Elliptische Kurven in der Charakteristik p>3 und die Implementierung der Arithmetik in der Programmiersprache Python

Studienarbeit T3_3101

Hochschule:	Duale Hochschule Baden-Württemberg Mannheim
Kurs:	TINF20IT2
Name:	Vorname Nachname
Matrikelnummer:	XXXXXX
E-Mail:	sXXXXXX@student.dhbw-mannheim.de

Studiengangsleiter:	Prof. Dr. Nathan Sudermann-Merx
Betreuer:	Prof. Dr. Reinhold Hübl
Bearbeitungszeitraum:	18.10.2022 - XX.XX.2023

Unterschrift des Betreuers: _____

Selbstständigkeitserklärung

Hiermit erkläre ich durch meine Unterschrift, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen Hilfsmittel als die angegebenen verwendet habe.

Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken – dazu gehören auch Internetquellen – als solche kenntlich gemacht habe.

Ort, Datum	Unterschrift Student

Zusammenfassung

Hier Text des Abstract in Deutsch.

Abstract

Hier Text des Abstract in Englisch.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abbildungsverzeichnis

1. Grundlagen

Diese Studienarbeit befasst sich mit dem komplexen Thema der Elliptischen Kurven in der Kryptographie. Die Kryptographie ist ein stark mathematisches Thema, bei welchem es zu Anfang der Legung einer Grundlage für das Verständnis der Inhalte dieser Studienarbeit. In diesem Kapitel werden sowohl die mathematischen als auch die kryptographischen Grundlagen zum Verständnis der in dieser Arbeit behandelten Elliptischen Kurven der Charakteristik p>3 gelegt.

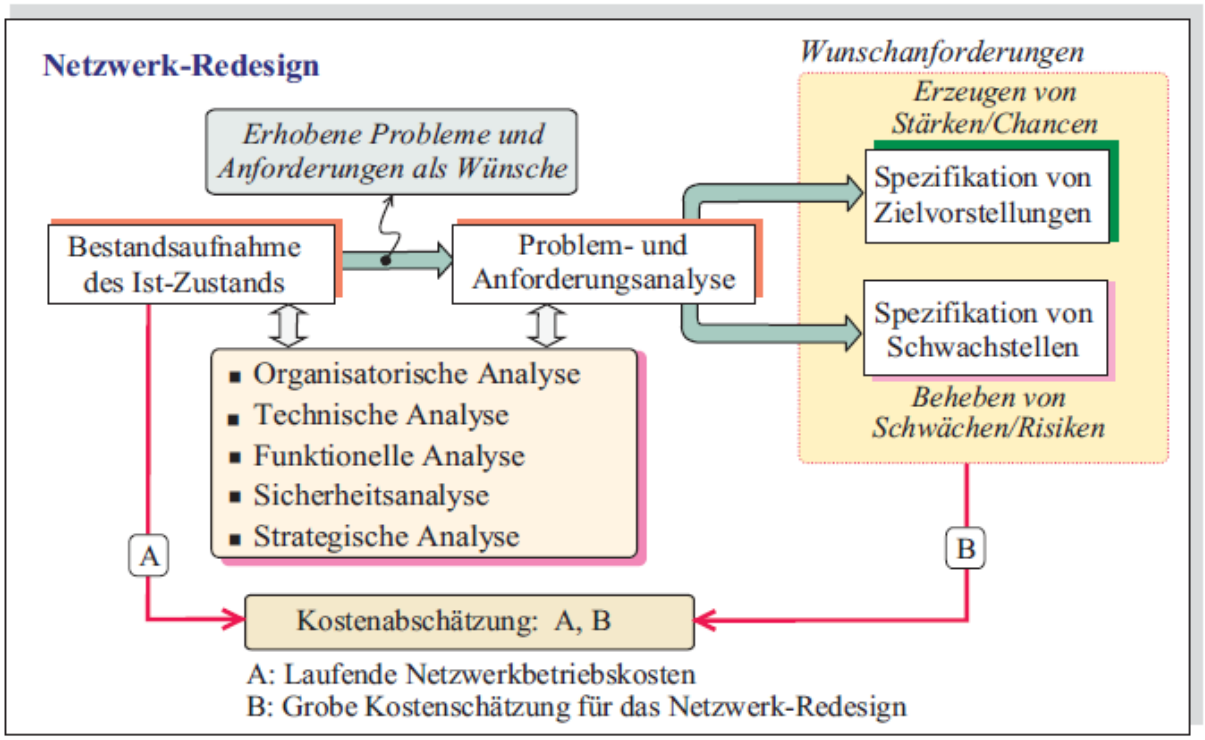

Abbildung 1.1.: Hauptaufgaben der Ist-Analyse beim Redesign einer Netzwerkinfrastruktur
Quelle: [**Berghammer.2021**]

1.1. Primzahlen

XXX

1.1.1. Definition

x

1.1.2. Eigenschaften

x

1.1.3. Bestimmung von Primzahlen

x

1.1.4. Rolle der Primzahlen in der Kryptologie

x

1.2. Algebraische Strukturen

Definiert durch die Zahlentheorie und als zentraler Untersuchungsgegenstand des mathematischen Teilgebietes der universellen Algebra, liefern algebraische Strukturen die Basis zur Realisierung komplexer symmetrischer und asymmetrischer Kryptosysteme, weshalb wir im folgenden Kapitel die Eigenschaften relevanter algebraischer Strukturen näher betrachten wollen. Darüber hinaus möchten wir Ihnen auch einige Werkzeuge zum Rechnen in der jeweiligen algebraischen Struktur an die Hand geben, welche zur späteren Realisierung von Kryptosystemen benötigt werden.

Unter einer sehr allgemeinen Betrachtung ist eine mathematische Struktur eine Liste nichtleerer Mengen, genannt Trägermengen, mit Elementen aus den Trägermengen, genannt Konstanten, und mengentheoretischer Konstruktionen über den Trägermengen. Diese sind konkret Funktionen über den Trägermengen. Im Weiteren beschränken wir uns auf den Fall einer einzigen Trägermenge, wodurch die Strukturen als homogen bezeichnet werden können.

Definition: Homogene algebraische Struktur Eine homogene algebraische Struktur ist ein Tupel $(M, c_1, \ldots, c_m, f_1, \ldots, f_n)$ mit $m, n \in \mathbb{N}$ und $n \geq 1$. Dabei ist M eine nichtleere Menge, genannt **Trägermenge**, alle c_i sind Elemente aus M, genannt die **Konstanten**, und alle f_i sind s_i-stellige Funktionen $f_i : M \to M$ im Fall $s = 1$ und $f_i : M^{s_i} \to M$ im Fall $s_i > 1$, genannt die (inneren) **Operationen**. Die lineare Liste$(0, \ldots, 0, s_1, \ldots, s_n)$ mit m Nullen heißt **Typ** oder die **Signatur**.

Laut dieser Definition muss eine homogen algebraische Struktur nicht unbedingt Konstanten enthalten, jedoch mindestens eine Operation. Das Paar $(\mathbb{N}, +)$ bildet beispielsweise eine homogene algebraische Struktur des Typs (2). Das 5-Tupel $(\mathbb{N}, 0, 1, +, \cdot)$ bildet ebenfalls eine homogen algebraische Struktur des Typs (0,0,2,2).
Algebraische Strukturen unterscheiden sich grundsätzlich durch ihren Typ. Wirklich charakterisiert werden sie aber erst durch die jeweils geltenden Axiome, d.h. bestimmte Eigenschaften, welche für die Konstanten und Operationen gefordert werden. Durch die Hinzunahme immer weiterer Axiome, entsteht eine Hierarchie immer feinerer Strukturen, an deren Anfang der Monoid steht.

1.2.1. Monoid

Definition: Monoid Eine algebraische Struktur $(M, e, \cdot)$ des Typs (0,2) heißt ein Monoid, falls für alle $x, y, z \in M$ die folgenden Monoid Aciome gelten:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$e \cdot x = x = x \cdot e$$

Gilt zusätzlich noch für alle $x, y \in M$ die Gleichung $x \cdot y = y \cdot x$, so heiß $(M, e, \cdot)$ ein **kommutatives Monoid**.
Die erste und die letzte Gleichung bilden das Assoziativ- und Kommutativgesetz ab. Durch die mittlere Gleichung wird ein neutrales Element e bezüglich der Operation gefordert, wobei sowohl die **Linksneutralität** als auch die **Rechtsneutralität** spezifiziert wird.
Beispiele für Monoide sind $(\mathbb{N}, 0, +)$, $(\mathbb{N}, 1, \cdot)$ und $(\mathbb{Z}, 0, +)$.

1.2.1.1. Gruppe

1.2.1.2. Ring

1.2.1.3. Körper

1.3. Allgemeines zur Verschlüsselung

XXX

1.3.1. Symmetrische und Asymmetrische Verschlüsselung

x

1.3.2. Diffie-Hellmann

x

1.4. Ziel der Arbeit

XXX

1.5. Geplante Vorgehensweise

XXX