Das CrypTool-Buch - TEXnische Details

Doris Behrendt, Bernhard Esslinger

DANTE e.V. Sommertagung 2022
Otto-von-Guericke-Universität Magdeburg

24. Juni 2022

Inhaltsverzeichnis

1 Historische Entwicklung 3

2 Was *ist* das CrypTool-Buch? 4

3 Überblick Inhalt des CTB 5

4 Statistik (kommende Version 2022) 6

5 Software 7

6 Nach Projektübernahme zuerst Hauptdatei bereinigen 9

7 Umstellung auf biblatex 13

8 Umstellung auf lualatex 18

9 Umstellung auf KOMA-Script 19

10 Arara 21

11 Formatierung unterwegs 23

12 siunitx 28

13 Code 31

14 Umbrüche in urls 42

15 Fußnoten 44

16 Floats 46

17 Zusammenführen von Englisch/Deutsch 48

18 Beschleunigen des Laufs 50

1 Historische Entwicklung

- 1998 CrypTool-Projekt (https://www.cryptool.org/de/) startete mit CT1
- 2008 zwei Nachfolge-Projekte gestartet; 2011 CT2 und JCT verfügbar
- ca. 10.000 Downloads der Desktop-Versionen (CT1, CT2 und JCT) pro Monat
- 2010 CrypTool-Online gestartet
  Grundlage klassisch HTML, CSS und JS. Die Website läuft im Client: Der Apache-Webserver liefert aus, was der Static-Site-Generator „Jekyll“ generierte. Das FrontEnd wird mit dem CSS-Framework „Bootstrap“ (v5) gestaltet. Die Funktionalität liegt in einzelnen CTO-Plugins, die meisten verwenden React. Zudem kann man nativen Code ausführen: a) Einmal über das Wasm-Web-Terminal, wenn er zu WebAssembly kompiliert wurde (mit Emscripten oder einem zu WASI kompilierenden Compiler). b) Oder durch Bibliotheken wie Pyodide, mit dann Python rein lokal im Client ausgeführt werden kann (das läuft im Hintergrund auch mit WebAssembly).
- 2010 MysteryTwister (Cipher Challenge Contest)
- Studenten aus aller Welt tragen mit ihren Arbeiten bei. Das Kernteam betreut und sorgt für Qualität und Auslieferung.

2 Was *ist* das CrypTool-Buch?

- Das CrypTool-Buch (CTB) ist ein Buch über Kryptografie. Es ist Teil des Open-Source-Projekts CrypTool (CT).
- Titel: Kryptografie lernen und anwenden mit CrypTool und SageMath
- Derzeit noch 12. Auflage 2018; neue Auflage 2022 fast fertig
- Erschien begleitend zu den Programmen des CT-Projekts: verbreitetste Lernprogramme für Kryptografie und Kryptoanalyse
- Mehr mathematische Grundlagen, tiefergehendere Behandlung der theoretischen Zusammenhänge, als in der CT-Onlinehilfe
- 1. Auflage im Jahr 2000 zusammen mit CT 1.2.01
- https://www.cryptool.org/de/documentation/ctbook/

3 Überblick Inhalt des CTB

1. Sicherheits-Definitionen und Verschlüsselungsverfahren
2. Papier- und Bleistift-Verschlüsselungsverfahren
3. Primzahlen
4. Einführung in die elementare Zahlentheorie mit Beispielen
5. Die mathematischen Ideen hinter der modernen Kryptografie
6. Hashfunktionen, Digitale Signaturen und PKIs
7. Elliptische Kurven
8. Einführung in die Bitblock- und Bitstrom-Verschlüsselung
9. Homomorphe Chiffren
10. Aktuelle Erkenntnisse zu diskreten Logarithmen, Faktorisierung und deren Praxisbezug
11. Krypto 202x Perspektiven für langfristige kryptografische Sicherheit
12. Einführung in die Gitterkryptografie

Anhänge z.B. zu SageMath, OpenSSL, ...

4 Statistik (kommende Version 2022)

- Anzahl Seiten: fast 700
- Dateigröße ca. 17 MB
- Laufzeit beim Kompilieren:
  - 8 min auf i7-9700K CPU @ 3.60GHz × 4, Ub 20.04.4 LTS
  - ca. 30 min auf i7-8550U CPU @ 1.80GHz × 4, Win 10
- Anzahl Downloads bisher: 25.000

5 Software

angeboten auf CT-Webseite: https://www.cryptool.org/de/

- CrypTool-Online (https://www.cryptool.org/de/cto/): Webseite mit Plugins zum Testen, Lernen und Entdecken von alter und moderner Kryptografie.
- CUDA-Tutorial https://www.cryptool.org/download/ctb/CTB-Chapter_CUDA_Tutorial-Cryptanalysis_of_Classical_Ciphers_Using_Modern_GPUs_and_CUDA_en.pdf
- zugehörige SageMath- und OpenSSL-Skripte https://www.cryptool.org/de/documentation/ctbook/sagemath und https://www.cryptool.org/de/documentation/ctbook/openssl
- Dokument PythonTex-by-Examples.pdf https://www.cryptool.org/download/ctb/PythonTex-by-Examples.pdf

Benutzt zur Erstellung des CTB:

- TEXLive und/oder MacTEX
- Arara
- svn
- Linkchecker https://www.topster.de/downloads/linkcheck.html

Beschrieben im CTB:

- SageMath, Jupyter
- CT1, CT2 etc.
- openssl

6 Nach Projektübernahme zuerst Hauptdatei bereinigen

- 800 Zeilen, davon mindestens (!) 373 Kommentarzeilen:

  grep -c '^[[:space]]*%' CT-Book-de.tex liefert 373 Nimmt das [[:space]] auch Tabs mit?

- inkludierte Teildateien schwer zu finden

```
582 % ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
583 %xy%%_17-01-19: Introduced LaTeX var CTBChapName to have a specific headline for the chapter bibliography
584 \renewcommand{\bibname}{Literaturverzeichnis \CTBChapName{}}  %xy%%_17-01-19:
585 \newcommand{\CTBChapName}{(Intro)}          \input{chapters/introduction.tex} % Working together of Book and Programm
586 \mainmatter % Ab hier beginnt Seitennummerierung mit arabischen Ziffern
587 \renewcommand{\CTBChapName}{(CryptoMeth)}    \input{chapters/cryptomethods.tex}
588 \renewcommand{\CTBChapName}{(Kap. PaP)}      \input{chapters/paper_and_pencil.tex}
589 \renewcommand{\CTBChapName}{(Kap. Primes)}   \input{chapters/primes.tex}
590 \renewcommand{\CTBChapName}{(Kap. NT)}       \input{chapters/numbertheory.tex}
591 \renewcommand{\CTBChapName}{(Kap. ModernCrypto)}  \input{chapters/moderncryptography.tex}
592 \renewcommand{\CTBChapName}{(Kap. DigSig)}   \input{chapters/digitalsignatures.tex}
593 \renewcommand{\CTBChapName}{(EllCurves)}     \input{chapters/ellipticcurves.tex}
594 \renewcommand{\CTBChapName}{(BitCiphers)}    \input{chapters/bitciphers.tex}
595 \renewcommand{\CTBChapName}{(Kap. HE)}       \input{chapters/homomorphicencryption.tex}
596 \renewcommand{\CTBChapName}{(DLogFact)}      \input{chapters/dlog-factoringdead.tex}
597 \renewcommand{\CTBChapName}{(Crypto2020)}    \input{chapters/crypto2020.tex}
```

- Pakete thematisch nicht geordnet; vorher:

  Zeile 180: \usepackage{color}

  Zeile 320: \RequirePackage{color}\definecolor{RED}{rgb}{1,0,0}

  nachher:

ctb2020.tex (~/ctb/trunk/ctb2020) - GVIM1

Datei Editieren Werkzeuge Syntax Puffer Ansicht TeX-Suite TeX-Environments TeX-Elements TeX-Math Hilf

```
260 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%----------index
261 \usepackage{makeidx}
262 \makeindex
263 % \makeindex[columns=3, title=Alphabetical Index] %%% TodoTodo_Nice
    -to-have-only: Alphabetzeichen als Header im Index. Tat nicht! -->
    Siehe usepackage{imakeidx}
264
265
266 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%--------graphik, farben
267 \usepackage{rotating}
268 \usepackage{graphicx} %BE_20180715
269 %% \graphicspath{{./figures/}}  %BE_2021-07-04: Worked fine for \in
    cludegraphics under Linux after adding the ending "/"
270 %%                              Could also use more than one path:
    \graphicspath{ {Pics/PDFs/} {Pics/JPGs/} {Pics/PNGs/} }
    @
```

ctb2020.tex

```
280 positioning,
281 shapes.multipart,
282 decorations,
283 decorations.pathmorphing,
284 decorations.pathreplacing,
285 quotes,
286 babel,
287 cd,
288 }
289 \tikzcdset{arrow style=tikz,diagrams={>={Stealth[length=7pt]}}}
290 %tikz l"ad xcolor!
291 \definecolor{f1}{HTML}{FFE5B9}%beige-orange
292 \definecolor{f2}{HTML}{EFF8FF}%hellgrau mit blaustich
293 \definecolor{f3}{HTML}{C9CBFF}%flieder-lila
```

- Einstellungen von Paketen vorne im Header wurden weiter hinten geändert, z. B.
  Zeile 209 Paket fullpage setzt alle Seitenränder auf 1,5 cm,
  aber
  Zeile 451 \addtolength{\footskip}{8pt}

- \newcommands:

  - über 200 Stück, viele davon garnicht benutzt, viele davon irgendwo in der Mitte einer inkludierten Datei, überschreiben sich teils gegenseitig;
  - das Rad, neu erfunden:

```
\newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}
```

  Doku amsmath:

5.2 \mod and its relatives

Commands \mod, \bmod, \pmod, \pod are provided to deal with the special spacing conventions of "mod" notation. \bmod and \pmod are available in LaTeX, but with the amsmath package the spacing of \pmod will adjust to a smaller value if it's used in a non-display-mode formula. \mod and \pod are variants of \pmod preferred by some authors; \mod omits the parentheses, whereas \pod omits the "mod" and retains the parentheses.

(5.1) $\gcd(n, m \bmod n); \quad x \equiv y \pmod b; \quad x \equiv y \mod c; \quad x \equiv y \pod d$

```
\gcd(n,m\bmod n);\quad x\equiv y\pmod b;
\quad x\equiv y\mod c;\quad x\equiv y\pod d
```

Überhaupt Mathematiksatz? How it started:

```
5644 prime to 26. Originally, plaintext and ciphertext are vectors ($P$
5645 and $C$). The encryption and decryption processes use matrix
5646 operations modulo 26: $C = P \cdot key$ $(mod$ $26)$. %Zweimal $...$-Klammer, damit Blank vor "(".
5647 %doris: unglaublich, die zeile da oben ;-) das ist ja schon so abstrus, dass
5648 %man das in die top 10 aufnehmen muss hihi
```

$$C = P * key \ (mod\ 26).$$

How it’s going:

```
operations modulo 26: $C = P \cdot \operatorname{key}
\pmod{26}$.
```

$$C = P \cdot \mathrm{key} \pmod{26}.$$

7 Umstellung auf biblatex

BibTEX? 202x? Nein.

Hinweis auf Philip Kime's Vortrag auf der Herbsttagung von Dante im Jahr 2019: https://www.dante.de/veranstaltungen/herbst2019/programm/

Vorher bibTEX, CTB gab es ja schon vor biblatex, aber bibTEXkann z. B. kein utf8/unicode.

Gewollt sind mehrere Bibliographien, und zwar eine Gesamtbibliographie und für jedes Chapter eine eigene.

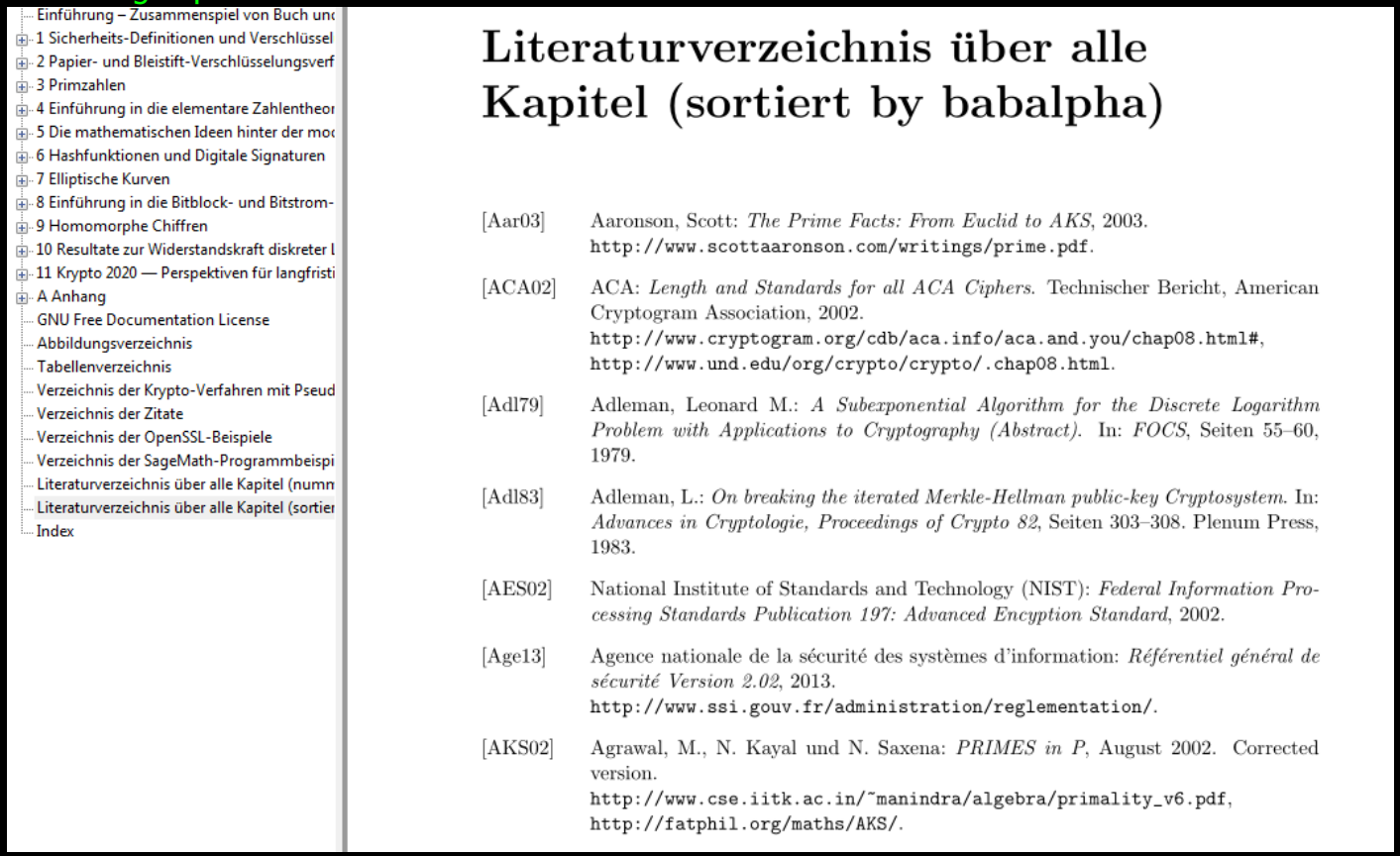
```
%im Header
\usepackage[backref,style=alphabetic,backend=biber,%
sorting=nyt,maxbibnames=99]{biblatex}
\addbibresource{references2020.bib}
. . .
%zu Beginn/am Ende eines Teilbibliographiebereichs
\begin{refsegment}
. . .
\end{refsegment}
. . .
%Gesamtbibliographie
\printbibliography[heading=bibintoc,heading=bibnumbered,
```

```
title={\iftoggle{de}{Gesamtliteraturverzeichnis}{Literature}}]
```

Außerdem nur noch eine statt bisher zwei (engl. und dt.) Dateien references∗.bib, darin Sprachunterscheidung mit \iflanguage z. B. so:

```
. . .
Note={\iflanguage{ngerman}{de blabla}{en foobar}}
. . .
```

Bibliographie vorher:



Literaturverzeichnis über alle Kapitel (sortiert by babalpha)

[Aar03] Aaronson, Scott: *The Prime Facts: From Euclid to AKS*, 2003. http://www.scottaaronson.com/writings/prime.pdf.

[ACA02] ACA: *Length and Standards for all ACA Ciphers.* Technischer Bericht, American Cryptogram Association, 2002. http://www.cryptogram.org/cdb/aca.info/aca.and.you/chap08.html#, http://www.und.edu/org/crypto/crypto/.chap08.html.

[Adl79] Adleman, Leonard M.: *A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography (Abstract).* In: *FOCS*, Seiten 55–60, 1979.

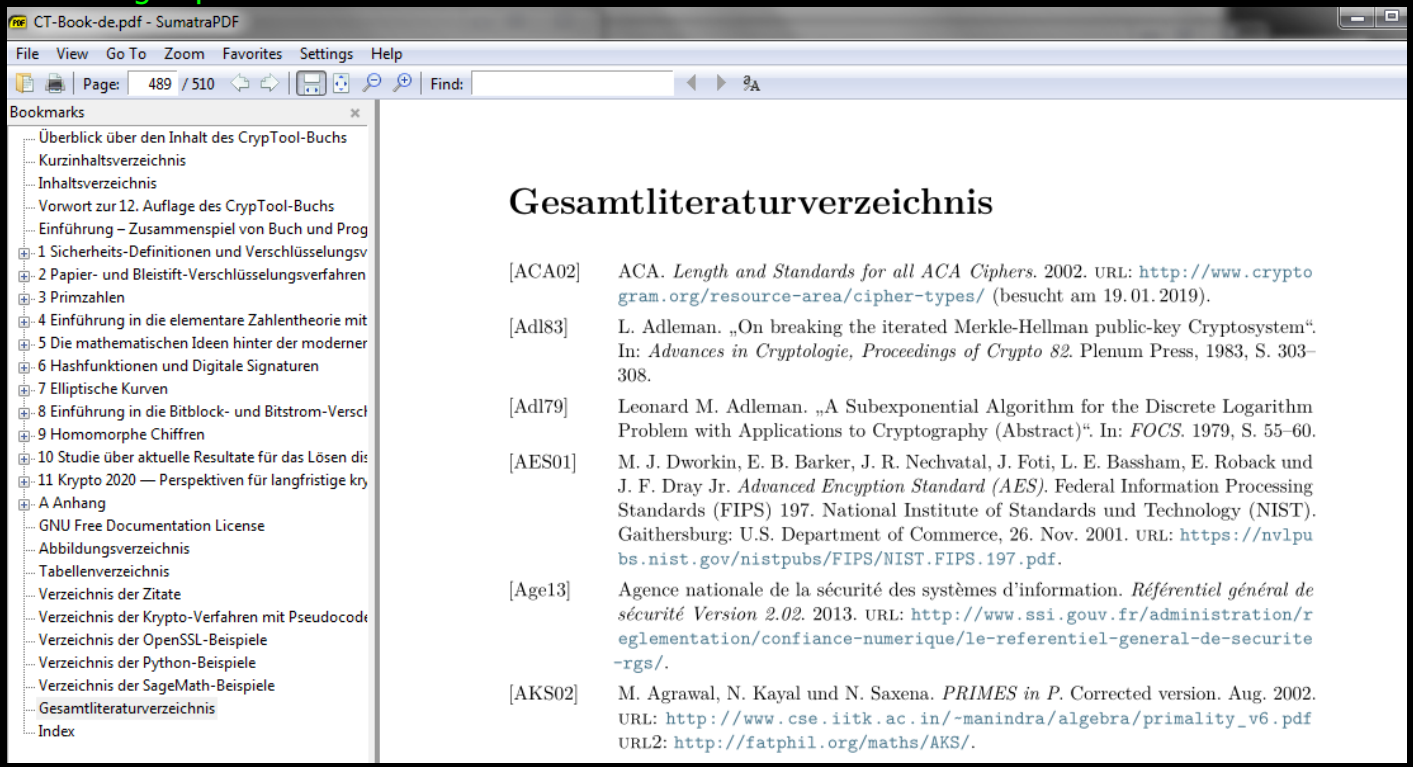
[Adl83] Adleman, L.: *On breaking the iterated Merkle-Hellman public-key Cryptosystem.* In: *Advances in Cryptologie, Proceedings of Crypto 82*, Seiten 303–308. Plenum Press, 1983.

[AES02] National Institute of Standards and Technology (NIST): *Federal Information Processing Standards Publication 197: Advanced Encyption Standard*, 2002.

[Age13] Agence nationale de la sécurité des systèmes d'information: *Référentiel général de sécurité Version 2.02*, 2013. http://www.ssi.gouv.fr/administration/reglementation/.

[AKS02] Agrawal, M., N. Kayal und N. Saxena: *PRIMES in P*, August 2002. Corrected version. http://www.cse.iitk.ac.in/~manindra/algebra/primality_v6.pdf, http://fatphil.org/maths/AKS/.

Bibliographie nachher:



Gesamtliteraturverzeichnis

[ACA02] ACA. *Length and Standards for all ACA Ciphers*. 2002. URL: http://www.cryptogram.org/resource-area/cipher-types/ (besucht am 19. 01. 2019).

[Adl83] L. Adleman. „On breaking the iterated Merkle-Hellman public-key Cryptosystem". In: *Advances in Cryptologie, Proceedings of Crypto 82*. Plenum Press, 1983, S. 303–308.

[Adl79] Leonard M. Adleman. „A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography (Abstract)". In: *FOCS*. 1979, S. 55–60.

[AES01] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback und J. F. Dray Jr. *Advanced Encyption Standard (AES)*. Federal Information Processing Standards (FIPS) 197. National Institute of Standards und Technology (NIST). Gaithersburg: U.S. Department of Commerce, 26. Nov. 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[Age13] Agence nationale de la sécurité des systèmes d'information. *Référentiel général de sécurité Version 2.02*. 2013. URL: http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

[AKS02] M. Agrawal, N. Kayal und N. Saxena. *PRIMES in P*. Corrected version. Aug. 2002. URL: http://www.cse.iitk.ac.in/~manindra/algebra/primality_v6.pdf URL2: http://fatphil.org/maths/AKS/.

Datei references-en.bib (vorher):

```
43 @Manual{AES-Standard:2002,
44   key = {AES},
45   title = {Federal Information Processing Standards Publication 197: Advanced
46   Encyption Standard},
47   year = {2002},
48   organization = {National Institute of Standards and Technology (NIST)},
49   _language = {USenglish},
50   language = {english},
51 }
```

Datei references2020.bib (nachher):

references-new.bib (~/Documents/crypto/ctb-aktuell/trunk/de) - VIM

```
 1
 2 @manual{AES-Standard:2002,
 3 sortname = {AES}, label={AES},
 4 author={M. J. Dworkin and E. B. Barker and J. R. Nechvatal and J. Foti
 5 and L. E. Bassham and E. Roback and J. F. Dray Jr.},
 6 title = {Advanced Encyption Standard (AES)},
 7 series={Federal Information Processing Standards (FIPS)},
 8 number={197},
 9 date= {2001-11-26},
10 organization= {National Institute of Standards and Technology (NIST)},
11 publisher={U.S. Department of Commerce},
12 location={Gaithersburg},
13 url={https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf},
14 }
15
```

8 Umstellung auf lualatex

Dateiencodings waren latin1; nur Umstellen in TeX/bib/etc-Datei von \usepackage[latin1]{. . .} auf \usepackage[utf8]{. . .} genügt nicht bzw. braucht man nicht (mehr);

Unicode zeitgemäß, zudem werden einige Pakete überflüssig, z.B. Paket morewrites nicht mehr gebraucht; Paket ae nicht mehr gebraucht, uvm.

Andere Fonts probieren, derzeit z.B. EB Garamond;

Nach wie vor offenes Problem: \usepackage[utf8]{luainputenc} wird immer noch gebraucht, um Umlaute in PDF Sidebar korrekt anzuzeigen bzw. wenn man es weglässt, kommt Error.

9 Umstellung auf KOMA-Script

Hat Nach- und Vorteile IMHO. Sind jetzt bei scrbook:

```
\documentclass[11pt, a4paper,
  listof=nochaptergap,
  listof=leveldown,
  \mylanguage,
  footheight=.5cm,headheight=.5cm,
  numbers=noendperiod,
  oneside, parskip=half-,
  toc=listofnumbered,toc=indexnumbered,
  toc=flat,table,x11names,%option zu xcolor
] {scrbook}
```

Insbesondere eigenes Verzeichnis für verschiedene selbst definierte Floats, hier für SageMath:

```
\DeclareNewTOC[
        counterwithin=section,
        %counterwithin=chapter,
  type = sagecode,
  types = sagecodes,
  %float,
  nonfloat,
```

```
  name = {\iftoggle{de}{SageMath-Beispiel}{SageMath Example}},
  listname = {\iftoggle{de}{Verzeichnis der
SageMath-Programmbeispiele}{List of SageMath Examples}}
]{lscfe} % lscfe = list of sagecodes fileextension
```

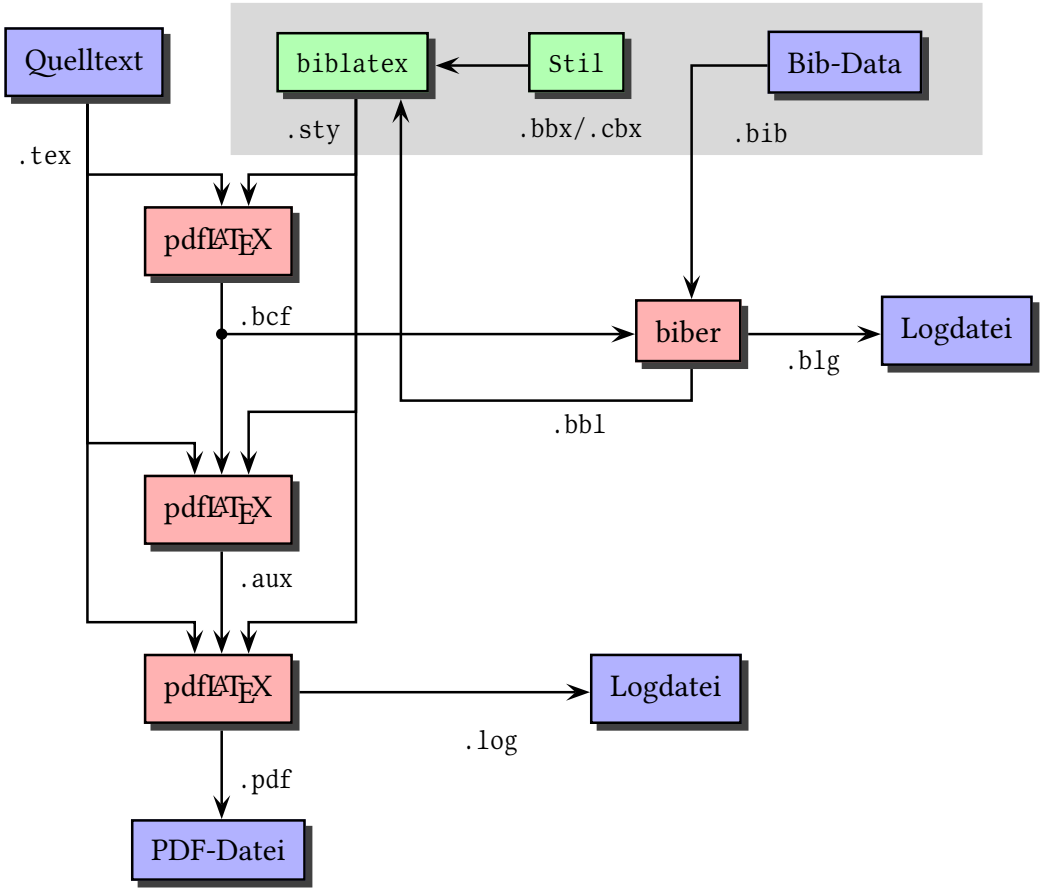
Dann Aufruf \begin{lscfe} . . . \caption{. . .}\end{lscfe} und im Anhang Erzeugung des Verzeichnisses mit \listofsagecodes.

(Floats → weiter unten nochmal)

Alle \tt , \bf etc. entfernen war viel Arbeit, außerdem gab es diverse Pakete, die sich mit KOMA offenbar nicht vertragen.

10 Arara

Man braucht mehrere Läufe, schon allein für die Literatur:



Graphik von Herbert Voß

Dazu kommt noch die Erstellung des Index. Wir nehmen arara:

```
%------------------------------------------------------- arara &co
% Build pdf via: $ arara ctb2020.tex
% arara: lualatex
% arara: biber
% arara: makeindex: {style: style.ist}
% arara: lualatex
% arara: makeindex: {style: style.ist}
% arara: lualatex
% arara: makeindex: {style: style.ist}
% arara: lualatex
% arara: lualatex
%% arara: clean:{extensions:[aux,bbl,bcf,blg,fdb_latexmk,fls,idx,
%% arara: --> ilg,ind,loc,lof,loos,lop,mw,mw.mw,
%% arara: --> out,run.xml,toc]}
% arara: halt if
% arara: --> loadObject('tada.jar',
% arara: --> 'tada.Tada').second.arara();
% arara: --> false
% ..............................................................
```

Danke an Paulo Cerada für tada.jar!

Manchmal auch TEXShop auf dem Mac:

```
% !TEX TS-program = lualatexmk
% !TEXTS-program = lualatex
% !BIBTS-program = biber
%wenn kein Leerzeichen vor TS dann inaktiv
```

11 Formatierung unterwegs

„Nur“ etwa 75 mal händisch vertikaler Abstand gesetzt:

```
1104     Details hierzu finden sich unter:
1105 \vspace{-10pt}
1106 \begin{itemize}
1107   \item[] {\url{http://www.cerias.purdue.edu/homes/ssw/cun}}
1108 \end{itemize}
1109
primes.tex
```

(b ist ungleich der Vielfachen von schon benutzten Basen wie $4, 8, 9$).

Details hierzu finden sich unter:
http://www.cerias.purdue.edu/homes/ssw/cun

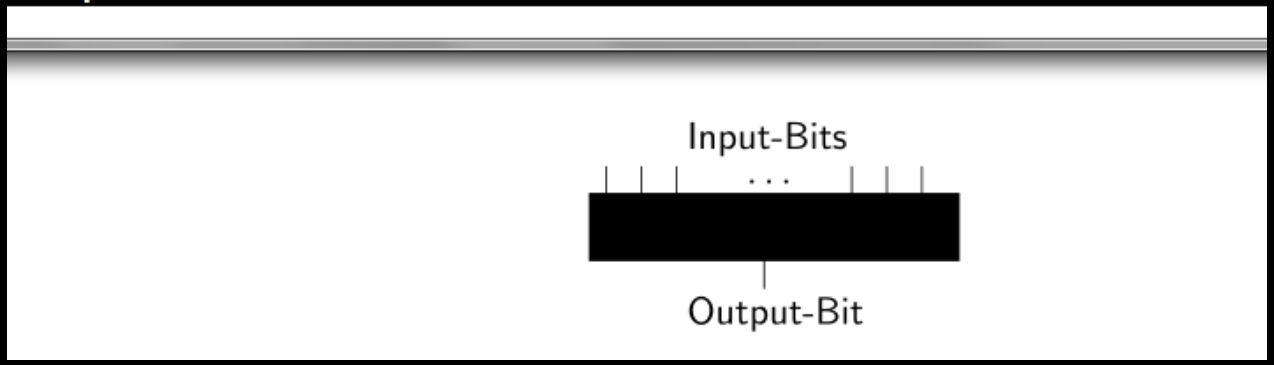
Aber auch desöfteren \\[1cm] und ähnliches.

ca. 150 Mal manuell \newpage

Best of:

```
288 Veranschaulichen kann man sich eine Boolesche Funktion durch eine
289 "`Black Box\index{Black Box}"':
290 \begin{center}
291 \begin{picture}(140,60)
292    \put(20,25){\colorbox{black}{XgXXXXXXXXX}}
293 %   \put(20,20){\framebox(100,20){$f$}}
294    \put(25,35){\line(0,1){10}}
295    \put(35,35){\line(0,1){10}}
296    \put(45,35){\line(0,1){10}}
297    \put(65,40){\ldots}
298    \put(95,35){\line(0,1){10}}
299    \put(105,35){\line(0,1){10}}
300    \put(115,35){\line(0,1){10}}
301    \put(70,20){\line(0,-1){10}}
302    \put(48,50){\sf Input-Bits}
303    \put(48,0){\sf Output-Bit}
304 \end{picture}
305 \end{center}
```

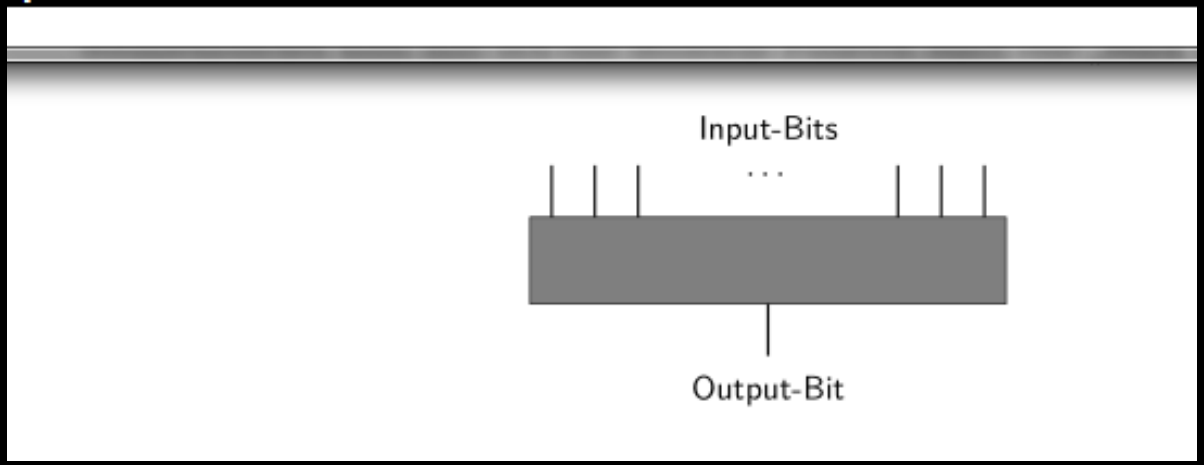
itciphers.tex



jetzt:

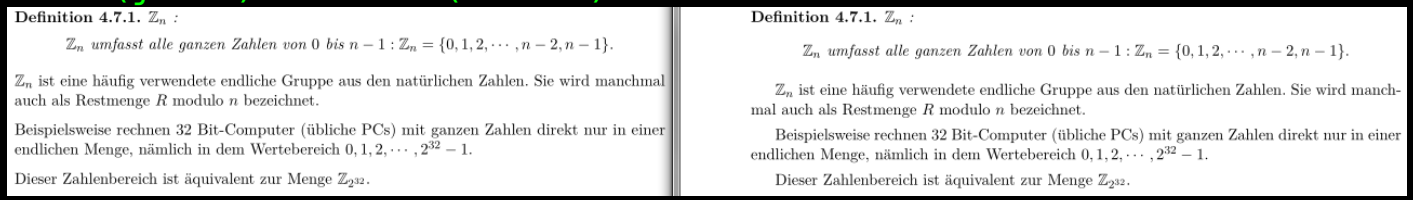
```
\begin{center}
\begin{tikzpicture}
%\draw[help lines](-3,-2)grid(3,2);
\path node [fill=black!50!white,minimum height=1cm,
minimum width=5.5cm,draw]at(0,0){};
\foreach \x in{-2.5,-2,-1.5,1.5,2,2.5}
\draw[thick](\x,.5)-- +(0,.6);
\draw[thick](0,-.5)-- +(0,-.6);
\node[]at(0,1){$\boldmath\dots$};
\node[]at(0,1.5){\textsf{Input-Bits}};
\node[]at(0,-1.5){\textsf{Output-Bit}};
\end{tikzpicture}
\end{center}
```

iphers.tex



Thema Indents:

Ohne (jetzt) vs. mit (vorher) Indents:



Definition 4.7.1. $\mathbb{Z}_n$ *:*

$\mathbb{Z}_n$ *umfasst alle ganzen Zahlen von* 0 *bis* $n-1 : \mathbb{Z}_n = \{0, 1, 2, \cdots, n-2, n-1\}$.

$\mathbb{Z}_n$ ist eine häufig verwendete endliche Gruppe aus den natürlichen Zahlen. Sie wird manchmal auch als Restmenge R modulo n bezeichnet.

Beispielsweise rechnen 32 Bit-Computer (übliche PCs) mit ganzen Zahlen direkt nur in einer endlichen Menge, nämlich in dem Wertebereich $0, 1, 2, \cdots, 2^{32} - 1$.

Dieser Zahlenbereich ist äquivalent zur Menge $\mathbb{Z}_{2^{32}}$.

Definition 4.7.1. $\mathbb{Z}_n$ *:*

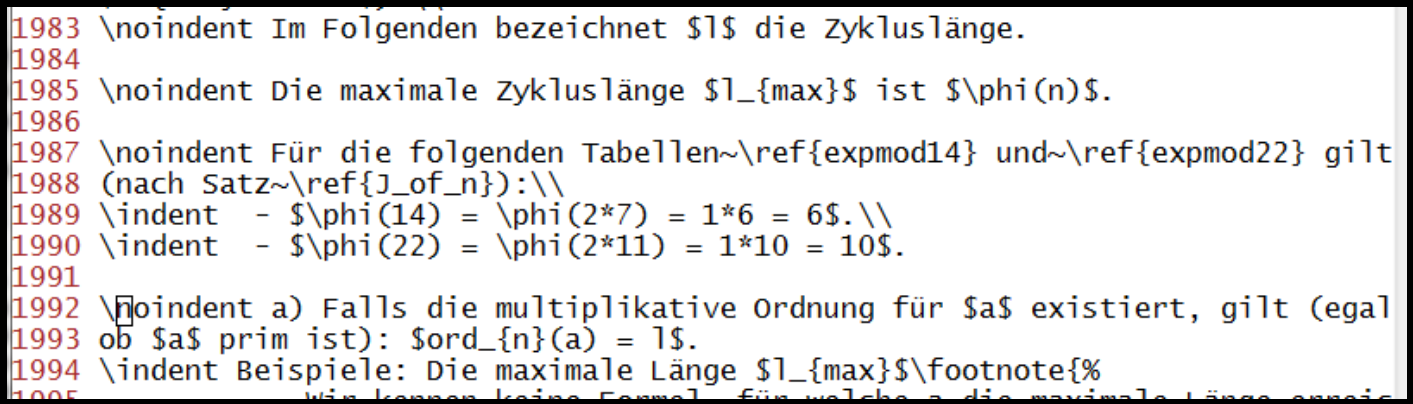
$\mathbb{Z}_n$ *umfasst alle ganzen Zahlen von* 0 *bis* $n-1 : \mathbb{Z}_n = \{0, 1, 2, \cdots, n-2, n-1\}$.

$\mathbb{Z}_n$ ist eine häufig verwendete endliche Gruppe aus den natürlichen Zahlen. Sie wird manchmal auch als Restmenge R modulo n bezeichnet.

Beispielsweise rechnen 32 Bit-Computer (übliche PCs) mit ganzen Zahlen direkt nur in einer endlichen Menge, nämlich in dem Wertebereich $0, 1, 2, \cdots, 2^{32} - 1$.

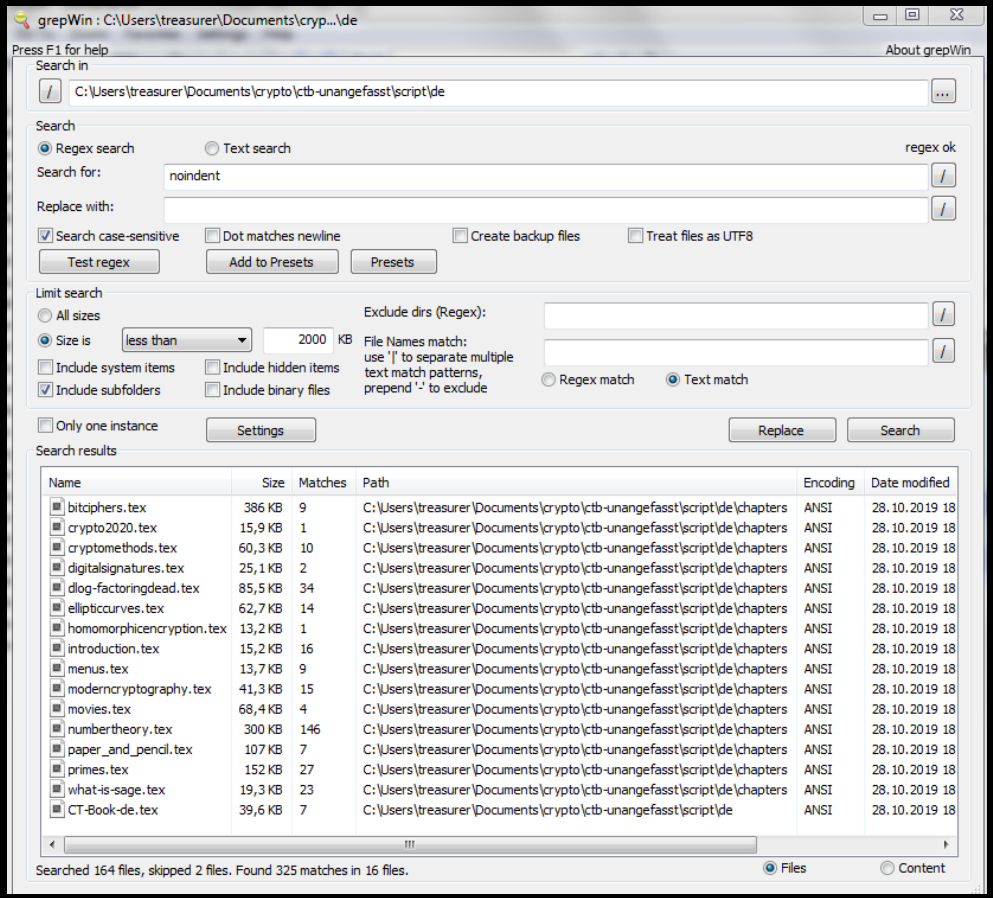
Dieser Zahlenbereich ist äquivalent zur Menge $\mathbb{Z}_{2^{32}}$.

Uns so hatte man sich „bei Bedarf“ der Indents entledigt:



```
1983 \noindent Im Folgenden bezeichnet $l$ die Zykluslänge.
1984
1985 \noindent Die maximale Zykluslänge $l_{max}$ ist $\phi(n)$.
1986
1987 \noindent Für die folgenden Tabellen~\ref{expmod14} und~\ref{expmod22} gilt
1988 (nach Satz~\ref{J_of_n}):\\
1989 \indent  - $\phi(14) = \phi(2*7) = 1*6 = 6$.\\
1990 \indent  - $\phi(22) = \phi(2*11) = 1*10 = 10$.
1991
1992 \noindent a) Falls die multiplikative Ordnung für $a$ existiert, gilt (egal
1993 ob $a$ prim ist): $ord_{n}(a) = l$.
1994 \indent Beispiele: Die maximale Länge $l_{max}$\footnote{%
```

grep lieferte 325 Treffer für \noindent :-)



Jetzt Problem gelöst mit:

```
\documentclass[..,parskip=half-,..]{scrbook}
```

12 siunitx

Insbesondere wegen \num für Formatierung langer Zahlen, aber z. B. auch für Bits und Bytes:

```
$\SI{245}{\byte}=(256-11) \si{\byte}=\SI{1960}{\bit}$ noch
        verschlüsseln, aber eine Datei der Länge
$(256-10) \si{\byte}=\SI{246}{\byte} =\SI{1968}{\bit}$
```

Für große Zahlen kann man mit siunitx z. B. den Tausendertrenner oder für Dezimalzahlen den Dezimalseparator vorgeben:

```
\usepackage{siunitx}
\sisetup{%
%binary-units=true, braucht man offb. nicht mehr
output-decimal-marker={\iftoggle{de}{,}{.}},
text-series-to-math = true,
propagate-math-font = true,
%group-separator =  default offb. im en. punkt, im dt. space
}
```

Vorher:

	Definition	Dezimalstellen	Wann	Wer
1	$2^{77.232.917} - 1$	23.249.425	26. Dez. 2017	Jonathan Pace
2	$2^{74.207.281} - 1$	22.338.618	7. Jan. 2016	Curtis Cooper
3	$2^{57.885.161} - 1$	17.425.170	25. Jan. 2013	Curtis Cooper
4	$2^{43.112.609} - 1$	12.978.189	23. Aug. 2008	Edson Smith
5	$2^{42.643.801} - 1$	12.837.064	12. Apr. 2009	Odd Magnar Strindmo
6	$2^{37.156.667} - 1$	11.185.272	6. Sep. 2008	Hans-Michael Elvenich
7	$2^{32.582.657} - 1$	9.808.358	4. Sep. 2006	Curtis Cooper/Steven Boone
8	$2^{30.402.457} - 1$	9.152.052	15. Dez. 2005	Curtis Cooper/Steven Boone
9	$2^{25.964.951} - 1$	7.816.230	18. Feb. 2005	Martin Nowak
10	$2^{24.036.583} - 1$	7.235.733	15. Mai 2004	Josh Findley
11	$2^{20.996.011} - 1$	6.320.430	17. Nov. 2003	Michael Shafer
12	$2^{13.466.917} - 1$	4.053.946	14. Nov. 2001	Michael Cameron
13	$2^{6.972.593} - 1$	2.098.960	1. Juni 1999	Nayan Hajratwala
14	$2^{3.021.377} - 1$	909.526	27. Jan. 1998	Roland Clarkson
15	$2^{2.976.221} - 1$	895.932	24. Aug. 1997	Gordon Spence
16	$2^{1.398.269} - 1$	420.921	November 1996	Joel Armengaud

Tabelle 3.2: Die größten vom GIMPS-Projekt gefundenen Primzahlen (Stand Jan. 2018)

Jetzt:

	Definition	Decimal Digits	When	Who
1	$2^{82\,589\,933} - 1$	24 862 048	Dec 7, 2018	Patrick Laroche
2	$2^{77\,232\,917} - 1$	23 249 425	Dec 26, 2017	Jonathan Pace
3	$2^{74\,207\,281} - 1$	22 338 618	Jan 7, 2016	Curtis Cooper
4	$2^{57\,885\,161} - 1$	17 425 170	Jan 25, 2013	Curtis Cooper
5	$2^{43\,112\,609} - 1$	12 978 189	Aug 23, 2008	Edson Smith
6	$2^{42\,643\,801} - 1$	12 837 064	Apr 12, 2009	Odd Magnar Strindmo
7	$2^{37\,156\,667} - 1$	11 185 272	Sep 6, 2008	Hans-Michael Elvenich
8	$2^{32\,582\,657} - 1$	9 808 358	Sep 4, 2006	Curtis Cooper/Steven Boone
9	$2^{30\,402\,457} - 1$	9 152 052	Dec 15, 2005	Curtis Cooper/Steven Boone
10	$2^{25\,964\,951} - 1$	7 816 230	Feb 18, 2005	Martin Nowak
11	$2^{24\,036\,583} - 1$	7 235 733	May 15, 2004	Josh Findley
12	$2^{20\,996\,011} - 1$	6 320 430	Nov 17, 2003	Michael Shafer
13	$2^{13\,466\,917} - 1$	4 053 946	Nov 14, 2001	Michael Cameron
14	$2^{6\,972\,593} - 1$	2 098 960	Jun 1, 1999	Nayan Hajratwala
15	$2^{3\,021\,377} - 1$	909 526	Jan 27 1998	Roland Clarkson
16	$2^{2\,976\,221} - 1$	895 932	Aug 24, 1997	Gordon Spence
17	$2^{1\,398\,269} - 1$	420 921	Nov 13, 1996	Joel Armengaud

Tab. 3.4: The largest 17 primes found by the GIMPS project (as of Apr 2022)

13 Code

Codebeispiele: Paket listings (obwohl minted auch interessant); Layout teils mit Zeilenumbruch nötig

```
\lstset{
literate=
{1}{1\allowbreak}1
{2}{2\allowbreak}1
{3}{3\allowbreak}1
```

⋮

```
\lstdefinestyle{winzig}{%
  basicstyle={\ttfamily\tiny},
  breaklines=true,
  backgroundcolor=\color{f2}
}
%
\lstdefinestyle{ssl}{% Code for OpenSSL examples
  basicstyle=\ttfamily\footnotesize,
  backgroundcolor=\color{f2}
}
```

Lange Codebeispiele aus externer Datei einlesen:\lstinputlisting

```
\begin{sslex}{Shell\iftoggle{de}{-Skript}{ script}
\texttt{hybrid-openssl-enc-dec.sh}}
{cm_opensslSample:hybridshellscript}
\lstinputlisting[style=winzig]{./code/openssl/hybrid-openssl-enc-dec.sh}
\end{sslex}
```

Sieht dann so aus:

```
# - openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -out privatekey2.pem -aes256
# - Here the pass phrase ("test") is delivered in the script itself (no prompt):
# openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -out privatekey2.pem -aes256 -pass pass:test

echo "- Look at the details of the private key file, which in openssl also contains the public values and some more ▸
 ▸values for faster calculations (output only in base64 and/or hex)"
openssl pkey -in privatekey.pem -text

echo "- Create the public key (from the private key)"
openssl pkey -in privatekey.pem -out publickey.pem -pubout

echo "- View the details of the public key (it only contains n and e as usual in maths)"
openssl pkey -in publickey.pem -pubin -text



printf "\r\n### (3) Asymmetric Encryption / Decryption with OpenSSL: Textbook RSA\n"

echo "- Encrypt a file called message.txt via RSA and public key"
openssl rsautl -encrypt -inkey publickey.pem -pubin -in message.txt -out message.txt.rsaenc

echo "- Decrypt file with the RSA and private key (privatekey.pem)"
openssl rsautl -decrypt -inkey privatekey.pem -in message.txt.rsaenc -out message.decrypted.txt

echo "- Check correctness: message.txt ?= message.decrypted.txt"
cmp -s "message.txt" "message.decrypted.txt"
CMPRESULT=$?
if [ $CMPRESULT -eq 0 ]; then
  echo "files are equal"
  cat message.txt
elif [ $CMPRESULT -eq 1 ]; then
  echo "files are not equal"
  cat message.txt
  cat message.decrypted.txt
else
```


OpenSSL Example A.7.2 ctd.

```
  echo "file cmp error"
fi
```

Alternative \begin/end{sagecommandline} aus dem Paket SageTEX: leider ungeeignet für unseren Usecase, denn:

Because of the way the environment is implemented, not everything is exactly like using Sage in a terminal: the two commands below (and the "if is prime" one above, did you notice that?) would produce some output, but don't here:

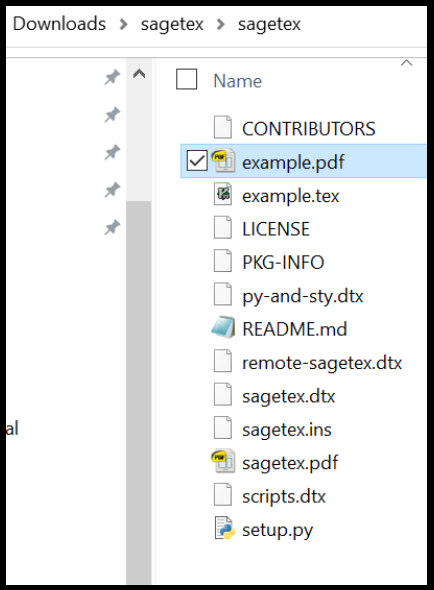
```
sage: x = 2010; len(x.divisors())
sage: print('Hola, mundo!')
None
```

The difference lies in the Python distinction between statements and expressions; we can use `eval()` for an expression and get its output, but we must use `exec` for a statement and can't get the output, if any.

Im Terminal sieht man den Unterschied:

```
sage: x=2022
sage: len(x.divisors())
8
sage: print('hallowelt')
hallowelt
```

Leider wird diese Einschränkung von sagecommandline nicht in der Doku erwähnt, sondern nur in der Datei example.pdf, die im ZIP-Ordner von CTAN geholt werden kann. https://www.ctan.org/pkg/sagetex



Im CTB gibt es nicht nur Code, sondern auch Pseudocode. Viele Pakete ausprobiert, schließlich entschieden für algpseudocodex.

```
\usepackage[italicComments=false,beginComment={},endComment={},
rightComments=false,% wirkt sich nur auf \Comment{} aus
beginLComment={},endLComment={},indLines=false]{algpseudocodex}
```

Workarounds nötig:

```
% define \dComment for use in \begin{algorithmic}; its just for changing the color of comments locally to the actual (saved) color
%see style file of algpseudocodex I took it from there and changed some stuff
\makeatletter
\algdef{SL}[LCOMMENT]{dComment}{0}[1]{%
\textcolor{saved}{#1}
\tabto{\CurrentLineWidth}% this saves current position in \TabPrevPos and fixes spacing up to here
\setlength{\algpx@tmpLen}{\dimexpr \linewidth - \TabPrevPos \relax}% set to remaining space on line
\makebox[0pt][l]{% start box here that takes no space (otherwise impacts spacing of text before)
\rule{\algpx@tmpLen}{0pt}% draw invisible rule from beginning of line until end of comment text
\algpx@commentFormat{\algpx@endLComment}% print end comment at the end
\algpx@setCodeBoxEast% since this takes 0 space, we have to set east of code box here explicitly
}}%
\pretocmd{\dComment}{\algpx@endCodeCommand}{}{}
\makeatother
%also used in pseudocode examples:
\newcommand{\dblock}[1]{\parbox[t]{.8\textwidth}{%
\begin{spacing}{1.1}
#1
\end{spacing}}\\}
```

LaTeX vorher:

```
\begin{tcolorbox}[colback=blue!9, boxrule=0mm, arc=4pt]\label{HR_Alg_LLL}
\textbf{Algorithm for LLL reduction}\\
\textbf{Input:} \hspace*{5pt}  $b_1,...,b_m \in\mathbb{R}^n$ (lattice basis), $\delta$ with $0<\delta \le 1$.\\
1. $k:=2$ (k is the stage; when entering stage k, the basis $b_1,...,b_{k-1}$ \\
\hspace*{48pt} is already LLL-reduced with $\delta$, the Gram-Schmidt coefficients\\
\hspace*{48pt} $\mu_{i,j}$ are calculated for $1\le j < i<k$ \\
\hspace*{48pt} as well as the normsquares $c_i = ||\hat{b}_i||^2_2$ for $i=1,...,k-1$)\\
2. WHILE $k\le m$\\
\hspace*{44pt} FOR $j=1,...,k-1$\\
\hspace*{70pt} $\mu_{k,j} := (b_k\cdot b_j - \sum_{i=1}^{j-1}\mu_{j,i}\mu_{k,i}c_i)/c_j$\\
\hspace*{44pt} $c_k := b_k\cdot b_k - \sum_{j=1}^{k-1}\mu_{k,j}c_j$\\
3.\hspace*{36pt} (size-reduce $b_k$)\\
\hspace*{44pt} FOR $j=k-1,...,1$\\
\hspace*{70pt} $\mu := \left\lceil\mu_{k,j}\right\rfloor$\\
\hspace*{70pt} FOR $i=1,...,j-1$\\
\hspace*{90pt} $\mu_{k,i} := \mu_{k,i} -\mu\mu_{j,i}$\\
\hspace*{70pt} $\mu_{k,j} := \mu_{k,j} - \mu$\\
\hspace*{70pt} $b_k := b_k - \mu b_j$\\
4. \hspace*{36pt} IF $\delta c_{k-1} > c_k + \mu_{k,k-1}^2 c_{k-1}$\\
\hspace*{48pt} THEN exchange $b_k$ and $b_{k-1}$\\
\hspace*{70pt} $k := max(k-1,2)$\\
```

LaTeX jetzt:

```
\begin{cproc}{
\iftoggle{de}{Algorithmus zur LLL-Reduktion}{Algorithm for
LLL reduction}}{HR_Alg_LLL}

\begin{algorithmic}[0]\onehalfspacing
\State
\textbf{input}
$b_1,\dots,b_m\in\mathbb{R}^n$
\iftoggle{de}{ (Gitterbasis)}{ (lattice basis)}, $\delta$
\iftoggle{de}{ mit }{ with }
$0\leq\delta\leq1$
\State \Comment{\iftoggle{de}{Schritt 1}{Step 1}}
\State
$k \gets 2$ \,\dblock{%besser h"andisch space dazu sieht
%besser aus, daher das \, vor \dblock; unten bei output
%braucht mans nicht, warum weiss ich nicht, evtl. weil
%fettdruck, da gr"o"ere schriftlaufweite also auch
%breiteres leerzeichen
\iftoggle{de}{%
($k$ bezeichnet die Stufe.
Bei Eintritt in Stufe $k$ ist die
Basis $b_1,\dots,b_{k-1}$ bereits
```

PDF vorher:

Algorithm for LLL reduction

Input: $b_1, ..., b_m \in \mathbb{R}^n$ (lattice basis), δ with $0 < \delta \leq 1$.

1. $k := 2$ (k is the stage; when entering stage k, the basis $b_1, ..., b_{k-1}$ is already LLL-reduced with δ, the Gram-Schmidt coefficients $\mu_{i,j}$ are calculated for $1 \leq j < i < k$ as well as the normsquares $c_i = ||\hat{b}_i||_2^2$ for $i = 1, ..., k-1$)
2. WHILE $k \leq m$
   FOR $j = 1, ..., k-1$
   $\mu_{k,j} := (b_k \cdot b_j - \sum_{i=1}^{j-1} \mu_{j,i}\mu_{k,i}c_i)/c_j$
   $c_k := b_k \cdot b_k - \sum_{j=1}^{k-1} \mu_{k,j}c_j$
3. (size-reduce b_k)
   FOR $j = k-1, ..., 1$
   $\mu := \lceil \mu_{k,j} \rfloor$
   FOR $i = 1, ..., j-1$
   $\mu_{k,i} := \mu_{k,i} - \mu\mu_{j,i}$
   $\mu_{k,j} := \mu_{k,j} - \mu$
   $b_k := b_k - \mu b_j$

PDF jetzt:

Crypto procedure 12.11.3: Algorithm for LLL reduction

input $b_1, \ldots, b_m \in \mathbb{R}^n$ (lattice basis), δ with $0 \leq \delta \leq 1$

Step 1

$k \leftarrow 2$ (k is the stage. When entering stage k, the basis $b_1, \ldots, b_{k-1}$ is already L^3-reduced with δ, the Gram-Schmidt coefficients $\mu_{i,j}$ are calculated for $1 \leq j < i < k$ as well as the normsquares $c_i = ||\hat{b}_i||_2^2$ for $i = 1, \ldots, k-1$)

Step 2

while $k \leq m$ **do**

  for $j = 1, \ldots, k-1$ **do**

    $\mu_{k,j} \leftarrow \frac{b_k \cdot b_j - \sum_{i=1}^{j-1} \mu_{j,i}\mu_{k,i}c_i}{c_j}$

  $c_k \leftarrow b_k \cdot b_k - \sum_{j=1}^{k-1} \mu_{k,j}c_j$

  Step 3 (size-reduce b_k)

  for $j = k-1, \ldots, 1$ **do**

    $\mu \leftarrow \lceil \mu_{k,j} \rfloor$

    for $i = 1, \ldots, j-1$ **do**

      $\mu_{k,i} \leftarrow \mu_{k,i} - \mu\mu_{j,i}$

    $\mu_{k,j} \leftarrow \mu_{k,j} - \mu$

    $b_k \leftarrow b_k - \mu b_j$

  Step 4

  if $\delta c_{k-1} > c_k + \mu_{k,k-1}^2 c_{k-1}$ **then**

    exchange b_k and b_{k-1}

    $k \leftarrow \max(k-1, 2)$

  else

    $k \leftarrow k+1$

offenes Problem:

wollte eigentlich Indent Lines, aber die können keinen Seitenumbruch:

3.2 indLines

possible values: `true`, `false`

default: `true`

If `true`, indent guide lines are drawn. The style of the lines can be customized as described in Section 4.1.

Example

`indLines=false`:

if $x > 0$ **then**
    $x \leftarrow x - 1$

`indLines=true`:

if $x > 0$ **then**
    $x \leftarrow x - 1$

Screenshot aus Doku von Paket algpseudocodex

14 Umbrüche in urls

How it started:

```
\usepackage[hyphens]{url} % options "hyphens" enables linebreaks nach Bindestrich in \url{}
                          % (evtl. usepackage url erst NACH usepackage hyperref?)
\appto\UrlBreaks{\do\a\do\b\do\c\do\d\do\e\do\f\do\g\do\h\do\i\do\j
\do\k\do\l\do\m\do\n\do\o\do\p\do\q\do\r\do\s\do\t\do\u\do\v\do\w
\do\x\do\y\do\z}
% Trennung in langen URLs nach jedem Kleinbuchstaben möglich (braucht manchmal zusätzlich sloopypar).
% Vgl http://tex.stackexchange.com/questions/3033/forcing-linebreaks-in-url  und \def\UrlBigBreaks{\do\/\do-\do:}
% http://tex.stackexchange.com/questions/241343/what-is-the-meaning-of-fussy-sloppy-emergencystretch-tolerance-hbadness
% --> use \sloppy
% http://golatex.de/silbentrennung-letzter-ausweg-sloppypar-t3535.html
% --> evtl. bessere Alternativen:
%        \begin{sloppypar}    ...   \end{sloppypar}
%     oder
%        \usepackage{microtype} %Sorgt für bessere Platzausnutzung der \hbox bei Umbrüchen
%        \setlength{\emergencystretch}{1em} %Sorgt für bessere Platzausnutzung der \hbox bei Umbrüchen
%
% \usepackage{breakurl}  %BE_2016Jul: War nicht nötig!
% http://www.undertec.de/blog/2011/10/latexbibtex-zeilenumbruch-in-url.html
```


[AKS02] Agrawal, M., N. Kayal und N. Saxena: *PRIMES in P*, August 2002. Corrected version.
http://www.cse.iitk.ac.in/~manindra/algebra/primality_v6.pdf,
http://fatphil.org/maths/AKS/.

[Bac84] Bach, Eric: *Discrete Logarithms and Factoring*. Technischer Bericht UCB/CSD-84-186, EECS Department, University of California, Berkeley, Juni 1984.
http://www.eecs.berkeley.edu/Pubs/TechRpts/1984/5973.html,
http://www.eecs.berkeley.edu/Pubs/TechRpts/1984/CSD-84-186.pdf.

How it’s going:

```
\usepackage{xurl}
%the following 3 counters have to be set manually, because
%biblatex does not understand xurl, but we want to avoid bad
%boxes resulting from not broken urls in the bib
\setcounter{biburllcpenalty}{1} \setcounter{biburlucpenalty}{1} \setcounter{biburlnumpenalty}{1}
```


[Age13] Agence nationale de la sécurité des systèmes d’information. *Référentiel général de sécurité Version 2.02*. 2013. URL: https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/ (cit. on pp. 416, 417).

[AKS02] M. Agrawal, N. Kayal, and N. Saxena. *PRIMES in P*. Corrected version. Aug. 2002. URL: https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf/ URL2: http://fatphil.org/maths/AKS/ (cit. on p. 179).

[Alb+19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. *The General Sieve Kernel and New Records in Lattice Reduction*. Cryptology ePrint Archive, Report 2019/089. 2019. URL: https://ia.cr/2019/089 (cit. on p. 483).

[Alf+14] W.R. Alford, Jon Grantham, Steven Hayman, and Andrew Shallue. “Constructing Carmichael numbers through improved subset-product algorithms”. In: *Math. Comp.* 83.286 (2014), pp. 899–915. URL: https://arxiv.org/abs/1203.6664 (cit. on p. 101).

[Bac84] Eric Bach. *Discrete Logarithms and Factoring*. UCB/CSD-84-186. June 1984. URL: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1984/5973.html URL2: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1984/CSD-84-186.pdf (cit. on p. 412).

15 Fußnoten

[151]- Mit dem Zahlentheorie-Lernprogramm **ZT** können Sie sehen,
a) wie Euklids Algorithmus den ggT berechnet (Lern-Kapitel 1.3, Seiten 14-19/21) und
b) wie Euklids erweiterter Algorithmus das multiplikative Inverse findet (Lern-Kapitel 2.2, Seite 13/40).
ZT können Sie aufrufen via CT1 Einzelverfahren ▷ Zahlentheorie interaktiv ▷ Lernprogramm für Zahlentheorie. Siehe auch Anhang A.5.
- In CT2 Kryptotutorien ▷ Die Welt der Primzahlen ▷ Zahlentheorie ▷ Zahlentheoretische Funktionen stehen die ff. Verfahren zur Verfügung: *Erweiterter euklidischer Algorithmus* und *Modulare multiplikative Inverse*.
- Siehe auch JCT Standard-Perspektive ▷ Visualisierungen ▷ Erweiterter Euklid / Wechselwegnahme.

Menüpfade der CT-Programme in Fußnoten: gewünscht: knappe Eingabe in TEX-File, markante und einheitliche Ausgabe im PDF

Derzeitige Lösung: benutzt ifthen, xkeyval und xstring

selfdefs.tex (~/ctb/trunk/ctb2020) - GVIM1

Datei Editieren Werkzeuge Syntax Puffer Ansicht TeX-Suite TeX-Environments TeX-Elements TeX-Math Hilfe

```
\newcommand{\wicx}[2][CTTTT]{%
%%%
% New command \wic ("Where in CT"):
% At least the optional [] and one argument kb is expected; at most the optional [] and 6 arguments ka,kb,kc,kd,ke,kf can be given.
% For the set optional value (accessed via #1) also \index is called. kc should only be there is a kb is there.
% The preset optional value "CTTTT" is just a dummy, to notice in PDF if no optional is set.
% Ist #1==CTO und kb==CTOURL, dann wird die CTO-URL ausgegeben.
% Ist #1==CTO und kb!=CTOURL, wird das kb-Argument als URL ausgegeben.
% Ist in dem optionalem Arg #1 ein Substring -NOPRINT", wird das optionale Arg. nicht ausggb.
% - The "%" after each case are necessary. If not too many blanks are added at the end.
%%%
    \begingroup
    \setkeys[zPRE]{wic}{#2}%
    %
    \ifthenelse{\equal{\cmdzPRE@wic@ka}{none}}%
      % {#1\index{#1}}%
      %% HIER ABFRAGE, ob in optionalem Arg ein -NOPRINT. Dies später noch VOR ka-Behandlung legen.
      {\IfSubStr{#1}{-NOPRINT}{}{#1\index{#1}}}%
      {#1\index{#1} \wicformat{\cmdzPRE@wic@ka~$\triangleright$}}%
    %
    \ifthenelse{\equal{\cmdzPRE@wic@kb}{none}}%
      {}%
      { % Hier darf das %-Zeichen nicht direkt dahinter sein, sonst ist nach CTO, CT1 etc kein Blank!
        % \ifthenelse{  \(\NOT 4<2 \OR 4>11\)\AND\isodd{4}  }  {A}{B}
        % \ifthenelse{\equal{\cmdzPRE@wic@kb}{CTOURL} \AND \equal{#1}{CTO}}%
        \ifthenelse{\equal{#1}{CTO}}%
          {%
            \ifthenelse{\equal{\cmdzPRE@wic@kb}{CTOURL}}%
```

16 Floats

NewDocumentEnvironment aus Paket xparse sowie Paket tcolorbox

```
%-------------------------------------sagecode und sageex
\DeclareNewTOC[
        counterwithin=section,
        %counterwithin=chapter,
  type = sagecode,
  types = sagecodes,
  %float,
  nonfloat,
  name = {\iftoggle{de}{SageMath-Beispiel}{SageMath Example}},
  listname = {\iftoggle{de}{Verzeichnis der
SageMath-Programmbeispiele}{List of SageMath Examples}}
]{lscfe} % lscfe = l sagecode fileextension

%usage: \begin{sageex}{title}{label}... or
%\begin{sageex}{title}{label}[shorttitle]
\NewDocumentEnvironment{sageex}{mmo}{%
\setlength\abovecaptionskip{0pt}
\begin{tcolorbox}[arc=0pt,
before={\bigskip\par},
after={\bigskip\par},
enhanced jigsaw, %enhanced standard jigsaw,
breakable,
bottomrule=4pt,
bottomtitle=.1em,
```

```
leftrule=0pt,rightrule=0pt,toprule=1.3pt,
boxsep=.1em,
%bottomrule at break=2pt,%no effect, interferes with jigsaw?
colframe=f3,%black!10!white,
colback=f6,%blue!4!white,
title={\IfNoValueTF{#3}%
{\captionaboveof{sagecode}{#1}\label{#2}}
{\captionaboveof{sagecode}[#3]{#1}\label{#2}}%
},
titlerule=0pt,
top=.2em,
coltitle=defaultcolor,%see selfdefs!
title after break={\tiny
\iftoggle{de}{Fortsetzung~SageMath-Beispiel}{ctd. SageMath Example}~\ref{#2}},
extras title after break={colbacktitle=black!10!white},
]}{
\end{tcolorbox}}
```

17 Zusammenführen von Englisch/Deutsch

Mit Paketen comment und/oder ifthen und etoolbox

im Header:

```
% rule of thumb: use toggle for XOR;  and use begin{de}...end{de}
% and begin{en}...end{en} for possibility to have inclusive OR or bigger blocks.
\begin{de}
  \newtoggle{de}
  \toggletrue{de}
  \usepackage[ngerman,english]{babel}
  \selectlanguage{ngerman}
\end{de}
\begin{en}
  \newtoggle{de}
  \togglefalse{de}
  \usepackage[english,ngerman]{babel}
  \selectlanguage{english}
```

```
\includecomment{de}  % Define environment de (must be done first, even if its excluded afterwards)
\includecomment{en}  % Define environment en (must be done first, even if its excluded afterwards)
\ifthenelse{\equal{\mylanguage}{ngerman}}
  {
    \newcommand{\myexclenvironlang}{\excludecomment{en}} % exclude en, if the German version is to be built
  }
  {
    \newcommand{\myexclenvironlang}{\excludecomment{de}} % exclude de, if the English version is to be built
  }
\myexclenvironlang  % Call the appropriate de/en exclusion environment
```

im Text:

```
\begin{de}
  Deutscher Text ...
```

```
\end{de}
%
\begin{en}
  English text follow here ...
\end{en}
--oder--
\iftoggle{de}{Verteilung für Lücken}{Distribution of gaps}
```

18 Beschleunigen des Laufs

Mit Paket comment nur Teildokument kompilieren:

```
\includecomment{notinmini}
\excludecomment{notinmini} % +++!!!+++ Wenn auskommentiert
%--> komplettes CTB wird erstellt und Compilieren dauert länger)
. . .
\begin{notinmini}
things that need not to be in a mwe
\end{notinmini}
things that shoud be in a mwe
```

Option draft des Pakets graphicx ausprobiert, aber produziert Error:

```
! LaTeX Error: Option clash for package graphicx.

See the LaTeX manual or LaTeX Companion for explanation.
Type  H <return>  for immediate help.
 ...

l.272 \graphicspath
                  {{./\myfigureSrc/}}
```

wieso? Wahrscheinlich banal, hatte nur noch keine Zeit, diesem Fehler nachzuspüren ...

Dateigröße einiger Graphiken verkleinern: matplotlib pgf export

Dankbar für weitere Vorschläge diesbezüglich!