^{k_1} * b_2^{k_2} * ... * b_r^{k_r} = \gamma^{(k_r l_1 + k_2 l_2 + ... + k_r l_r)}$
$\Rightarrow k \equiv k_1 l_1 + ... + k_r l_r$ mod n.
Sammle so viele solcher Kongruenzen, daß sich die l_i bestimmen lassen.

(b) **Schritt:**
Wähle zufällige $x \in \{0, 1, ..., n-1\}$.
Prüfe, ob $\alpha\gamma^x$ B-Element ist; falls ja bestimme $x_1, x_2, ..., x_r$:
$\alpha\gamma_1^x = b_1^{x_1} * b_2^{x_2} * ... * b_r^{x_r} = \gamma^{(x_1 l_1 + ... + x_r l_r)}$
$\alpha = \gamma^z; \gamma^z = \gamma^{(x_1 l_1 + x_2 l_2 + ... + x_r l_r)}$

$\Rightarrow z \equiv x_1 l_1 + ... + x_r l_r - x$ mod n

Damit das Verfahren funktioniert, muß sich leicht überprüfen lassen, ob ein $b \in G$ B-Element ist und die x_i müssen leicht berechenbar sein.

Anwendung

i) $G = \mathbb{Z}_p^*$, p ist Primzahl; $T < p$; $B := \{\tilde{p} \in \mathbb{P} : \tilde{p} \leq T\}$

ii) $G = \mathbb{F}_{p^m}^*$, p ist Primzahl; $r \leq m;\ B := \{f \in \mathbb{F}_p[x] : firr.;\ degf \leq r\}$

Beispiel

$G = \mathbb{Z}_{1697}^*$;

$3^z \equiv 8 \mod 1697$;

$T := 7;\ B := 2, 3, 5, 7$

$3^1 \equiv 2^0 * 3^1 * 5^0 * 7^0 \mod 1697$

$3^{12} \equiv 2^3 * 3^0 * 5^1 * 7^1 \mod 1697$

$3^{235} \equiv 2^1 * 3^1 * 5^1 * 7^0 \mod 1697$

$3^{879} \equiv 2^1 * 3^0 * 5^0 * 7^3 \mod 1697$

$1 \equiv l_2\ mod 1697$

$12 \equiv 3l_1 + l_3 + l_4 \mod 1697$

$235 \equiv l_1 + 2l_2 + l_3 \mod 1697$

$879 \equiv l_1 + 3l_4 \mod 1697$

$12 \equiv 3l_1 + l_3 + l_4 \mod 1697$

$233 \equiv l_1 + l_3 \mod 1697$

$879 \equiv l_1 + 3l_4 \mod 1697$

$1009 \equiv -2l_3 + l_4 \mod 1697$

$646 \equiv -l_3 + 3l_4 \mod 1697$

$283 \equiv 5l_4 \mod 1697$

$\Rightarrow$ (Euklidischer Algorithmus)$l_4 \equiv 735 \mod 1696$ (d.h. $3^{735} \equiv 7 \mod 1696$)

$\Rightarrow l_1 \equiv 370 \mod 1696$ und $l_3 \equiv 1559 \mod 1696$

$8 * 3^{38} \equiv 5^4 \mod 1697$

$\Rightarrow z \equiv 4 * 1559 - 38 \equiv 1110 \mod 1696$

Laufzeit

$l_p[\frac{1}{2}$,c] ($l_n[u, v] = exp(v * (log$ n$)^4 *$ (log log n$)^{1-u}$)

Variante mit Zahlenkörpersieb $l_p[\frac{1}{3}, (\frac{64}{9})^{\frac{1}{3}}]$.

Kapitel 11

Integrität

11.1 Hashfunktionen

Definition 11.1.1 *Σ Alphabet, Σ^* ist die Menge aller Zeichenketten über Σ (bel. Länge)*

1.) $n, m \in N^*$; eine Funktion: $h : \Sigma^* \to \Sigma^n$ heißt Kompressionfunktion.

2.) $n \in N^*$; eine Funktion: $h : \Sigma^* \to \Sigma^n$ heißt Hashfunktion.

3.) Sei h Kompression- bzw. Hashfunktion, $D = \Sigma^m$ bzw. $D = \Sigma^*$ ist der Definitionsbereich.

a) h heißt schwach kollisionsresistent, falls zu gegebenem $x \in D$ praktisch kein $x' \in D$ mit $h(x) = h(x')$ gefunden werden kann.

b) h heißt stark kollisionsresistent, falls praktisch kein Paar $(x, x') \in D^2$ gefunden werden kann mit $h(x) = h(x')$.

Kompressions- bzw. Hashfunktionen sollen effektiv berechenbar sein.

schwach kollisionsresistent $\Rightarrow$ Einwegfunktion.

Anwendung

1.) Passwortdateien; 2.) Dateiintegrität

Dafür reicht schwach kollisionsressistent.

Es gibt Protokolle, die starke kollisionsresitent erfordern.

4. **Geburtstagsparadoxon**

   Unter $\approx \sqrt{|\Sigma^n|} = |\Sigma|^{\frac{2}{n}}$ Werten in D findet man mit Wahrscheinlichkeit $> \frac{1}{2}$ eine Kollision $\rightarrow |\Sigma|^{\frac{n}{2}}$ groß genug!

   Praxis:

   $\Sigma = \{0,1\};\ n \geq 128$

11.2 Merkles-Meta-Verfahren

Sei $g : \{0,1\}^m \rightarrow \{0,1\}^n$ Kompressionsfunktion.

Wir definieren

$h : \{0,1\}^* \rightarrow \{0,1\}^n$.

Der Einfachheithalber $r := m - n > 1;\ x \in \{0,1\}^*$

5. **1. Schritt:** Definiere $\tilde{x} = x_1 * x_2 * ... * x_t$;

   $x_i \in \{0,1\}^r,\ 1 \leq i \leq t$ folgendermaßen:

   i) Vor x so viele Nullen, daß Gesamtlänge teilbar durch r

   ii) Hänge r Nullen an

   iii) Nehme die Binärentwicklung der Orginallänge von x:

      a) Hänge soviele Nullen an, daß die Länge durch $(r-1)$ teilbar ist

      b) Fülle durch 1-en auf an der 1, (r+1),(2r+1),... -Stelle, so daß die Länge durch r teilbar ist.

   iv) Hänge den String aus iii) hinten an.

Beispiel

$x = 111010111,$ Länge $= (1001)_2$; Sei r=4

i) 000111010111

ii) 00011101011110000

iii) a) $1001 \rightarrow 100100$

b) $\rightarrow 11001100$

iv) 0001 1101 0111 0000 1100 1100

Bemerkung

Jedes Wort, daß aus der Länge von x entstanden ist, fängt mit 1 an.

6. **2. Schritt:** $H_0 := 0$ "$\in \{0,1\}$";
$H_i := g(H_{i-1} \circ x_i\}$; i=1,2,...,t; $h(x) := H_t$

Proposition 11.2.1 *Falls g kollisionsressistent ist*
$\Rightarrow$ *h ist kollisionsresisstent.*

Beweis

Buchmann Kapitel 10.4

11.3 MACs (Message Authentication Codes)

Definition 11.3.1 *Sei k eine Menge von Schlüsseln und für jedes* $k \in K$ *eine Hashfunktion:* $h_k : \Sigma^* \rightarrow \Sigma^n$.
Die Familie $\{h_k\}_{k \in K}$ *heißt MAC.*

Anwendung

A und B vereinbaren ein geheimes $k \in K$.

A schickt Nachricht m zusammen mit dem Hashwert $h_k(m)$ an B.

B überprüft den Hashwert $\rightarrow$ Nachricht kommt von A.

11.4 Konkrete Hashfunktion

a) Kompressionsfunktion aus Verschlüsselungsfunktion

Sei $e_k : \{0,1\}^n \rightarrow \{0,1\}^n;\ k \in K = \{0,1\}^n$ Verschlüsselungsfunktion, z.B. Rijandal etc. (vgl. Kapitel 4) $\rightarrow$ Kompressionsfunktion

$h : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ durch z.B.:

i) $h(k,x) := e_k(x) \bigoplus x$

ii) $h(k,x) := e_k(x) \bigoplus x \bigoplus k$

iii) $h(k,x) := e_k(x \bigoplus k) \bigoplus x$

iv) $h(k,x) := e_k(x \bigoplus k) \bigoplus x \bigoplus k$

b) Praktische Hashfunktionen

MD4 (wurde vor ein paar Jahren geknackt),

MD5 (gilt als Wackelkandidat), SHA-1, RIMPD-128, RIMPD-160

Kapitel 12

Signaturen

Problem

B soll überprüfen können, ob eine Nachricht tatsächlich von A kommt.

Lösung

„Elektronische Unterschrift“ mit Public-Key-Verfahren,

d.h. A hat privaten Schlüssel zur Erzeugung der Signatur,

B hat öffentlichen Schlüssel zur Verifikation (Überprüfung).

7. **Vorteil** gegenüber MACs: Nur öffentliche Schlüssel zur Verifikation.

12.1 RSA-Signatur

Allgemeines Prinzip:

$E_e : \mathcal{P} \to \mathcal{C}$ Verschlüsselungsfunktion, e öffentlicher Schlüssel

$D_d : \mathcal{C} \to \mathcal{P}$ Dechiffrierfunktion, d ist ein privater Schlüssel

$D_d \circ E_e = id_{\mathcal{P}}, \quad E_e \circ D_d = id_e$

Sei $\mathcal{P} = \mathcal{C}$

A hat Paar (e,d),

B hat e,

A will m signieren, er schickt (m,s) an B.

B verifiziert die Signatur.

Signatur

einer Nachricht $m \in \mathcal{P}$ ist $s := D_d(m)$

Verifikation

überprüfen, ob $m = E_e(s)$

12.1.1 Realisierung mit RSA

8. **Schlüsselerzeugung** p,q Primzahlen und groß;

   $n = p \cdot q$; $e \in \mathbb{N}$ mit

   $ggt(e, \varphi(n)) = 1 \quad (\varphi(n) = (p-1) \cdot (q-1));\ d \in \mathbb{N} : ed \equiv 1 \mod \varphi(n)$

   A weiß d privater Schlüssel

   B weiß (n,e) öffentlicher Schlüssel

   Beispiel

   $p = 37,\ q = 41,\ n = 1517,\ \varphi(n) = 1440;\ \mathcal{P} = \mathcal{C} = \mathbb{Z}_n;$
   $e = 997,\ d = 13$ (es gibt $13 \cdot 977 \equiv 1 \mod 1440$); $m = \overline{273}$

   A schickt das Paar (m,s) an B mit

   $s = D_d(m) = m^d = \overline{273}^{13} = \overline{14} \mod 1517$

   B verifiziert m=$E_e(s) = s^e = \overline{14}^{997} = \overline{273} \mod 1517$
   $\Rightarrow$ Nachricht kommt von A.

9. **Mögliche Angriffe**

(a) **Existenzielle Fälschung** C wählt irgend ein $s \in \mathbb{Z}_n$ er setzt $m = s^e$

($\rightsquigarrow$ kann ein gültiges Nachrichten-Signatur-Paar erzeugen)

(b) **Multiplikativität** Seien $(m_1, s_1),\ (m_2, s_2)$ 2 gültige Nachrichten-Signatur-Paare (für gleiche Schlüsselpaare)

$\Rightarrow$ $(m_1 \cdot m_2, s_1 \cdot s_2)$ ist ebenfalls ein gültiges Paar.

Lösung

Hashfunktion; Wähle öffentliche bekannte kollisionsresistente Hasfunktion

$h : \mathcal{P} \to \mathbb{Z}_n$

Signatur $s = h(m)^e$

Verifikation überprüfe $h(m) = s^d$

Weiterer Vorteil: beliebig lange Klartexte

Bemerkung

Man kann auch Redundanz von Texten vorschreiben, z.B. alle Buchstaben doppelt:

„HHAALLLLOO“ statt „HALLO“

12.1.2 El-Gamal-Signatur

$G = \mathbb{Z}_p^*$, p ist Primzahl, $\gamma \in G$ Erzeuger; Hashfunktion

$h : \mathcal{P} \to \{1, \ldots, p-2\}$ $\quad a \in \{1, \ldots, p-1\}$ $\quad A := \gamma^a$

öffentlich: (p,γ,a,h)

$privat \quad : a$
nur A bekannt

Signatur

A schickt Nachricht $m \in \mathcal{P}$ zusammen mit einem Paar (r,s) wobei

$r = \gamma^k \ mod\ p$ mit zufälligem $k \in \{1, \ldots, p-1\}$ mit

$ggt(k, p-1) = 1 \qquad s := k^{-1}((h(m) - ar)\ mod\ (p-1))$

wobei $k^{-1} \cdot k \equiv 1\ mod\ (p-1)$

Verifikation

i) $1 \leq r \leq p-1$

ii) B überprüft $a^r \cdot r^s \equiv \gamma^{h(m)}\ mod\ p$

10. **Begründung**

$$A^r \cdot r^s = \gamma^{a \cdot r} \cdot \underbrace{\gamma^{k \cdot s}}_{\gamma^{(h(m)-ar)\ mod\ (p-1))}} \equiv \gamma^{a \cdot r \cdot h(m)-ar}\ mod\ p \equiv \gamma^{h(m)}\ mod\ p$$

Beispiel

$p = 271,\ \gamma = \overline{6} \in \mathbb{Z}_{271}^*$ ist Erzeuger;

$p - 1 = 270 = 2 \cdot 3^3 \cdot 5$

($\rightsquigarrow$ schlecht gewählt wegen Pohlig-Hellmann etc.) $a = 20$;

$A = \overline{6}^{20} = \overline{259} \mod 271\ h(m) = 101$

Signatur

A wählt k=13 (teilerfremd zu 270)

$r = \gamma^k = \overline{271}\ mod\ p$

$k^{-1}(h(m) - ar) \equiv 167\ mod\ 270$

$r = 234; \quad s = 167 \rightsquigarrow$ B

Verifikation

i) $1 \leq r \leq p - 1 = 270$

ii) $A^r \cdot r^s = 259^{234} \cdot 234^{167} \equiv 218\ mod\ 271$
$\gamma^{h(m)} = 6^{101} \equiv 218\ mod\ 271$
$\rightsquigarrow$ Nachricht kommt von A.

Praxis p ≈ 300 Dezimalstellen ($3 \cdot 10^{10^2}$)

Nachteil gegenüber RSA längere Signatur, (viel) weniger effektiv

Vorteil Geht auch mit anderen zyklischen Gruppen (z.B. elliptischen Kurven über endlichen Körpern)

Angriffsmöglichkeiten

(a) Bei unsicherer Hashfunkltion h, z.B. $\mathcal{P} = \{1, \ldots, p-2\},\ h = id$ (also ohne Hashfunktion)
existenzielle Fälschung: C kann ein gültiges Tripel (m,r,s) produzieren.
C setzt $r := \gamma^u \cdot A^v \mod p$;
dann gilt
$A^r \cdot r^s = \gamma^{a \cdot r} \cdot \gamma^{u \cdot s} \cdot \gamma^{a \cdot v \cdot s}$
(wählt $s :\equiv -r \cdot r^{-1} \mod (p-1)$ dazu $ggt(v, p-1) = 1$)
$\Rightarrow \quad v \cdot s \equiv -r$
$\Rightarrow \quad A^r \cdot r^s \equiv \gamma^{u \cdot s} \mod p$,
C setzt $m \equiv u \cdot s \ \rightsquigarrow \ (m, r, s)$ ist ein gültiges Tripel.

(b) Falls zweimal das gleiche k verwendet wird:
$s_1 \equiv k^{-1}(h(m_1) - ar) \mod p$
$s_2 \equiv k^{-1}(h(m_2) - ar) \mod p;\ (r = \gamma^k)$.
Falls C die Tripel $(m_1, r, s_1)\ und\ (m_2, r, s_2)$ abhört,
so kennt er
$s_1 - s_2 \equiv k^{-1}(h(m_1) - h(m_2))\ mod\ (p-1)$,
falls $ggt(h(m_1) - h(m_2), p-1) = 1$ ($\rightsquigarrow$ oder kleiner)
$\rightsquigarrow$ k kann berechnet werden.
$\rightsquigarrow\ a \equiv r^{-1}(h(m_1) - k \cdots_1)$
$\rightsquigarrow$ **C kennt privaten Schlüssel a!!!**

Bemerkung
Die Bedingung $1 \leq r \leq p-1$ ist **wichtig!!!**
C habe gültiges Tripel (m, r, s) abgehört. Er will Nachricht $\tilde{m}$ signieren.
Dazu sucht er mit dem chin. Restsatz $\tilde{r} \equiv \alpha \cdot r\ mod\ p$, wobei
$\alpha := \gamma^{s^{-1}(h(\tilde{m}) - h(m))}$ mit $s^{-1} \cdot s \equiv 1\ mod\ p$

(Vorausetzung dafür $\underbrace{(h(m) - ar)}_{invertierbar}\ mod\ (p-1)$
$s = k^{-1}(h(m) - ar))$ $\tilde{s} := s$
$\rightsquigarrow$ $(\tilde{m}, \tilde{r}, \tilde{s})$ gültiges Tripel (aber $1 \leq r \leq p-1$ nicht erfüllt)
$A^{\tilde{r}} \cdot \tilde{r}^{\tilde{s}} \equiv A^r \cdot (\alpha \cdot r)^s\ mod\ p \equiv \underbrace{A^r \cdot r^s}_{\gamma^{h(m)}} \cdot (\gamma^{s^{-1}(h(\tilde{m}) - h(m))})^s\ mod\ p$
$\equiv \gamma^{h(m)} \cdot \gamma^{h(\tilde{m}) - h(m)}\ mod\ p \equiv \gamma^{h(\tilde{m})}\ mod\ p$
Alternative: Buchmann Kapitel 11.4.6

Bemerkung
In der Praxis wird eine Variante verwendet:
DSA: Digital-Signature- Algorithm $\rightsquigarrow$ effektiver

Kapitel 13

Identifikation

Beispiel

- Einloggen am Rechner
- Homebanking

Mögliche Verfahren:

- Paßwörter (gespeichert werden die Hashwerte)
- Einmalpaßwörter *PIN / TAN*, falls die Übertragung abhörbar ist
- **Challenge-Response Verfahren:**

  1. – A identifiziert sich bei B, indem B eine Zufallszahl r wählt und A diese *signiert*
     – B überprüft die Signatur
       * symmetrisch, z.B. MAC
       * Public-Key Verfahren
  2. **Zero-Knowledge Verfahren:**
     – spezielle Identifikations Protokolle

Bemerkung
In der Praxis verwendet man **TTP** ("Trusted Third Party"), um die Zuordnung Identität $\longrightarrow$ Schlüssel zu zertifizieren.

13.1 Zero-Knowledge Verfahren

Bei einem Zero-Knowledge Protokoll überzeugt ein *Prover* A einen *Verifier* B davon, daß er ein bestimmtes Geheimnis kennt, ohne daß B *irgendeine* Information über das Geheimnis hinzugewinnt.
Beweisbar in folgendem Sinn:
Zero-KnowledgeEigenschaft:
Ein Protokoll hat die Zero-Knowledge Eigenschaft, falls eine Protokollmitschrift gefälscht werden kann (d.h. ohne Kenntnis des Geheimnisses), die sich nicht von einer echten Protokollmitschrift unterscheiden läßt.

Beispiel(Fiat Shamir (1985))

- Schlüsselerzeugung: p, q prim, $n = pq$, $s \in \mathbb{Z}_n^*$ zufällig, $v = s^2$
- öffentlich: (n, v)
- A's privater Schlüssel: s
- Protokoll:

  1. A wählt $x \in \mathbb{Z}_n^*$ zufällig und schickt $y = x^2$ an B
  2. B wirft Münze (d.h. wählt zufällig $e \in \{0, 1\}$) und schickt e an A

  1. Fall: e=0

  3. A schickt dann x an B
  4. B verifiziert $y = x^2$

  2. Fall: e=1

  3. A schickt $u = sx$ an B
  4. B prüft $u^2 = vy$

  Das Protokoll wird k-mal wiederholt, dadurch sinkt die Betrugswahrscheinlichkeit $< (\frac{1}{2})^k$

Bemerkung

1. Zero-Knowledge Eigenschaft:

   Falls e bekannt, dann kann man (C) ohne Kenntnis von s korrekt antworten:

   - $e = 0$: C wählt beliebiges $x \in \mathbb{Z}_n^*$ und $y = x^2$
   - $e = 1$: C wählt beliebiges $u \in \mathbb{Z}_n^*$ und setzt $y = u^2 v^{-1} \Rightarrow u^2 = vy$

   (Als Mitschrift ist es nicht erkennbar, ob die Folge der e zufällig ist oder von C gesetzt wurde)

2. Ohne Kenntnis von e, müßte C sowohl x mit $y = x^2$, als auch $u = xs$ kennen

   $\Rightarrow$ er kennt $s = ux^{-1}$, d.h. ein Betrüger übersteht eine Runde Fiat Shamir mit Wahrscheinlichkeit $\frac{1}{2}$

Beispiel
$p = 37,\ q = 41,\ n = 1517,\ s = 752,\ v = s^2 = 1180$
1. Runde:

- A wählt $x = 195$, schickt $y = x^2 = 100$ an B
- B würfelt $e = 1$
- A schickt $u = sx = 752 \cdot 195 = 1008$ an B
- B verifiziert $u^2 = sx = 1008^2 = 1191,\ vy = 1180 \cdot 100 = 1191$ ok

2. Runde:

- A wählt $x = 409$, schickt $y = 409^2 = 411$ an B
- B würfelt $e = 0$
- A schickt $x = 409$ an B

- B verifiziert $409^2 = 411$ ok

Bemerkung Fiat-Shamir-Feige Verfahren:
In der Praxis zur Beschleunigung parallel:

1. A wählt k Elemente $x_1, \ldots, x_k \in \mathbb{Z}_n^*$
2. B wählt k Elemente $e_1, \ldots, e_k \in \{0, 1\}$ die restlischen Schritte entsprechend.

Zwei weitere praktisch verwendete Zero-Knowledge Protokolle sind:

- Schnorr (Sicherheit beruht auf Diskretem Logarithmus)
- Guillou Quisquater (Sicherheit $\Leftrightarrow$ RSA Sicherheit)

(Fiat-Shamir-Feige: Sicherheit $\Leftrightarrow$ Rabin Verfahren)

Kapitel 14

Elliptische Kurven

14.1 Einführung

Bezeichnungen:
Sei: k Körper, $P(x, y) \in k[x, y]$ Polynom

Definition 14.1.1 *Die Lösungsmenge der Gleichung* $P(x, y) = 0,\ x, y \in k$ *heißt* algebraische Kurve

Beispiel
$k = \mathbb{R},\ P(x, y) = x^2 + y^2 - 1$ Einheitskreis
Kompaktifizierung durch Hinzufügen des Punktes bei ∞.
(Hintergrund: Projektiver Raum, statt z.B. $x^2 + x = y \in k^2$ betrachtet man die *Homogenisierung* $x^2 + xz = yz$ in $P_k^2 := k^3 \setminus \{0, 0, 0\}/\sim$ mit $\forall\ \alpha, \beta \in k^3 \setminus \{0, 0, 0\} : \alpha \sim \beta \Leftrightarrow \exists\ \lambda \in k : \alpha = \lambda\beta$)
Beispiel
$k = \mathbb{C}$ $\rightsquigarrow$: Kurve ist reel 2-dimensional, Funktionentheorie $\rightsquigarrow$ Fläche $\rightsquigarrow$ Riemannsche Fläche;

- Topologie:
  - Sphäre mit Geschlecht $g = 0$
  - Torus mit Geschlecht $g = 1$
  - Brezel mit Geschlecht $g = 2, \ldots$

- Lineare Gleichungen und quadratische Formen $\rightsquigarrow g = 0$
- elliptische Kurven haben Geschlecht g=1
- sonstige haben Geschlecht $g > 1$

Beispiel
$k = \mathbb{Q}$ Zahlentheorie:

- $g = 0$: d.h. quadratisches oder lineares Polynom
  $\rightsquigarrow$ Lösungsmenge gut verstanden (Hasse Prinzip)
- $g > 1$: *Satz von Mordell Faltings (1983):*
  Es gibt nur endlich viele rationale Lösungen
- $g = 1$: elliptische Kurven, reichhaltige Theorie, *Satz von Morell Weil:*
  Die Lösungsmenge ist eine endlich erzeugte abelsche Gruppe.

14.2 Elliptische Kurven

Ab jetzt: Sie k ein Körper mit $char(k) \neq 2, 3$

Bemerkung
$char(k) = 2$ ist für die Kryptographie wichtig.

Definition 14.2.1 *Das kubische Polynom $x^3 + ax + b, a, b \in k$ habe keine doppelten Nullstellen.*
Dann heißt

$$E := \{(x, y) \in k^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \; (\dagger)$$

elliptische Kurve.
$\mathcal{O}$ ist der ausgezeichnete Punkt Punkt bei $x = \infty$.

Bemerkung

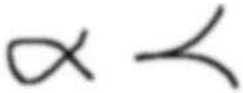


Abbildung 14.1: Selbstüberschneidung und Spitze

- Jede Gleichung der Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

läßt sich für $char(k) \neq 2, 3$ auf die Form $(\dagger)$ bringen

- Das kubische Polynom

$$P(x, y) = y^2 - x^3 - ax - b$$

hat keine doppelten Nullstellen

$\Leftrightarrow gradP(x, y) \neq 0$ überall

$\Leftrightarrow \triangle := -16(4a^3 + 27b^2) \neq 0$ *Diskriminante*

- Alternative Definition.:

Elliptische Kurve ist eine nichtsinguläre Kurve mit Geschlecht 1 und ausgezeichnetem Punkt $\mathcal{O}$

- $\triangle = 0$ würde bedeuten, daß die Kurve Selbstüberschneidungen oder Spitzen hat (siehe Abbildung 14.1).

Beispiel

1. $y^2 = x^3 - 4x + 2,\ \triangle > 0$ (Abbildung 14.2)
2. $y^2 = x^3 - 3x + 3,\ \triangle < 0$ (Abbildung 14.3)

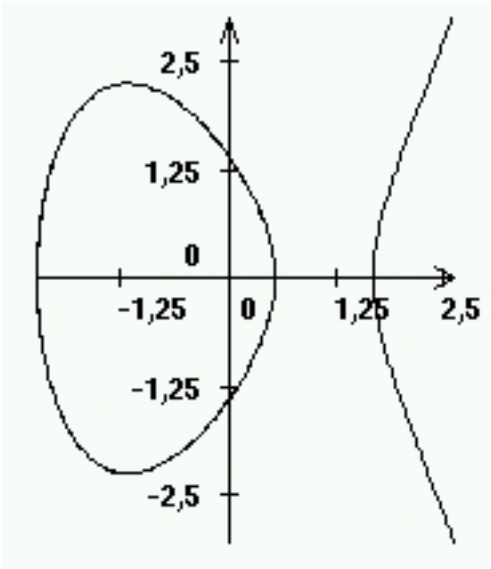


Abbildung 14.2: $y^2 = x^3 - 4x + 2,\ \triangle > 0,$

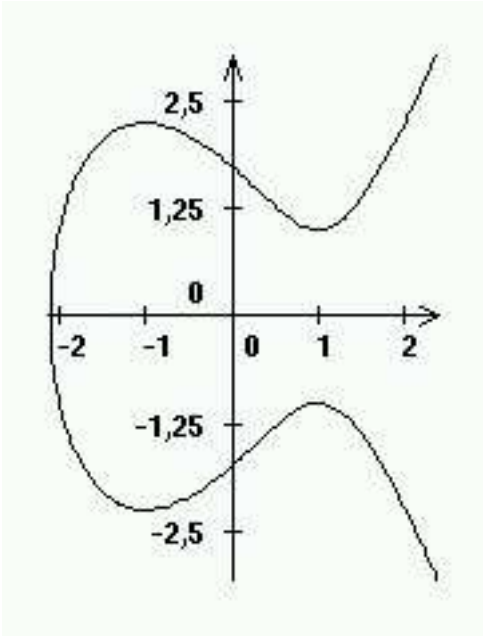


Abbildung 14.3: $y^2 = x^3 - 3x + 3,\ \triangle < 0,$

Gruppenstruktur von $(E, +)$

Folgender Gedankengang führt zu einer Definition für die Addition von zwei Punkten $\in E$:
Sei $y = \lambda x + \mu$ Gleichung einer Gerade und $(x, y) \in k^2$ ein Schnittpunkt von der Gerade und E, dann gilt:
(i) $y = \lambda x + \mu$
und (ii) $(\lambda x + \mu)^2 = x^3 + ax + b$.

(ii) $\Leftrightarrow x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + b - \mu^2 = 0 \quad (\dagger)$, eine kubische Gleichung!

Sind $P = (x_1, y_1), \quad Q = (x_2, y_2) \in k^2$ zwei Punkte von E, so legen sie eine Gerade fest:

$$y = \lambda x + \mu, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = y_1 - \lambda x_1$$

x_3 ist die 3. Lösung der kubischen Gleichung $(\dagger)$.
Ist nun $T = (x_3, y_3)$ der dritte Schnittpunkt von E und der Geraden, so ist $P + Q$ definiert durch $R = (x_3, -y_3)$, Also T wird an der x-Achse gespiegelt.

Beispiel
$k = \mathbb{Q}$: aus 2 rationalen Lösungen läßt sich eine dritte konstruieren (siehe Abbildung 14.4).

Definition 14.2.2 *Seien* $P = (x_1, y_1) \quad Q = (x_2, y_2)$ *zwei Punkte der elliptischen Kurve* E.
$R = P + Q$ *ist folgendermaßen definiert:*

1. *Fall:* $P = \mathcal{O}$, *dann*
$$R = P + Q = Q,$$
also $\mathcal{O}$ *ist das Neutrale Element der Gruppe*

2. *Fall:* $\mathcal{O} \neq P \quad \mathcal{O} \neq Q$ *aber* $(x_2, y_2) = (x_1, -y_1)$
(P *liegt senkrecht über oder unter* Q*)*
$$\Rightarrow R = P + Q = \mathcal{O}$$

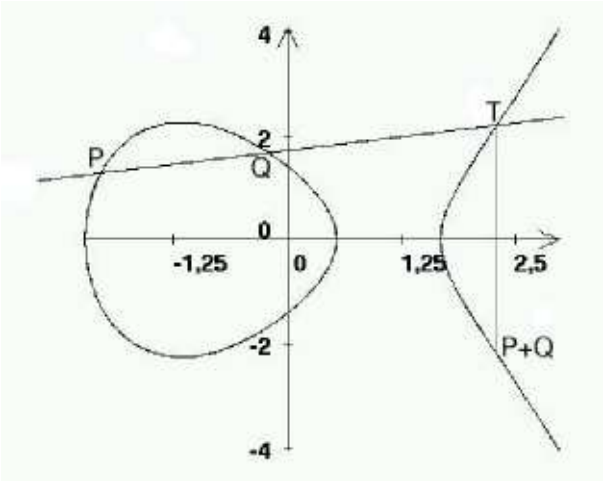


Abbildung 14.4: Beispiel für die Verknüpfung

3. *Fall:* $\mathcal{O} \neq P = Q$ *und* $y_2 = y_1 \neq 0$*, dann*

$$R = P + Q = (x_3, y_3)$$

mit $x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1$ *und* $\lambda = \frac{3x_1^2+a}{2y_1}$

4. *Fall:* $\mathcal{O} \neq P \neq q \neq \mathcal{O} \quad (x_2, y_2) \neq (x_1, -y_1)$*, dann*

$$R = P + Q = (x_3, y_3)$$

mit $x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$ *und* $\lambda = \frac{y_2-y_1}{x_2-x_1}$

Bemerkung
λ ist die Steigung der Verbindungsgeraden PQ.

Satz 14.2.3 $(E, +)$ *ist eine abelsche Gruppe.*
(Beim Beweis ist nur die Assoziativität schwer zu zeigen)

Beispiel
$k = \mathbb{C}$. Für jede elliptische Kurve E über $\mathbb{C}$ existiert ein Gitter Λ in $\mathbb{C}$ und eine meromorphe Funktion $\wp_\Lambda : \mathbb{C} \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ $(= \mathbb{C} \cup \{\infty\})$ ($\wp$ ist die Weierstraßsche $\wp$-Funktion), mit folgenden Eigenschaften:

- $\wp_\Lambda$ ist Λ-periodisch: $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)\ \forall\ \lambda\ \in\ \Lambda,\ \forall\ z\ \in \mathbb{C}$
- $\wp_\Lambda$ erfüllt die Differentialgleichung

$$(\wp'_\Lambda(z))^2 = \wp^3_\Lambda(z) + a\wp_\Lambda(z) + b$$

- $\phi : \mathbb{C}/\Lambda \longrightarrow E$ mit $z \longmapsto (\wp_\Lambda(z), \wp'_\Lambda(z)))$ ist ein Gruppenisomorphismus.

Beispiel
$k = \mathbb{Q}$, $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$: *Satz von Mordell Weil:*
(E,+) ist eine *endlich erzeugte* abelsche Gruppe:

$$(E, +) = \mathbb{Z}^r \bigoplus T.$$

- T ist endliche Gruppe, der *Torsionsanteil*
- r ist der Rang.

14.3 Elliptische Kurven über endlichen Körpern

Sei $k = \mathbb{F}_q, \quad q = p^m, \quad p$ prim, $p \neq 2, 3$

1. $\#E$:

$$E = \{(x, y)\mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

$\Rightarrow \#E = \sum_{x\in\mathbb{F}_q} \#\{y \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} + 1$
$\rightsquigarrow \#E \leq 2q + 1$
Heuristich: Für ungefähr die Hälfte aller $x \in \mathbb{F}_q$ ist $x^3 + ax + b$ ein Quadrat (die Hälfter aller $\tilde{x} \in \mathbb{F}_q$ ist ein Quadrat).
$\rightsquigarrow \#E \approx 1 + 2\frac{q}{2}q = 1 + q$

Satz 14.3.1 *(Hasse): Es gilt*

$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$$

Algorithmus von Schoof ermöglicht effektive Berechnung von $\#E$.

2. Struktur von(E,+):

   Satz 14.3.2 $(E,+)$ *ist direkte Summe von zwei zyklischen Gruppen*

   $$(E,+) = \mathbb{Z}_n \bigoplus \mathbb{Z}_m,$$

   für n, m *geeignet.*

Beispiel
$y^2 + x^3 + x + 6 \mod 11$, d.h. $k = \mathbb{F}_{11},\ p = q = 11 (\triangle \neq 0)$.
Man erhält (z.B. durch Ausprobieren)

$$\begin{aligned} E \quad &= \quad \{\mathcal{O}, (2,7), (5,2), (8,3), (10,2), (3,6), (7,9), \\ &\qquad (7,2), (3,5), (10,9), (8,8), (5,9), (2,4)\} \\ \Rightarrow \#E &= 13 \end{aligned}$$

$(E,+)$ ist zyklisch mit Erzeuger $(2,7)$:

1. $2(2,7) = (5,2)$
2. $3(2,7) = (8,3)$, usw

Kapitel 15

ECC (elliptic curve cryptographie)

$q = p^m,\ p$ prim, $p \neq 2, 3,\ \ E/\mathbb{F}_q,\ y^2 = x^3 + ax + b,\ \Delta \neq 0,\ (E, +)$ elliptische Kurve.

15.1 Diffie-Hellman-Schlüsselaustausch

$P \in E$ Element mit großer Ordnung. Diffie-Hellman-Schlüsselaustausch wie gewohnt nur mit additiv geschriebener Verknüpfung.

1. A wählt k_a aus $\mathbb{N}^*$,

   B wählt $k_b \in \mathbb{N}^*$

2. A schickt $k_a \cdot P (\in E)$ an B,

   B schickt $k_b \cdot P (\in E)$ an A

3. A berechnet $k_a \cdot (k_b \cdot P) = (k_a k_b)P = K \in E$,

   B berechnet $k_b(k_a P) = K \in E$

   A und B kennen jetzt den geheimen Punkt $K \in E$.

15.2 El-Gamal à la Menezes-VanStone

Menge der Klartexte $\mathcal{P} = \mathbb{F}_q^* \times \mathbb{F}_q^*, \quad |\mathcal{P}| = (q-1)^2$.
Sei $K = (x_k, y_k)$ der geheime Schlüssel;

wir nehmen an $x_k,\ y_k \in \mathbb{F}_q^*$.
Eine Nachricht $m = (m_1, m_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ wird verschlüsselt durch $c = (c_1, c_2) = (m_1 x_k, m_2 y_k) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

Konkret öffentlicher Schlüssel: q, E, P, $k_b P$
B's privater Schlüssel : k_b , $m = (m_1, m_2)$ sei Nachricht von A für B.

1. A wählt k_a und berechnet $k = k_a k_b P = (x_k, y_k) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

   A schickt $(k_a P, m_1 x_k, m_2 y_k)$ an B:

2. B berechnet $k_a k_b P = K = (x_k, y_k)$, sowie $m_1 = m_1 x_k x_k^{-1},\ m_2 = m_2 y_k y_k^{-1}$

Bemerkung

1. Die naheliegende El-Gamal-Variante wäre $\mathcal{P} = E$ und $m \in \mathcal{P}$ durch c=m+k zu verschlüsseln.

   zwei Nachteile:

   a) $|\mathcal{P}| = q + 1$

   b)Wie bettet man „echte" Texte in E ein?

2. Vorteile von ECC:

   a) höhere Effizienz: zwar kompliziertere Verknüpfungen, wird aber überkompensiert durch kürzere Längen (Schlüssel ect.)

   b)Viele verschiedene elliptische Kurven: zu allen q,a,b: $\Delta \neq 0$

Kapitel 16

Primzahlbeweise und Faktorisierung mit ell. Kurven

16.1 Pseudokurven

Sei $n \in \mathbb{N}^{\geq 2},\ n \neq 2, 3,\ a, b \in \mathbb{Z}_n,\ \Delta = -16(4a^3+27b^2),\ ggT(\Delta, n) = 1$
$E = \{(x, y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$
n prim $\rightsquigarrow$ E elliptische Kurve,
n nicht prim $\rightsquigarrow$ sogenannte Pseudokurve.
$P = (x_1, y_1), Q = (x_2, y_2), P, Q \in E.$
In der Regel kann $P + Q \in E$ genauso definiert werden wie in 11.2.
Ausnahme:
In der Definition der Steigung $\lambda = \dfrac{3x_1^2 + a}{2y_1}$ (Fall 3, Problem, falls $y_1 \notin \mathbb{Z}_n^*$) bzw. $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ (Fall 4, Problem, falls $x_2 - x_1 \notin \mathbb{Z}_n^*$)
$\rightsquigarrow$ P+Q nicht definiert.
Aber dann hat man einen echten Teiler von n gefunden !!
$(1 < (y_1, n) < n$ *oder* $1 < (x_2 - x_1, n) < n)$

Lemma 16.1.1 *$p \mid n$ prim und E' die durch $y^2 = x^3 + \bar{a}x + \bar{b}$ über $\mathbb{F}_p$ definierte elliptische Kurve. $P, Q \in E$*

a) Die Abbildung $\varphi : E \to E',\ (x, y) \to (x \mod p,\ y \mod p)$ erfüllt

$\varphi(P+Q) = \varphi(P) + \varphi(Q)$, *falls P+Q definiert.*

b) Ist kP *für ein* $k \in \mathbb{N}^*$ *definiert und* $kP \neq \mathcal{O}$, *so gilt* $k\varphi P \neq \mathcal{O}$

16.2 Goldwasser-Killian-Test

(Elliptic curve primality proving)

Satz 16.2.1 *n, E wie oben.* $s,\ m \in \mathbb{N},\ s \mid m,\ P \in E$ *mit* mP *definiert und*
$mP \neq \mathcal{O}$, *aber für alle Primteiler q von s ist (*$\frac{m}{q}P$ *definiert) und* $\frac{m}{q}P \neq \mathcal{O}$.
Dann gilt für jeden Primteiler $p \mid n$*:*
$\#E' \equiv 0 \mod s$.
Falls $s > (n^{\frac{1}{4}} + 1)^2$, *so ist n prim.*

Beweis
Lemma b)
$\Rightarrow s \mid \text{ord}(\varphi(P)) =: P' \in E'$
$\Rightarrow$ erste Beh.
Falls $s > (n^{\frac{1}{4}} + 1)^2$
$\Rightarrow \#E' > (n^{\frac{1}{4}} + 1)^2$
$\overset{Satz von}{\underset{Hasse}{\Rightarrow}} \#E' < (p^{\frac{1}{2}} + 1)^2$
$\Rightarrow p > n^{\frac{1}{2}}$ für jeden Primteiler von n
$\Rightarrow$ p Primzahl.

16.3 Lenstras Elliptic-curve-method ECM zur Faktorisierung

n, E wie oben. $p \mid n$ prim , $P \in E,\ P' = \varphi(P) \in E'$.
Sei k ein Vielfaches von $\#E'$
$\Rightarrow kP = \mathcal{O}$
$\Rightarrow$ kP nicht definiert oder $kP = \mathcal{O}$.

2. Möglichkeit ist unwahrscheinlich.
Erste Möglichkeit liefert dagegen einen Teiler von n!!
vgl. oben , Nenner von $\lambda \notin \mathbb{Z}_n^*$
Kandidat für k: $k = \prod_{p_i^{e_i} \leq B} p^{e_i}$ (wie in Pollards (p-1)).
Funktioniert, falls in einem $\#E'$ nur kleine Primfaktoren vorkommen.
Falls kein Erfolg, wähle neues $E/\mathbb{Z}_n$.

Kapitel 17

Quantenalgorithmus von Shaw zur Faktorisierung

Sei $m \in \mathbb{N}^*, s \in \{0, 1, 2, \ldots, 2^m - 1\}$;
Binärdarstellung $s = (e_{m-1} \ldots e_2 e_1 e_0), e_i \in \{0, 1\}$
$V_s = |e_{m-1} > |e_{m-2} > \ldots |e_1 > |e_0 >$ m Qbit
(z.B. $m = 2, s = 2 = (10)_2, V_2 = |1 > |0 >$)
$\mathcal{H} = \{ \sum_{s=0}^{2^m-1} a_s V_s | a_s \in \mathbb{C}, \sum |a_s| = 1\}$= Raum der physikalischen Zustände $\subseteq \mathbb{C}^{2^m}$,
$\mathcal{H}$ unitärer Vektorraum, V_s ONB.
Jede Zustandsänderung ist eine unitäre Abbildung $\mathcal{H} \to \mathcal{H}$.
Man kann diese durch Kombination elementarer Gatter realisieren.

Quanten-Fourier-Transformation:

$QFT_m : \mathcal{H} \to \mathcal{H}, \quad V_s \to \frac{1}{2^{\frac{m}{2}}} \sum_{r=0}^{2^m-1} \exp\left(\frac{2\pi i r s}{2^m}\right) V_r$

QFT_m benötigt $\binom{m}{2}$ elementare Gatter.

Idee von Shaws Algorithmus

Zu $x \in \mathbb{Z}_n^*$ bestimmt man mit Quantenalgorithmus die Ordnung g von x.
Falls g gerade ist und $x^{\frac{g}{2}} \not\equiv -1 \mod n$, dann ist $ggT(x^{\frac{g}{2}} - 1, n)$ echter Teiler von n, da $(x^{\frac{g}{2}} - 1)(x^{\frac{g}{2}} + 1) = x^g - 1 \equiv 0 \mod n$.

Man wählt $m = 3L, L = \lceil log_2 n \rceil$.

Der Anfangszustand $\mathcal{H} \ni \psi_0 = \frac{1}{2^L} \sum_{s=0}^{2^{2L}-1} V_s \otimes V_0$, (d.H. letzte Qbits sind alle $|0>$) daraus macht man mit $O(L^3)$ elementare Gatter

$\mathcal{H} \ni \psi_1 = \frac{1}{2^L} \sum_{s=0}^{2^{2L}-1} V_s \otimes V_{x^s}$

QFT_{2L} auf die ersten 2L Qbits angewendet:

$\mathcal{H} \ni \psi_2 = \frac{1}{2^{2L}} \sum_{s=0}^{2^{2L}-1} \sum_{s=0}^{2^{2L}-1} \exp(\frac{2\pi irs}{2^{2L}}) V_r \otimes V_{x^s}$

Dann Messung der Qbits. Die Wahrscheinlichkeit für $V_r \otimes V_{x^j}$ beträgt

$$\frac{1}{2^{4L}} | \sum_{s \equiv j \mod g} \exp(\frac{2\pi irs}{2^{2L}}) |^2$$

groß nur dann, wenn $r \cdot g \sim d \cdot 2^{2L}$, sonst allgemeines Wegheben, d.h. $g \approx d \cdot \frac{2^{2L}}{r}$.

Experiment muss mehrfach wiederholen

$\rightsquigarrow$ gutes Indiz für g.

Kapitel 18

Quantenkryptographie

1. A schickt ein Photon an B mit einer der folgenden Polarisationen:

   $\underset{a0}{\updownarrow}\ \underset{a1}{\leftrightarrow}\ \underset{b0}{\searrow}\ \underset{b1}{\swarrow}$

2. B benutzt für jedes Photon einen von 2 Filtern: $\underset{a}{+}\ \underset{b}{\times}$,

   z.B falls A Möglichkeit a gewählt hat und B ebenfalls a $\rightsquigarrow$ Polarisation,

   wenn B dagegen b verwendet

   $\rightsquigarrow$ Wahrscheinlichkeit $\frac{1}{2}$ für a0 und $\frac{1}{2}$ für a1.

3. A und B teilen sich mit welche Möglichkeiten sie für welches Photon benutzt haben $\sim \frac{n}{2}$ Photonen beide gleich

   $\rightsquigarrow$ Folge von $\sim \frac{n}{2}$ Bits.

Clou: Lauscher zerstört die Hälfte dieser $\frac{n}{2}$ Bits
$\rightsquigarrow$ A und B bemerken den Fehler.