Algorithmische Zahlentheorie

Diese Arbeit beschäftigt sich mit der theoretischen Grundlage für die asymmetrische Kryptografie. Es werden zunächst die benötigten Grundlagen der Zahlentheorie gegeben, um anschließend einen genaueren Blick auf die Algorithmen zur Primzahlerkennung, des Diffie-Hellmann Austausches und der Anwendung elliptischer Kurven zu geben. Neben der Ausarbeitung verwendeter Algorithmen wird auch die Laufzeit dieser untersucht. Zufallszahlengeneratoren werden nicht betrachtet.

Im folgenden werden die Grundlagen der Zahlentheorie eingeführt, um anschließend ausgewählte Algorithmen, die in der asymmetrischen Kryptographie eingesetzt werden, betrachten zu können. Zum Nachschlagen weiterer Informationen über Persönlichkeiten der Zahlentheorie mit historischer Einordnung, bietet das Buch [12] von Jochen Ziegenbalg einen guten Überblick.

Grundlagen

In diesem Kapitel werden die Grundlagen zur Analyse von Primzahlen und dem diskreten Logarithmus gegeben. Dazu werden im allg. nur die Definitionen und Sätze geliefert. Für Beweise der hier angeführten Sätze sei auf die Bücher [1], [2], [6], [4] **[TODO noch weiter wenn nötig [x],[y],[z]]** verwiesen. Es wird vorausgesetzt, dass die Rechenvorschriften des Modulo bekannt ist.

Algebraische Strukturen

In diesem Kapitel werden die algebraischen Strukturen: Halbgruppen, Gruppen, Ringe und Körper vorgestellt. Diese werden für ein späteres Kapitel benötigt. Die algebraischen Strukturen beschreiben ein abstraktes Rechnen mit Zahlen. Dies ermöglicht gezielter nur die Rechenregeln an sich zu untersuchen, unabhängig von der Rechengröße und der jeweiligen Operation. Ein Anwendungsbereich ist u. a. in der Kryptographie zu finden. [7]

Halbgruppen

Eine Halbgruppe ist eine Menge M mit einer assoziativen Operation $\circ$, geschrieben mit (M, $\circ$) oder einfach nur M. Zur Erinnerung, das Assoziativgesetz besagt: $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in M$. Es gilt für sämtliche Elemente einer Halbgruppe. Das Zeichen $\circ$ ist Platzhalter für eine beliebige Operation. Der Wertebereich von $\circ$ ist eine Teilmenge von M so dass, $a \circ b \in M$ für alle $a, b \in M$. Für das Zeichen $\circ$ werden auch die folgenden Operationszeichen verwendet: $*$, $\cdot$, $+$. Auch muss die Menge nicht zwangsläufig M sein. [2]

Durch das Assoziativgesetz können also Klammern weggelassen werden. Zum besseren Verständnis konkrete Beispiele von Halbgruppen [2]:

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Halbgruppen mit der Addition als Operation, ebenso wie mit der Multiplikation.

- Wenn a $\circ$ $b = |b{-}a|$ für alle $a, b \in \mathbb{Z}$, dann ist ($\mathbb{Z}$, $\circ$) keine Halbgruppe. Da in diesem Fall (1 $\circ$ 2) $\circ$ 3 = 1 $\circ$ 3 = 2 ist, aber 1 $\circ$ (2 $\circ$ 3) = 1 $\circ$ 1 = 0 ist. Ein verändern der Klammerung ergibt unterschiedliche Ergebnisse, somit ist das Assoziativgesetz nicht mehr gewährleistet, wodurch $\mathbb{Z}$ in diesem Fall keine Halbgruppe mehr sein kann.

Sobald es ein neutrales Element in einer Halbgruppe gibt heißt dieses **Monoid**. Ein neutrales Element ist immer dann gegeben wenn es ein e $\in$ M gibt, sodass für alle a $\in$ M gilt: a $\circ$ e = e $\circ$ a = a. Dieses weitere Axiom muss von jeder Halbgruppe erfüllt werden um ein Monoid zu sein. Als Zeichen für ein Monoid wird neben e oft auch 1 verwendet, bei den Operationszeichen $\circ$, $\cdot$, $*$. Wird das + als Operationszeichen verwendet ist oft 0 das neutrale Element. [2]

Wenn ein Monoid auch das folgende Axiom erfüllt, ist es eine **Gruppe**. Existiert für alle a $\in$ G ein b $\in$ G, sodass a $\circ$ b = b $\circ$ a = e gilt, so heißt b invers zu a. [2]

Ringe

In einem Ring als Algebraische Struktur sind mehr als nur eine Operation vorhanden. Eine Menge R mit den zwei Operationen + und $\cdot$ auf R ist genau dann ein Ring wenn folgenden drei Bedingungen gelten [2]:

- (R, +) ist eine abelsche Gruppe. (Eine Operation $\circ$ auf einer Menge M heiß kommutativ oder abelsch, wenn: a $\circ$ b = b $\circ$ a für alle a, b $\in$ M gilt.)
- (R, $\cdot$) ist ein Monoid
- Für alle a, b, c $\in$ R gilt: a(b + c) = ab + ac, (a + b)c = ac + bc (Distributivgesetze)

Zusätzlich heißt ein Ring kommutativ, wenn die Operation $\cdot$ kommutativ ist. Ein Ring besitzt also immer eine kommutative Addition und eine nicht notwendigerweise kommutative Multiplikation. Die beiden Distributivgesetze verbinden diese beiden Operationen miteinander. Ein Ring heißt nullteilerfrei wenn a $\cdot$ b = 0 ist und dadurch impliziert wird, dass a = 0 oder b = 0 sein muss, für alle a, b $\in$ R. Wenn es für ein a $\in$ R ein b gibt, so dass ab = ba = 1 gilt, dann ist a invertierbar oder eine Einheit. Alle Elemente im Monoid (R, $\cdot$) wo dies zutrifft sind in einer multiplikativen Gruppe zusammengefasst, bezeichnet wird diese mit R*. [2]

Es gibt spezielle Ringe, die sogenannten Körper. Ist eine Menge (K, +, $\cdot$) ein Ring und ist $(K/\{0\}, \cdot)$ eine kommutative Gruppe, heißt K ein Körper. Alle von Null verschiedenen Elementen sind Einheiten und es gilt: K* = $K/\{0\}$. [2]

Integritätsbereiche

Wie in [3] angegeben ist ein Integritätsbereich ein kommutativer, nullteilerfreier Ring R mit Einselement. Aus dieser Definition ergeben sich die Integritätsbereiche der ganzen

Zahlen $\mathbb{Z}$, der ganzen Gauß'schen Zahlen $\mathbb{Z}$[i] und des Polynomrings in einer Unbestimmten X über einem Körper K, der K[X] bezeichnet wird.

$$\mathbb{Z}[i] = \{n + im \in \mathbb{C} : n, m \in \mathbb{Z}\}$$

$$K[X] = \{p(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \mid a_i \in K, n \in \mathbb{N}\}$$

Des weiteren wird ein Integritätsbereich mit einer Funktion $\beta : R \longrightarrow \mathbb{N}$, für die gilt:

$$\mathrm{x = qy + r, \quad q, r \in R, mit\ r = 0\ oder\ } \beta(\mathrm{r}) < \beta(\mathrm{y})$$

als euklidischer Ring bezeichnet und lässt die Division mit Rest zu. Wie in [3] gezeigt, ist jeder der Ringe Z, Z[i] und K[X], für einen beliebigen Körper K, euklidisch. Die Erkenntnis das es weitere Integritätsbereiche als $\mathbb{Z}$ gibt, wird in den effizienten Primzahltests wieder aufgegriffen.

Die Teilbarkeit einer Zahl a $\in$ R durch b $\in$ R ohne Rest wird b $\mid$ a geschrieben. Kann a durch b nicht ohne Rest geteilt werden, wird b $\nmid$ a geschrieben.

Restklassenringe in $\mathbb{Z}$

Restklassenringe $\mathbb{Z}/\mathrm{m}\mathbb{Z}$ oder auch $\mathbb{Z}_\mathrm{m}$ ergeben sich aus der Definition einer Addition und Multiplikation auf Restklassen. Eine Restklasse bezeichnet zwei Zahlen $\in \mathbb{Z}$ die bei der Division durch m $\in \mathbb{N}$ den gleichen Rest haben. Diese zwei Zahlen sind also in der gleichen Restklasse. Die Anzahl der Restklassen in einem Restklassenring ist gleich m. Die Äquivalenzrelation der beiden Zahlen bezüglich der Restklasse, kann wie folgt definiert werden: Zwei Zahlen x, y $\in \mathbb{Z}$ heißen kongruent modulo m $\in \mathbb{N}$ wenn m $\mid x - y$. In Zeichen:

$$x \equiv y \ mod \ m$$

Die zugehörigen Beweise und Rechenvorschriften für Restklassenringe finden sich in [3].

Euklidischer Algorithmus

Der euklidische Algorithmus wird zur Berechnung des größten gemeinsamen Teiler zweier Zahlen benötigt. Der Algorithmus findet in fast allen weiteren Betrachtungen Anwendung und wird deshalb explizit angegeben. Wie in [8] bewiesen, kann der Algorithmus folgend definiert werden:

Sind m, n $\in \mathbb{N}$ zwei natürliche Zahlen mit m $\leq$ n und m $\nmid$ n, so gilt:

$$ggT(m, n) = ggT(n \ mod \ m, m).$$

Euler'sche φ-Funktion

Die Eulersche phi Funktion φ(m) berechnet die Anzahl teilerfremder Zahlen für eine gegebene Zahl m $>$ 1. Also gilt nach [3]:

$$\varphi(m) = Card((\mathbb{Z}/m\mathbb{Z})^*).$$

Mit Card(M) ist die Kardinalität der Menge M gemeint. Die Bezeichnung $(\mathbb{Z}/\mathrm{m}\mathbb{Z})^*$ steht für die Menge der Zahlen aus $\mathbb{Z}/\mathrm{m}\mathbb{Z}$ die ein multiplikatives Inverses besitzen. Geschrieben sieht die Menge wie folgt aus:

$$(\mathbb{Z}/m\mathbb{Z})^* = \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid ggT(a,m) = 1\}.$$

Die Menge $\mathbb{Z}_{\mathrm{m}}^*$ kann auch Einheitengruppe genannt werden. Ein Beispiel für den Restklassenring modulo 10 ($\mathbb{Z}_{10}^*$) sind die Elemente 1, 3, 7 und 9. In [9] kann gut nachvollzogen werden warum ein multiplikatives Inverses von a existiert, wenn der ggT(a,m) = 1 ist.

Konzept

TODO Konzept...

Primzahlen

Natürliche Primzahlen werden definiert durch Zahlen ¿ 1 die nur durch Eins oder sich selbst teilbar sind. Wie im Kapitel Primfaktorzerlegung gezeigt, können alle natürlichen Zahlen mit einer Multiplikation von Primzahlen erzeugt werden. Sie bilden sozusagen die Bausteine aller natürlichen Zahlen. Die Unberechenbarkeit mit der sie auftreten gibt Mathematikern schon seit Jahrtausenden Rätsel auf und ist ein Grundstein unserer heutigen Verschlüsselungsverfahren. In anderen Zahlensystemen als den natürlichen Zahlen ist die gewohnte Definition von Primzahlen nicht vollständig/korrekt. Sie sagt nur etwas über die Irreduzibelität eines Elements in einem Integritätsbereich aus. Da in den natürlichen Zahlen aber jedes irreduzibles Element auch prim ist reicht diese Definition für $\mathbb{N}$ aus. Für alle Integritätsbereiche gilt für die Primheit folgende Definition nach [3]:

Ein Element $\mathrm{p} \in \mathrm{R} \setminus (\mathrm{R}^* \cup \{0\})$ heißt prim oder Primelement, wenn für alle $\mathrm{a}, \mathrm{b} \in \mathrm{R} \setminus \{0\}$ gilt:

$$p \mid ab \Longrightarrow p \mid a \text{ oder } p \mid b.$$

Mit Hilfe der Primzahlen kann der Restklassenring $\mathbb{Z}/\mathrm{m}\mathbb{Z}$ spezialisiert werden. Ist m eine Primzahl p, so ist $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ ein Körper und wird auch $\mathbb{F}_{\mathrm{p}}$ bzw. $\mathbb{GF}_{\mathrm{p}}$ bezeichnet.

Neben den normalen Primzahlen gibt es weitere sogenannte Pseudoprimzahlen. Diese Primzahlen verhalten sich bezogen auf einen Algorithmus genauso wie echte Primzahlen, sie sind jedoch zusammengesetzt. Ein Beispiel für solche Zahlen sind Carmichaelzahlen die in einem späteren Kapitel thematisiert sind.

Leider gibt es keine bekannten effizienten Verfahren um Primzahlen zu generieren. Dennoch kann man Primzahlen recht einfach raten. Grundsätzlich ist es möglich eine große Anzahl von Zahlen auszuschließen. Man denke an: nur ungerade Zahlen, die Teilungsgesetze und die Tatsache das alle Primzahlen ¿ 3 in der Form 4k +1 oder 4k +3, k $\in \mathbb{N}$ vorliegen. Alle geratenen Zahlen müssen jedoch einem Primzahltest(vgl. Kapitel **??**) zur Verifizierung unterzogen werden. In [11] ist beschrieben wie ein Generierungsprozess erfolgen kann.

In diesem Kapitel soll der diskreter Logarithmus betrachtet werden. Es werden Anwendungspeilspiele aufgezeigt und genauer erläutert weswegen sich der diskreter Logarithmus besonders gut in der Kryptografie als Einwegfunktion eignet. Zu beginn wird das grundsätzliche Problem beim diskreten Logarithmus an einem Beispiel praxisnahe erläutert, um im Anschluss auf Algorithmische Lösungen einzugehen wie der diskreten Logarithmus in $\mathbb{Z}_{\mathrm{p}}^*$ und auf elliptische Kurven berechnet werden kann. Hierfür wird der Baby-Step-Giant-Step-Algorithmus vorgestellt.

Das Problem des diskreten Logarithmus im Detail

Es existiert eine Primzahl p, ein erzeugendes Element g für $\mathbb{Z}_{\mathrm{p}}^*$ sowie eine ganze Zahl x. Zu der diskreten Exponentialfunktion $g^x \ mod \ p$ gibt es die diskrete Logarithmusfunktion, die zu einem gegebenen y und g, x beschreibt. Somit ist x der diskrete Logarithmus von y zur Basis g. ($y = g^x \ mod \ p$) Jede Zahl aus $\mathbb{Z}_{\mathrm{p}}^*$ lässt sich als Potenz von g darstellen, wenn g ein erzeugendes Element von $\mathbb{Z}_{\mathrm{p}}^*$ ist. Ist dies nicht der Fall, so muss es nicht zu jedem $y \in \mathbb{Z}_{\mathrm{p}}^*$ einen diskreten Logarithmus geben. [1] Um das eigentliche Problem des diskreten Logarithmus zu verstehen ist es hilfreich, die Logarithmen in $\mathbb{R}$ mit Logarithmen in $\mathbb{Z}_{\mathrm{p}}^*$ gegenüberzustellen.

$$\begin{aligned} y &= g^x \\ 1024 &= 2^x \\ x &= log_2 1024 \\ x &= 10 \end{aligned} \tag{0.1}$$

$$\begin{aligned} y &= g^x \ mod \ p \\ 10 &= 2^x \ mod \ 11 \\ x &= log_2 10 \\ x &= 3.32193... \ \lightning \end{aligned} \tag{0.2}$$

Die Gleichungen aus (0.1) zeigen wie der Logarithmus von x zur Basis g, mit der Logarithmusfunktion berechnet werden kann. Auf diese Weise sind Gleichungen für die positiven reellen Zahlen $\mathbb{R}^+$ immer eindeutig lösbar. Für die Gleichungen aus (0.2) wird ebenfalls mit der Logarithmusfunktion versucht, den Logarithmus von 10 zu Basis 2 zu erhalten. Als Ergebnis erhält man eine Zahl die nicht in $\mathbb{Z}_{\mathrm{p}}^*$ enthalten ist. Was auch nicht verwundert, da die Logarithmusfunktion *mod* 11 gar nicht berücksichtigt. Genau hier ist das grundsätzlich Problem beim diskreten Logarithmus. Es gibt keine mathematische Rechenoperation die es ermöglicht den diskreten Logarithmus in einem endlichen Körper mit nur einem Rechenschritt zu berechnen. Um dennoch eine Lösung zu erhalten, scheint das Enumerationsverfahren das naheliegendste zu sein. Hierbei werden einfach alle Werte die für x in frage kommen durchprobiert. So ist die Lösung der Gleichungen aus (0.2), $x = 5$. [10] Für sehr große Gruppen, wo x Beispielsweise eine 160 Bit große Zahl ist, gibt es bis heute keine Algorithmen die den diskreten Logarithmus effizient berechnen.[1] Es gibt allerdings eine ganze Reihe von Algorithmen die in der Lage sind den diskreten Logarithmus gezielter zu berechnen als das naive Ausprobieren. Nachfolgend soll der Baby-Step-Giant-Step-Algorithmus genauer betrachtet werden.

Diskreter Logarithmus auf elliptische Kurven

In Kapitel **??** wurde die Addition von Punkten und Skalaren auf elliptische Kurven beschrieben. In diesem Unterkapitel soll kurz beschrieben werden was genau der Logarithmus auf einer elliptische Kurven über $\mathbb{Z}_p^*$ ist. Für eine elliptische Kurve E über den Primkörper $\mathbb{Z}_p^*$ mit den Punkten $P, Q \in E(\mathbb{Z}_p^*)$, gibt es ein $k \in \mathbb{Z}_p^*$ sodass die folgende Gleichung erfüllt ist:

$$Q = kP$$

So wird die Zahl k als diskreter Logarithmus von Q zur Basis P bezeichnet. Den diskreten Logarithmus aus $E(\mathbb{Z}_p^*)$ zu bestimmen, ist noch einmal ungleich komplexer als aus $\mathbb{Z}_p^*$. Dieses Berechnungsproblem wird **E**lliptic **C**urve **D**iscrete **L**ogarithmen **P**roblem, kurz **ECDLP**, genannt.

Fazit

TODO Fazit....

Bezüglich der Sicherheit von heutigen kryptographischen Verfahren muss man sich aktuell keine sorgen machen, zumindest wenn die Mindestanforderungen bezüglich der Größe des Körpers und der Schlüssellänge eingehalten werden. Bei zu kleinen Schlüssellängen ist auch bei der besten Verschlüsselung heutzutage keine Sicherheit gegeben.

Der Höhepunkt im Bereich der Verschlüsselung kann noch nicht erreicht sein. Noch schnellere und effizientere und somit „sicherer" Verschlüsselungstechniken werden benötigt um auch zukünftigen Anforderungen gerecht zu werden. Den die nötigen Algorithmen um sämtliche heutigen Verschlüsselungen zu brechen existieren schon, laut Peter W. Shor. Diese stellt er in [5] vor. Diskrete Logarithmen können in polynomialer Zeit berechnet werden, es muss nur noch gelingen einen Quantencomputer zu bauen.

Anhang

TODO Anhang...

Literaturverzeichnis

Bücher

[1] Albrecht Beutelspacher, Heike B. Neumann und Thomas Schwarzpaul. *Kryptografie in Theorie und Praxis.* Wiesbaden: Vieweg + Teubner und GWV Fachverlage GmbH, 2010.

[2] Oliver Deiser und Caroline Lasser. *Erste Hilfe in Linearer Algebra.* Berlin Heidelberg: Springer Spektrum, 2015.

[3] Otto Forster. *Algorithmische Zahlentheorie.* Wiesbaden: Springer Fachmedien, 2015.

[4] Markus Hufschmid. *Information und Kommunikation.* Wiesbaden: Teubner Verlag, 2006.

[5] Peter W. SHOR. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. 600 Mountain Ave. Murray Hill, NJ 07974, USA: AT und T Bell Labs, 1994.

[6] Stephan SPITZ, Michael PRAMATEFTAKIS und Joachim SWOBODA. *Kryptographie und IT-Sicherheit*. Wiesbaden: Vieweg + Teubner Verlag und Springer Fachmedien, 2011.

[8] Angelika STEGER. *Diskrete Strukturen Band 1*. Berlin Heidelberg: Springer, 2007.

[9] Gerald TESCHL und Susanne TESCHL. *Mathematik für Informatiker Band 1*. Berlin Heidelberg New York: Springer, 2007.

[10] Dirk WALLERSTORFER. *DLP/ECDLP Probleme und Lösungen*. Fachhochschul für Computer- und Mediensicherheit in Hagenberg, 2006.

[11] Kurt-Ulrich WITT. *Algebraische und zahlentheoretische Grundlagen für die Informatik*. Wiesbaden: Springer Fachmedien, 2014.

[12] Jochen ZIEGENBALG. *Elementare Zahlentheorie*. Wiesbaden: Springer Spektrum, 2015.

Alles Andere

[7] Prof. Dr. Frauke SPRENGEL. *Kryptographie und Algorithmen*. Techn. Ber. Hochschule Hannover, 2012.