Impressum

Chefredakteur (V.i.S.d.P.):
StD Dr. Ludger Humbert
Redaktion: StD Christian F. Görlich
& Fachseminare Informatik Hamm und Arnsberg
Layout: Ludger Humbert (Vorlage von Torsten Bronger)

Copyright: Für namentlich gekennzeichnete Artikel übernimmt die Autorin die Verantwortung.

SOME RIGHTS RESERVED

Der Inhalt unterliegt der ↘ creativecommons.org/licenses/by-nc-sa/2.0/de-Lizenz …

If Fase … auch im Netz (↘ humbert.in.hagen.de/iffase)
ISSN 1861-0498

If Fase

IF FASE: INFORMATIKFACHSEMINARE HAMM, ARNSBERG

Bildung
Fachseminare
Veranstaltungen
Informatiksysteme
Ausbildungsschulen

If Fase

Nr. 6 HERAUSGEGEBEN VON DER IF FASE-REDAKTION 1. Februar 2006

Termine

Mittwoch, 1. Februar 2006

Vereidigung Jahrgang 2006
11:00 Uhr
Hamm + Arnsberg

Beginn des Vorbereitungsdienstes
↘ seminar.ham.nw.schule.de

Treffen des Arnsberger Fachseminars Informatik 2006
14:35-15:25
Arnsberg: Studienseminar

Grundlegende Elemente des Fachseminars. Organisation, Vorbereitung weiterer Treffen, zur Intensivphase, …
↘ seminar.ham.nw.schule.de

Mittwoch, 1. Februar 2006

Treffen des Hammer Fachseminars Informatik 2006
nach der Vereidigung-12:30
Hamm: Studienseminar

Einweisung des 2006er Jahrgangs in die Informatiksysteme im Studienseminar - erstes Einloggen und Klärung grundlegender Fragen bzgl. der ersten Veranstaltung am Freitag.
↘ seminar.ham.nw.schule.de

Freitag, 3. Februar 2006

Einführung in die Nutzung der Informatikmittel des Seminars
9:00-16:30
Hamm: Studienseminar

Die Nutzung der Informatikmittel des Studienseminars erfolgt personenbezogen. Daher ist eine individuelle Einführung notwendig, die von den Informatikreferendarinnen der Jahrgänge 2005 und 2006 für alle anderen Referendarinnen und Lehramtsanwärterinnen individuell durchgeführt wird.
↘ www.ham.nw.schule.de/pub/bscw.cgi/d223775/InformatikmittelEinfuehrung.pdf

KurzNotiert

Logo: LBS

Aus dem am 27. Januar 2006 in Münster vorgelegten sogenannten „LBS-Kinderbarometer“ (für das Kinder zwischen neun und vierzehn Jahren in NW befragt wurden) sei folgende Meldung wiedergegeben:
Nach Ansicht der Kinder ist die „Internetkompetenz“ vorrangig Männersache: Die Väter verfügen aus Sicht von Mädchen und Jungen gleichermaßen über die größte Kompetenz in der Familie. Erst auf Rang 2 folgen die Lehrer. Auffällig ist, dass sich die befragten Jungen in Sachen Internet für kompetenter als das Lehrpersonal halten, die Mädchen sich selbst aber eher durchschnittliche Noten geben. Die Mütter werden von beiden Geschlechtern auf den letzten Platz in der Kompetenzrangliste verwiesen.
Das „LBS-Kinderbarometer“ ist eine Initiative der LBS und des NRW-Jugendministeriums. Seit 1998 werden regelmäßig Daten erhoben.

LaTeX – Teil 6: Erstellung von UML-Diagrammen (2)

In einer Reihe von Artikeln in der If Fase werden nützliche Elemente von LaTeX vorgestellt, die erprobt sind und bei der täglichen Arbeit der Informatiklehrerin eingesetzt werden.

(von Dr. Ludger Humbert) In den bisher vorgelegten sechs Teilen der Artikelserie – Ausgaben 0 … 5: ↘ humbert.in.hagen.de/iffase/Archiv – wurden Hinweise zur Installation, grundlegenden Arbeitsweisen, Quellen zu Dokumentationen, die Arbeit mit KOMA-Script, Hinweise auf PSTricks und als stärker inhaltsbezogene Elemente die Erstellung von Arbeitsblättern, Struktogrammen, Automatengrafen und einigen Elementen von UML thematisiert. In dieser Ausgabe beschäftigen wir uns mit einer weiteren Möglchkeit zur Erstellung von Diagrammen der Unified Modeling Language (UML).

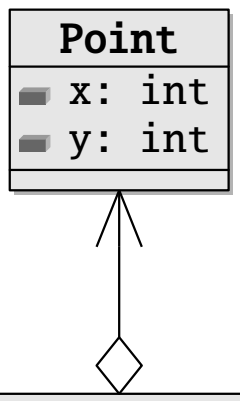
Dazu wird ein relativ junges Paket zum Einsatz gebracht, das mit Hilfe von METAPOST einfache Programmierschnittstellen für folgende Diagrammtypen zur Verfügung stellt -- *MetaUML* (↘ metauml.sourceforge.net):

- Class Diagram – Klassendiagramm
- Activity Diagram – Aktivitätsdiagramm
- State Machine Diagram – Zustandsmaschinendiagramm
- Use Case Diagram – Anwendungsfalldiagramm

Der Autor von *MetaUML* **Ovidiu Gheorghieş** hat die Möglichkeit, Sequenzdiagramme zu erstellen, bisher noch nicht eingebaut. Dieser Anforderung wird hoffentlich in einer der folgenden Versionen entsprochen.

UML-Diagramme mit METAPOST erstellen

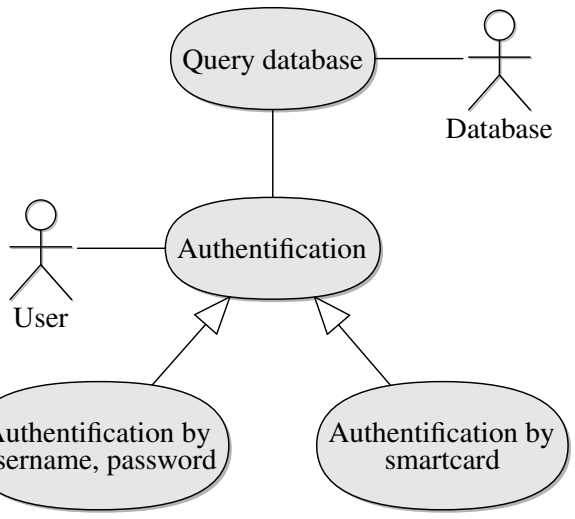
Wir verwenden hier Beispiele, die in den Materialien des Autors vorgestellt und dokumentiert werden. Die Realisierung ist an dem Gegenstandsbereich orientiert, so dass sich für die Erstellung eine objektorientierte Schreibweise geradezu anbietet.



*Klassendiagramm mit **MetaUML***

```
input metauml;
beginfig(1);
Class.A("Point")
("+x: int",
"+y: int") ();
Class.B("Circle")
("radius: int")
("+getRadius(): int",
"+setRadius(r: int):void");
A.nw = (0,0);
B.n = A.s - (0,45);
Class_draw.A;
Class_draw.B;
drawRelation(aggregationUni)(A.s -- B.n);
endfig;
end
```

Der angegebene Quellcode erzeugt das Klassendiagramm aus der Abbildung. Dabei wird deutlich, dass die Schreibweise recht intuitiv ist und eine [halb-] automatische Generierung aus Quellcode sich geradezu anbietet. Der Autor dieses Artikels hat ein einfaches Pythonprogramm geschrieben, das mit dem Standardparser `pyclbr` aus Python-Quellcode Klassendiagramme erstellt.



*Anwendungsfalldiagramm mit **MetaUML***

Quellcode für das Anwendungsfalldiagramm:

```
input metauml;
beginfig(1);
Actor.user("User");
Actor.db("Database");
Usecase.dbquery("Query database");
Usecase.auth("Authentification");
Usecase.authA("Authentification by", "username, password");
Usecase.authB("Authentification by", "smartcard");
auth.w = user.human.e + (30,0);
dbquery.s = auth.n + (0,30);
db.human.w = dbquery.e + (30,0);
authB.left - authA.right = 30;
authB.midy = authA.midy;
.5[authB.w, authA.e] = (auth.midx, auth.bottom - 50);
drawObjects(user, auth, dbquery, db, authA, authB);
clink(inheritance)(authA, auth);
...
endfig;
end
```

Von METAPOST zu PDF und SVG

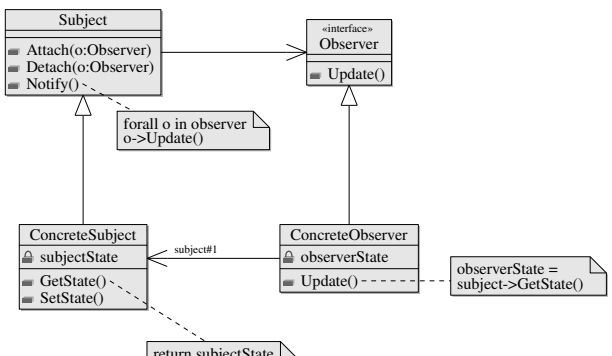
Der METAPOST-Quellcode stellt nicht das Ende, sondern den Anfang der Kette der Arbeiten dar. Um *.mp-Dateien, die programmierte Grafiken repräsentieren, in andere Formate umzuwandeln, ist als erstes `mptopdf` zu erwähnen. Damit werden aus dem METAPOST-Format PDF-Dateien erstellt. Das Werkzeug `mptopdf` ist Bestandteil üblicher tetex-Distributionen und sollte damit auf jedem LaTeX-System standardmäßig installiert sein. Der Aufruf `mptopdf usecase.mp` generiert eine oder mehrere PDF-Dateien, da eine *.mp-Quelle mehrere Abbildungen enthalten kann.

Die Werkzeuge für die Umwandlung der PDF-Datei nach *.svg setzen Elemente voraus, die kein Bestandteil von LaTeX sind: `pstoedit skconvert gzip` Im Folgenden wird die Aufrufreihenfolge angegeben, mit der aus der PDF-Datei, die oben erstellt wurde, eine *.svg-Datei erzeugt wird.

```
pstoedit -page 1 -dt -psarg "-r9600x9600" -f sk usecase-1.pdf usecase.sk
skconvert usecase.sk usecase.svg
gzip -S z --best usecase.svg
```

Für die weitere Arbeit mit diesem Paket sei neben dem Manual auf die folgenden Quellen verwiesen:

- Artikel -- **Ovidiu Gheorghieş** : An Introduction to MetaUML (↘ www.tug.org/tex-archive/graphics/metapost/contrib/macros/metauml/doc/metauml_NTG_article.pdf)
- MetaUML Library of Patterns -- UML for LaTeX/METAPOST (↘ thor.info.uaic.ro/~ogh/lop)



Wettbewerbe – Wissenschaftsjahr Informatik

Wettbewerb für Lehrer/innen

(von Dr. Ludger Humbert) Wie der Webseite der GI zum Lehrer/innen-Preis (↘ www.gi-ev.de/wir-ueber-uns/wettbewerbe/lehrerinnen-preis) entnommen werden kann, wurde im vergangenen Jahr (2005) wieder ein Lehrer/innen-Preis vergeben. Die Vergabe wurde durch die GI-Fachgruppe Informatiklehrerinnen und Informatiklehrer (ILL (↘ www.gi-informatiklehrer.de)) vorbereitet. Die Verleihung an den Kollegen *Torsten Harzer* vom Beruflichen Schulzentrum für Technik und Wirtschaft, Freiberg wurde im Rahmen der GI-Jahrestagung vom Präsidenten der GI Prof. Dr. Matthias Jarke durchgeführt. Der Kollege erhielt den Preis für seine Arbeit über „Steganographie als eine Möglichkeit zur Übermittlung von geheimen Informationen und zum Schutz vor Spionage“.
Durch den Wettbewerb soll nicht nur gezeigt werden, dass die Informatik an sich in die Schulen gehört, sondern auch deutlich werden, dass sich die GI für einen „guten“ Informatikunterricht einsetzt.

2006 – Wissenschaftsjahr Informatik

Nachdem sehr erfolgreichen Wissenschaftsjahr 2005 (Einsteinjahr) folgt das Wissenschaftsjahr 2006. ↘ einstieg-informatik.de.

Einstieg Informatik – Neues Logo

„Mit dem Projekt „Einstieg Informatik“ wollen wir die Informatik für Jugendliche allgemein verständlich darstellen und sie anregen, sich darüber hinaus mit dem Thema Informatik zu beschäftigen. Im Frühjahr 2006 werden wir unser Projekt auf Messen und überall dort, wo viele junge Leute sind, vorstellen. Das dabei verwendete Material werden wir gerne auch Dritten zur Verfügung stellen.“

„Die Grundlage für das Projekt wird ein Web-Angebot sein, auf dem wir allen Interessierten jugendgerecht aufbereitete Materialien rund um die Informatik zur Verfügung stellen.“

Wettbewerb für junge Schüler/innen

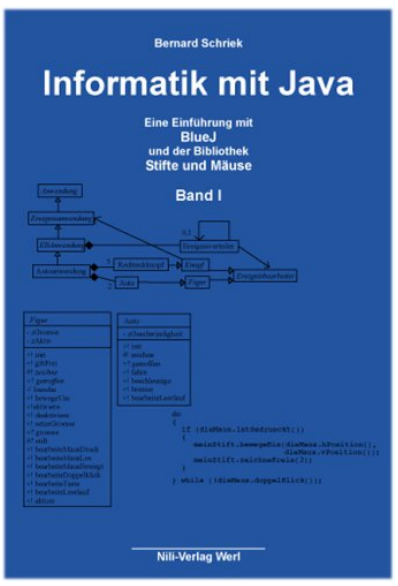
„Bei einem neuen Informatik-Wettbewerb sollen insbesondere jüngere Jugendliche in einer Online Welt Aufgaben und Problemstellungen der Informatik spielerisch begegnen.“

Bessere Lehrerbildung
dank Informatik
Fachseminar Informatik, Hamm - Partner im Wissenschaftsjahr 2006 • www.informatikjahr.de

Lesen

(von Dr. Ludger Humbert)

Schriek, Bernard : Informatik mit Java

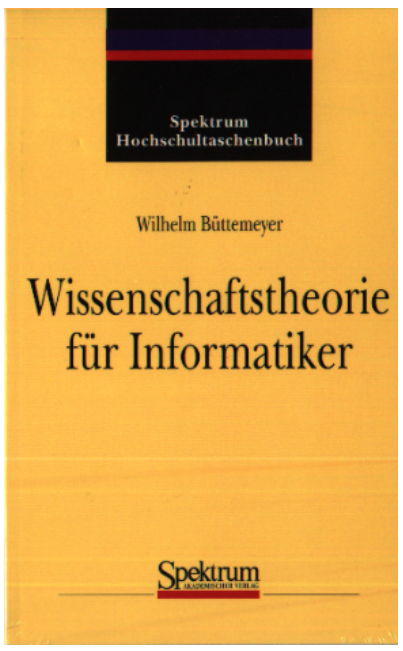


Informatik mit Java

Bernard Schriek (einer unserer Ausbildungslehrer) hat den ersten Band seiner angekündigten *Trilogie* vorgelegt. Wir brauchen Informatikbücher für die Hand der Schülerin. Meine Kritik richtet sich wesentlich auf die durch das Buch implizierte sequentielle Darstellung in Form einer „Treppe“, die nur einen Weg vorsieht. Außerdem kann die Vermischung von Werkzeugen und Konzepten zu einer unbeabsichtigten Kopplung führen. Gerade die Schülerinnen, die Schwierigkeiten mit der Komplexität der Gegenstände haben, werden dadurch m. E. möglicherweise behindert.

Trotz der Kritik empfehle ich die Anschaffung ausdrücklich.

Wilhelm Büttemeyer : Wissenschaftstheorie für Informatiker



Wissenschaftstheorie für Informatiker

Warum sollte sich eine Informatiklehrerin überhaupt mit Fragen zur Wissenschaftstheorie belasten? Warum interessiert sich die Schulinformatik für wissenschaftstheoretische Fragestellungen? Dieser von der Fachwissenschaft stark vernachlässigte Bereich birgt spannende Einsichten in die Entwicklung unserer Wissenschaft, ihrer Ziele und Methoden. Unbedingt lesen ;-)

Einsatz von Tabellenkalkulationssoftware im Mathematikunterricht

(von Ralf Greb und Markus Hufnagel) Für uns Informatiker ist es wichtig, unsere Fachkenntnis fächerübergreifend einzusetzen. Das gilt beispielsweise für den Einsatz von Tabellenkalkulationssoftware in anderen Fächern, etwa Mathematik. Die Autoren haben zu diesem Thema zwei Fortbildungsveranstaltungen durchgeführt, zum einen im Mathematikfachkollegium ihrer Schule, zum zweiten in ihrem Fachseminar Mathematik. Sie berichten in diesem Artikel von ihren Erfahrungen.

Es gibt Tabellenkalkulationssoftware verschiedener Anbieter, so z. B. Excel von Microsoft, die Tabellenkalkulation von StarOffice sowie die frei verfügbaren Tabellenkalkulationssysteme Gnumeric (Linux – Bestandteil von Gnome), innerhalb von OpenOffice oder auch KOffice (Linux – Bestandteil von KDE) und viele andere mehr. Die Autoren haben sich dazu entschieden, bei ihren Veranstaltungen einen produktunabhängigen Zugang zu wählen und die Konzepte und Funktionen vorzustellen, die exemplarisch für Tabellenkalkulationssoftware sind.

Zunächst stellte sich die Frage in welchen Jahrgangsstufen die Tabellenkalkulationssoftware Einsatz im Mathematikunterricht findet. Dies ist vor allem in den Stufen 7 und 11 der Fall. In Jahrgang 7 sieht der Lehrplan vor, dass die Schülerinnen und Schüler die Themen Zuordnungen und ihre Darstellungen, Zinsrechnung und Prozentrechnung mit Hilfe eines Tabellenkalkulationssystems vertiefen. In Stufe 11 dient die Tabellenkalkulationssoftware zur Veranschaulichung der beschreibenden Statistik.

Begonnen wurden die jeweiligen Veranstaltungen durch eine kurze Einführung in die wichtigsten Funktionen und Prinzipien der Tabellenkalkulationssoftware:

- Das Datenblatt und sein Aufbau
- Die Zelle und ihre Eigenschaften und Methoden
- Rechenvorschriften und Funktionen
- Das Prinzip des automatischen Ausfüllens
- Absolute und relative Zellenverweise
- Verschiedene Arten von Diagrammen, ihre Erstellung und ihre Eigenschaften

Wegen der unterschiedlichen Voraussetzungen und Vorkenntnisse, die die Teilnehmer an diesen Veranstaltungen mitbrachten, war es erforderlich in der praktischen Durchführung einen differenzierten Zugang zur Tabellenkalkulationssoftware anzubieten. Für Anwender mit keinen oder geringen Erfahrungen wählten wir einen Einstieg über elementare und kleinschrittige Arbeitsblätter, welche, aufeinander aufbauend, schrittweise in die grundlegenden Funktionen der Tabellenkalkulationssoftware einführen. Dies geschah unter der Verwendung von einfachen mathematischen Problemstellungen, wie der Erstellung von Tabellen und der automatischen Generierung zugehöriger Diagramme. Die fortgeschrittenen Teilnehmer aus den Fachkollegien erstellten selbständig Arbeitsblätter zur Anwendung der Tabellenkalkulationssoftware bei komplexeren mathematischen Aufgabenstellungen, wie sie etwa bei der beschreibenden Statistik auftreten.

Gute Anregungen für die Durchführung von solchen Veranstaltungen lieferte uns der Vortrag von Prof. Dr. Peter Hubwieser (TU München, Didaktik der Informatik) bei der INFOS 2005, die im Herbst in Dresden stattfand. Die Vortragsfolien finden sich unter dem URL:

- Technische Universität Dresden (↘ is11009.inf.tu-dresden.de/downloads/folien/37.pdf)

Weitere hilfreiche Hinweise liefern die Arbeitsblätter unter den URLs:

- Pädagogische Hochschule Heidelberg (↘ www.ph-heidelberg.de/wp/filler/lv2005w6/cimu/excel/Einfuehrung-EXCEL-Ablatt1.pdf)
- Pädagogische Hochschule Heidelberg (↘ www.ph-heidelberg.de/wp/filler/lv2005w6/cimu/excel/Einfuehrung-EXCEL-Ablatt2.pdf)

PGP-Verschlüsselung von E-Mails

(von Daniel Boettcher und Dr. Ludger Humbert) PGP ist die Abkürzung für **P**retty **G**ood **P**rivacy.
Es wird dargestellt, wie mit Hilfe des PGP-Verfahrens E-Mails signiert und verschüsselt werden können. Der Aufruf der PGP-Funktionen wird in das E-Mail-Programm integriert und ermöglicht so ein fließendes Arbeiten ohne Kontextbrüche. Weiterhin existieren einige graphische Oberflächen, die die Bedienung der PGP-Programme vereinfachen, welche jedoch in diesem Text nicht diskutiert werden. Die Beschreibung richtet sich an Personen, die bereits mit Unix-Systemen (i. W. Ausführen einfacher Kommandos auf Konsolenebene) vertraut sind. Für weitergehende Hinweise wird auf umfangreiche Dokumentationen im Internet verwiesen.

PGP

„*Man hat auch dann das Recht, jemandem etwas ins Ohr zu flüstern, wenn sein Ohr tausend Meilen weit entfernt ist*“ (Phil Zimmermann).

Mit dem Begriff „PGP“ wird ein Verschlüsselungsprogramm bezeichnet, das 1991 von Philipp Zimmermann veröffentlicht wurde, und bald zum Internet-Standard zählte. Zu erwähnen ist, dass die Veröffentlichung des Programms gegen die Export-Gesetze der USA verstieß und damit für einiges öffentliches Interesse sorgte. Technisch wird der RSA-Algorithmus genutzt, ein asymmetrisches Verschlüsselungsverfahren: Beim Austausch verschlüsselter Daten besitzt jeder Teilnehmer einen öffentlichen und einen privaten Schlüssel. Eine Datei (oder E-Mail) wird auf der Basis des – frei zugänglichen – öffentlichen Schlüssels des Empfänger verschlüsselt. Die Entschlüsselung ist danach nur mit Hilfe des privaten Schlüssels des Empfängers möglich. Ein großer Vorteil dieses Verfahrens ist, dass keine geheimen Schlüssel über ungesicherte Wege zwischen den Kommunikationspartnern ausgetauscht werden müssen. Zur Authentifizierung des Absenders und Sicherstellung des unveränderten Dateiinhaltes kann für eine Datei mittels des privaten Schlüssels des Absenders eine Signatur erstellt werden, die dann wiederum vom Empfänger anhand der Datei und des öffentlichen Schüssel verifiziert werden kann.

Gnu Privacy Guard (GnuPG)

Durch diverse kommerzielle Interessen bedingt, war der Quellcode zeitweise nicht öffentlich verfügbar – ein Unding für eine derart sensible Materie. So wurde (neben den weiterhin verfügbaren auch kommerziellen Lösungen) eine komplette (auch von Rechten Dritter) freie, der GPL unterliegende Neuimplementierung des Verfahrens von Werner Schmidt vorgenommen, die als Standard anzusehen ist.
Die Weiterentwicklung von GnuPG wird vom Bundeswirtschaftsministerium gefördert, das leistungsstarke Verschlüsselung der allgemeinen Öffentlichkeit zur Verfügung stellen will.

Mac – Gnu Privacy Guard (GnuPG)

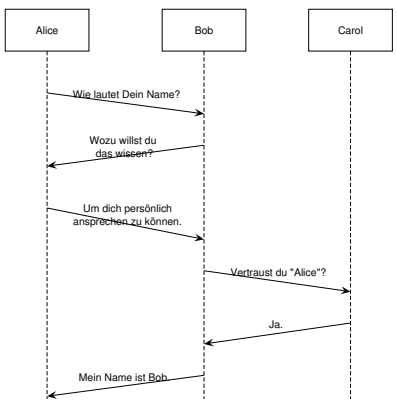
Installation und Benutzung

The GNU Privacy Guard (↘ www.gnupg.org) ist die primäre Anlaufstelle für die zur Installation notwendigen Quellen. Die bekannten Distributionen stellen Pakete zur Verfügung, die mit dem jeweiligen Paketmanagement bruchlos in die eigene Umgebung übernommen werden können. Dennoch ist es angezeigt, die Kommandozeile zu benutzen, um eine Kontrolle über die Erzeugung des privaten und des öffentlichen Schlüssels zu erhalten.

```
gpg --version # liefert die Version > 1.4.0
gpg --gen-key # Erzeugen des Schluesselpaares
$ Passphrase angeben # bitte keine Umlaute
gpg --list-keys # zeigt die Schluessel
```

Weitere Aktionen, die hier nicht mit ihren Kommandos angegeben werden.

- Export des öffentlichen Schüssels in eine Textdatei
- Öffentlichen Schüssel über einen Schlüsselserver zur Benutzung freigeben
- Beglaubigung eines [fremden] öffentlichen Schlüssels: Hierbei geht es um Vertrauen und Glaubwürdigkeit. Dies kann letztlich nur „persönlich“ geprüft werden. Dennoch ist gerade dies nicht immer möglich. Dann kann die Schlüsseldatei von einem vertrauenswürdigem Dritten signiert werden:



Prüfung durch eine dritte Person

Integration: E-Mail-Klient

E-Mail-Klienten verfügen über Schnittstellen zur Ver- und Entschlüsselung. Diese stellt Möglichkeiten bereit, um Kommandos an das oben benutzte Werkzeug weiterzureichen.

- Stephan Beyer: Der GNU Privacy Guard – Pro-Linux (↘ www.pro-linux.de/berichte/gnupg.html)
- Enigmail - Schnittstelle für Mozilla (↘ enigmail.mozdev.org)

Python – eine didaktisch geeignete Programmiersprache?

(von Dr. Ludger Humbert) Programmiersprachen, die im Unterrichtszusammenhang lernwirksam eingesetzt werden sollen, sind didaktischen Anforderungen zu unterwerfen. An Beispielen soll verdeutlicht werden, wie eine Programmiersprache offen weiterentwickelt wird und so zunehmend Anforderungen, die aus dem Ausbildungssektor kommen, konstruktiv aufnimmt.

Kriterien zur didaktischen Eignung einer Programmiersprache

In der Diplomarbeit von *Ingo Linkweiler* (November 2002) (↘ ingo-linkweiler.de/diplom/Diplomarbeit.pdf) wurde die Eignung von Python zur schnellen Softwareentwicklung geprüft. Als Nebenfrage wurden folgende Anforderungen an eine Programmierspache, die im Informatikunterricht eingesetzt werden kann, formuliert und am Beispiel von Python geprüft (vgl. Seite 85–108):

- Unterstützung unterschiedlicher Paradigmen der Programmierung
- Einfache Lesbarkeit
- Orthogonalität: einfache, klare und widerspruchsfreie Konzepte
- So einfach wie möglich: Verzicht auf Unnötiges
- Schnelle Erlernbarkeit
- Eingabehilfen bei der Implementierung
- Verfügbarkeit von Lernwerkzeugen zur Visualisierung

Python – durch Weiterentwicklung didaktische Eignung verbesern

Als Ergebnis der Prüfung ergab sich die besonders gute Eignung von Python für den Einsatz im Informatikunterricht durchaus auch im Vergleich mit anderen Sprachen (Beispiele zur Orthogonalität).

Wünsche aus Kreisen von Ausbilderinnen fanden Gehör und wurden in aktuellen Python-Versionen realisiert:

- stärkere Objektorientierung – `text.__len__()`
- boolescher Typ mit den Werten `True` und `False`

Die folgende Konstruktion funktioniert mit dem „decorator“, der ab Python 2.4 Bestandteil der Sprache ist: `@typecheck(int, str, str)` Diese Zeile – vor die Funktionsdeklaration geschrieben – sorgt dafür, dass beim Aufruf die Typen genau dieser Festlegung entsprechen. Damit wird der Fehler **TypeCheckException** (für den formalen Parameter „a“ wird explizit „int“ gefordert) bei dem folgenden Codeschnipsel erkannt und angezeigt.

```
@typecheck(int, str, str)
def meine_funktion(a, b, c): pass
meine_funktion('5', 'x', 'y')
```

Das Modul „typecheck“ ist über ↘ cheeseshop.python.org/pypi/typecheck zugänglich.