Algebraische Strukturen

Thomas Markwig

http://www.mathematik.uni-kl.de/~keilen

22. Oktober 2007

Übungen

- Jede Woche ein Übungsblatt.
- Aufgaben “zu Hause” bearbeiten und zur Lösung einreichen.
- Diskutiert über Lösungsansätze und Lösungen mit Kommilitonen.
- Schreibt die gefundene Lösung selbst in Euren eigenen Worten auf.
- Übungen starten diese Woche!

Übungsgruppen

- Anmeldung zu den Übungsgruppen online via:

  https://www.mathematik.uni-kl.de:5000

- Anmeldung bis Mittwoch, 24. Oktober, 10:00 Uhr
- Bekanntgabe der Einteilung Mittwoch, ab 14:00 auf meiner Webseite
- Abgabe der Aufgaben einzeln oder in Zweiergruppen
- Mögliche Übungstermine sind im Anmeldesystem zu sehen!
- Einteilung erfolgt mittels Optimierungsprogramm, das Eure Wünsche berücksichtigt

Zählen

Übungsteilnehmer zählen!

Übungsblätter

- Ausgabe der Übungsblätter jeweils montags nachmittags
- Abgabe der Übungsblätter jeweils am folgenden Montag bis 10:00 Uhr
- Abgabe erfolgt in den Briefkasten mit dem Namen des Übungsgruppenleiters im Erdgeschoß von Gebäude 48 links neben dem Haupteingang

Leistungsnachweis

- Für die erfolgreiche Teilnahme an den Übungen gibt es eine Übungsschein.
- Voraussetzung dazu:
  - Regelmäßige *Teilnahme*, d.h. Anwesenheit in den Übungen und Abgabe von selbständig und sinnvoll bearbeiteten Aufgaben
  - Bestehen der Klausur am

    Samstag, den 9.2.08, 13:30-15:00 Uhr

Bewertung

- Die Note auf dem Schein ist die Klausurnote.
- Weicht das Klausurergebnis erheblich von den Leistungen der Übungen ab, kann die Note um eine Notenstufe gehoben werden, auch von Nichtbestehen auf Bestehen:
- Voraussetzung für das Anheben der Note ist:

  Die Aufgaben wurden erkennbar selbständig gelöst, d.h. nicht, daß die Lösung ohne Zusammenarbeit mit anderen gefunden wurde, aber sie ist verstanden und mit den eigenen Worten aufgeschrieben.
- Wo der Eindruck entsteht, daß die Lösungen überwiegend von anderen abgeschrieben wurden, wird die Note unter keinen Umständen angehoben.

Voraussetzungen

- Hörerkreis sehr inhomogen, 1.-4. Semester.
- Grundlegende Elemente der mathematischen Sprache und der Logik werden vorausgesetzt (z.B. Mengen, Abbildungen, $\exists$, $\forall$, $\Longrightarrow$, ...).
- Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ und ihre grundlegenden Eigenschaften werden als bekannt vorausgesetzt.
- Diese werden aber parallel in der ersten Woche in Grundlagen der Mathematik I genauer erläutert.

Vorlesungsskript

- Ich erstelle ein Skript zur Vorlesung.
- Jede Woche wird es um die gerade behandelten Inhalte ergänzt.
- Es wird auf meiner Webseite zum Herunterladen stehen.
- Es wird sich im Stil fundamental von der Vorlesung unterscheiden.
- Bitte teilt mir alle Fehler mit, die ihr findet!
- Bitte druckt es NICHT an der Univerisität aus!

Motivation

- Ich will mit drei Anwendungsproblemen beginnen, die mit den Methoden der Vorlesung bearbeitet werden können.
- Allerdings habe ich die Vorlesung noch nicht fertig vorbereitet, und ich garantiere nicht für alle Probleme, daß wir wirklich zu ihnen kommen.

Strichcodes

Wieso piepst die Kasse, wenn der Strichcode falsch eingegeben wird?

Strichcodes

Wieso piepst die Kasse, wenn der Strichcode falsch eingegeben wird?

Antwort: Der Strichcode ist nicht in der Datenbank.

Was kodiert ein Strichcode?

- Ein Strichcode identifiziert ein Produkt eindeutig.
- Er wird dem Produkt vom Hersteller zugeordnet, nicht vom Verkäufer.
- Der Code enthält folgende Informationen:
  - das Land, in dem der Code vergeben wurde (2-3 Ziffern)
  - der Herrsteller des Produktes (4-5 Ziffern)
  - die Artikelnummer des Herstellers (5 Ziffern)

Wieso ist er nicht in der Datenbank?

- Problem:
  - Wegen der systematischen Vergabe des Codes sind viele Codes sehr ähnlich.

Wieso ist er nicht in der Datenbank?

- Problem:
  - Wegen der systematischen Vergabe des Codes sind viele Codes sehr ähnlich.
- Lösungsansatz:
  - Füge dem Code redundante, d.h. überflüssige zusätzliche, Information an.
  - Die muß von dem forderen Teil abhängen und erkennen, wenn ein Fehler eingegeben wurde.

Wieso ist er nicht in der Datenbank?

- Problem:
  - Wegen der systematischen Vergabe des Codes sind viele Codes sehr ähnlich.
- Lösungsansatz:
  - Füge dem Code redundante, d.h. überflüssige zusätzliche, Information an.
  - Die muß von dem forderen Teil abhängen und erkennen, wenn ein Fehler eingegeben wurde.
- Erste Idee:
  - Schreibe den ganzen Code zweimal hintereinander.
  - Damit wird der Code zu lang und noch fehleranfälliger.

Lösungsansatz

- Man kommt mit einer Ziffer aus, der Prüfziffer.
- Dabei spielt die Gruppe $\mathbb{Z}_{10}$ eine wichtige Rolle.
- Ähnliche Verfahren mit verschiedensten Gruppen gibt's bei:

- ISBN-Nummern mit der Gruppe $\mathbb{Z}_{11}$
- Seriennummern auf Banknoten (DM-Scheine) mit der Gruppe $\mathbb{D}_{10}$
- Kreditkarten, Showview, Personalausweisen, ...

Kodierungstheorie

- Das obige Problem ist bekannt als Prüfziffernkodierung.
- Es ist ein Spezialfall des allgemeineren Problems, Informationen über einen störanfälligen Kanal zu schicken:

- Ziel war es lediglich, Fehler zu erkennen.
- Aber, häufig möchte die Fehler nicht nur erkennen, sondern auch gleich korrigieren.

Beispiel: CD's

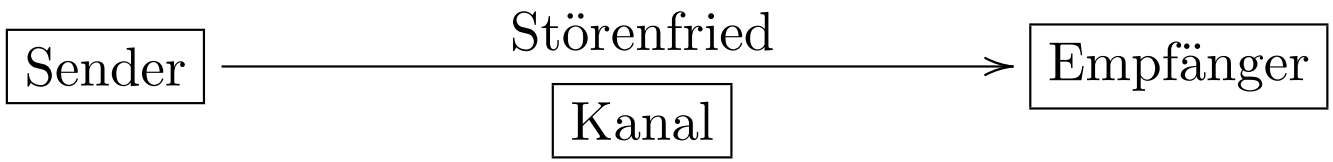
- Man kann das Abspielen von CD's in dieses Schema pressen:
  - Sender = Musikband
  - Kanal = CD + CD-Spieler
  - Empfänger = Hörer
- Erkennt man beim Strichcode einen Fehler, so scannt man ihn noch mal ein, hat die CD einen Kratzer, dann hilft auch kein nochmaliges lesen der CD!
- Kleinere Fehler sollte also wirklich korrigiert werden.
- Man braucht schnelle Verfahren!

Idee

- Information auf einer CD Blöcken fester Länge bestehend aus Nullen und Einsen gespeichert.
- Ein Block ist eine Informationseinheit, wie bei den Strichcodes ein Strichcode.
- Man muß mehr redundante Information anhängen, als nur eine Ziffer.
- Die Menge M der als fehlerfrei geltenden Blöcke muß eine zusätzliche Struktur haben:
  - lineare Codes: M ist ein Vektorraum (lineare Algebra hilft)
  - zyklische Codes: M ist ein Ideal im Polynomring (Algebra hilft)
- CD's verwenden aufwendige zyklische Codes.

Kryptographie

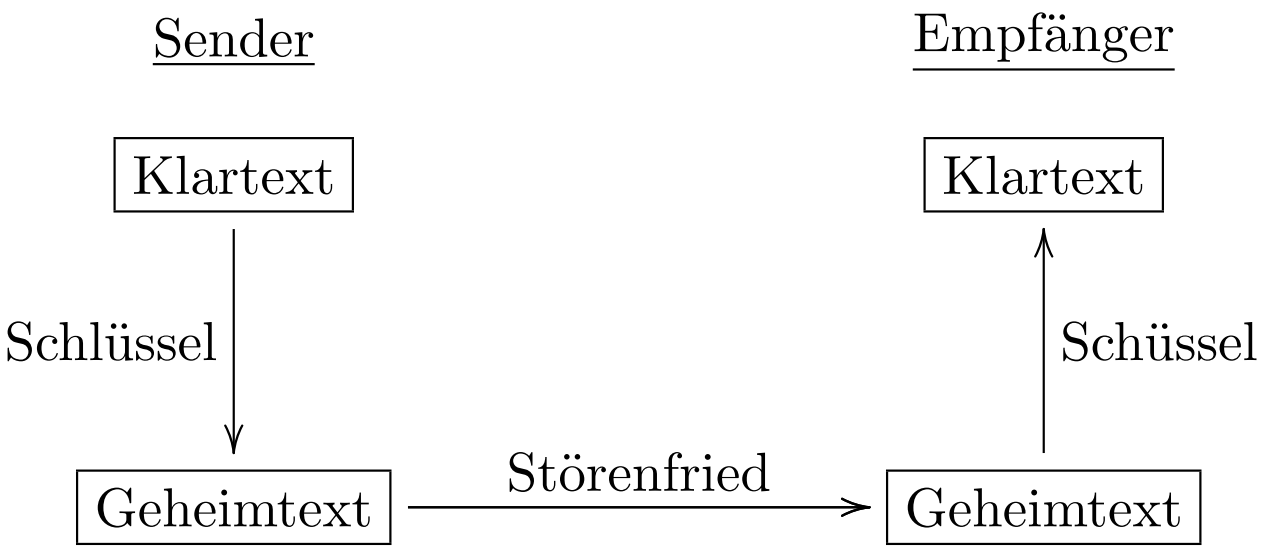
- Auch in der Kryptographie schickt man Informationen über einen störanfälligen Kanal:



- Die Störung ist hier aber ein ungebetener Störenfried.
- Es gibt zwei grudlegende Ziele:
  - die Information geheim zu halten (z.B. die eigene PIN beim Onlinebanking) oder
  - die Information vor Veränderung zu schützen (z.B. wohin das Geld überwiesen werden soll beim Onlinebanking).

Abhilfe

- Man wehrt sich dageben durch Verschlüsselung und Entschlüsselung der Nachrichten.
- Schema:



Caesar-Chiffre

- Ein simples Antikes Verfahren ist die Caesar-Chiffre.
- Buchstaben des Alphabets zyklisch verschieben, z.B.

a	b	c	d	e	$\ldots$	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$
m	n	o	p	q	$\ldots$	j	k	l

- Zum Verschlüsseln bzw. Entschlüsseln braucht man als Schlüssel nur zu wissen, um wieviele Buchstaben nach rechts verschoben wurde. In unserem Beispiel: 12.

Caesar-Chiffre

- Ein simples Antikes Verfahren ist die Caesar-Chiffre.
- Buchstaben des Alphabets zyklisch verschieben, z.B.

a	b	c	d	e	$\ldots$	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$
m	n	o	p	q	$\ldots$	j	k	l

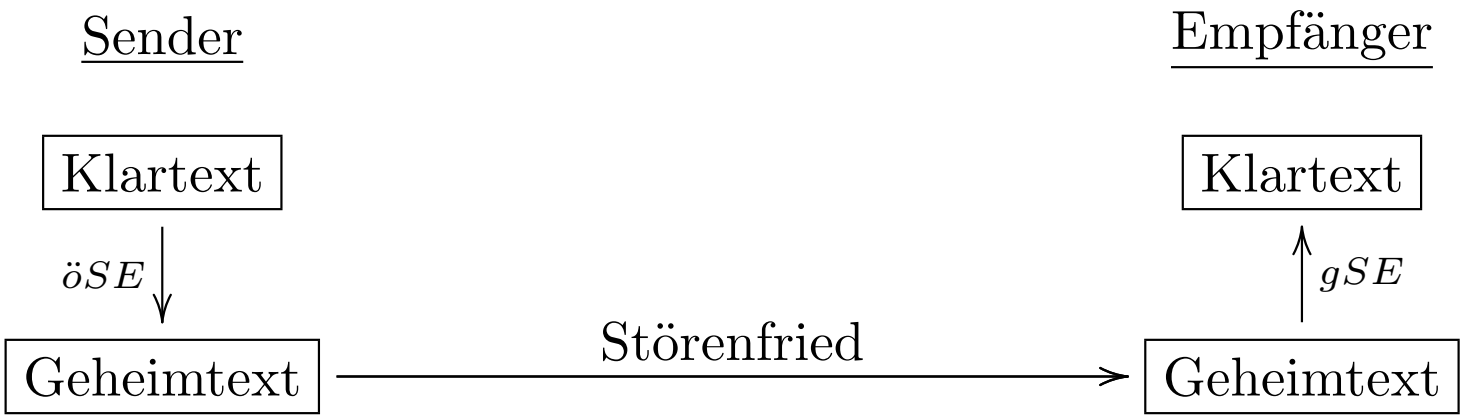
- Zum Verschlüsseln bzw. Entschlüsseln braucht man als Schlüssel nur zu wissen, um wieviele Buchstaben nach rechts verschoben wurde. In unserem Beispiel: 12.
- Problem, der Schlüssel muß geheim bleiben, also über einen sicheren Kanal ausgetauscht werden.
- Verfahren heißt symmetrisch, weil der gleiche Schüssel verschlüsselt und entschlüsselt.

Asymmetrische Verfahren

- Idee:
  - man sollte verschiedene Schlüssel zum Verschlüsseln und zum Entschlüsseln haben
  - die Kenntnis von einem sollte es nicht erlauben, den anderen zu finden
- Dann könnte jeder einen geheimen und einen öffentlichen Schlüssel haben.

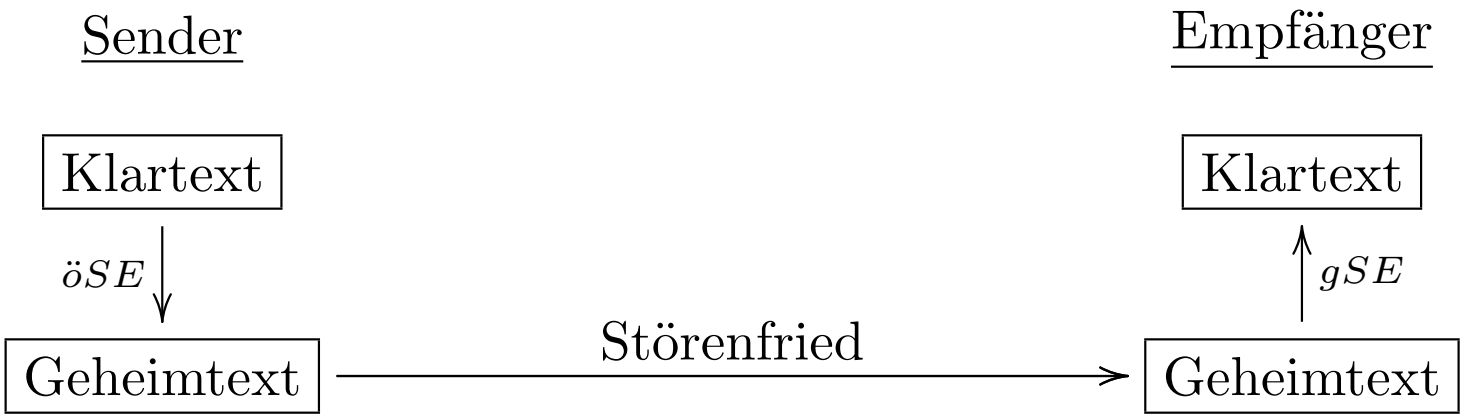
Asymmetrische Verfahren

- Nachrichten geheim verschicken:

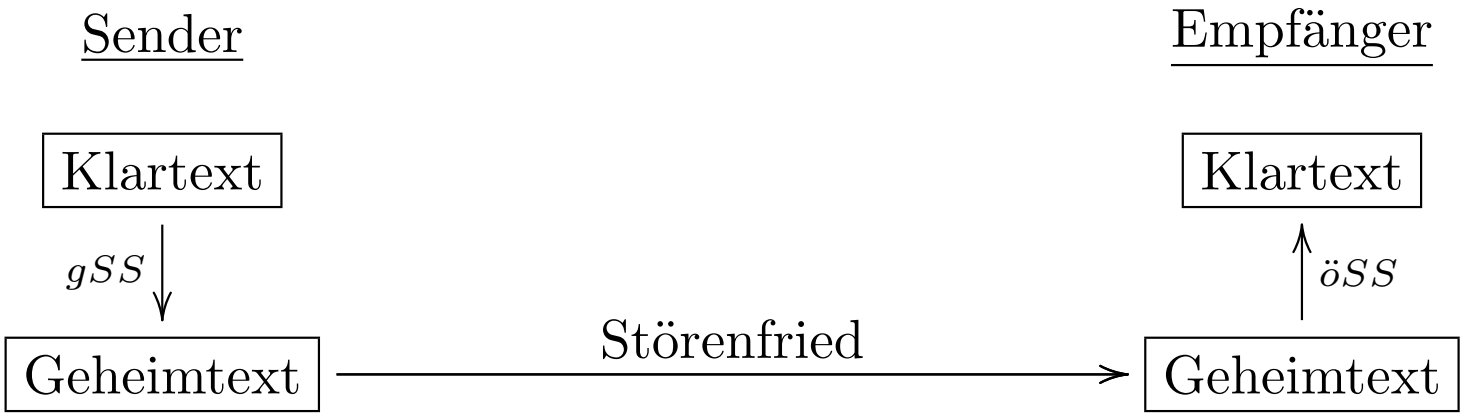


Asymmetrische Verfahren

- Nachrichten geheim verschicken:



- Nachrichten vor Veränderung schützen:



RSA-Verfahren

- Ronald Rivest, Adi Shamir und Leonard Adleman haben 1977 ein solches Verfahren gefunden.
- Man braucht als Zutaten:
  - die Primfaktorzerlegung in den ganzen Zahlen,
  - den Chinesichen Restsatz und
  - den kleinen Satz von Fermat.
- Wenn wir gut vorankommen, können wir diese in der Vorlesung zeigen.