inforum

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 27, Nr. 1 – Februar 2003 ISSN 0931-4008

Inhalt

Impressum

infoWWW

ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9 – 13
48149 Münster

E-Mail: ziv@uni-muenster.de
WWW: http://www.uni-muenster.de/ZIV/

Redaktion: H. Pudlatz (G 83-31672, pudlatz@uni-muenster.de)
E. Sturm (G 83-31679, sturm@uni-muenster.de)

Satzsystem: Corel WordPerfect 8.0 für Windows 98/NT

Druck: Drucktechnische Zentralstelle der WWU
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial

E. Sturm

Diskutieren Sie auch mit Kollegen oder Kommilitonen beim Mittagessen, was Sie alles vergeblich auf Ihrem PC zu installieren versucht haben, sei es zuhause oder im Dienst?

Da wurde etwa gegen eine Bluetooth-Maus gekämpft, die partout nur installiert werden wollte, wenn schon eine normale Maus vorhanden war. Auch wurden, bis alles lief, ca. 6 verschiedene Treiber und ein Service-Pak fürs Betriebssystem benötigt. Oder ein privates Funk-LAN ließ sich erst dann konfigurieren, wenn man zunächst eine ältere Treiberversion aus dem Internet aufgespielt hatte.

Bei Software ist es ähnlich: Man kauft eine CD mit einem Programm, das kompromissunwillig zunächst QuickTime Version 4 installieren will, obwohl QuickTime 6 schon vorhanden ist und beide Versionen nicht koexistieren können.

All dies ist sicher nicht gemeint, wenn Sie im ersten Artikel aufgefordert werden, Ideen zur Weiterentwicklung der Informationsverarbeitung in Münster einzubringen. Allerdings bemüht sich das ZIV im Rahmen der eigenen Möglichkeiten, für Benutzerfreundlichkeit zu sorgen, etwa indem immer mehr Dienste über einen Browser ansprechbar sind. So finden Sie auch das Neueste von perMail in diesem i .

Dass Probleme nicht nur auf die IT beschränkt sind, können Sie im Artikel über die Baumaßnahmen im ZIV-Gebäude Einsteinstraße nachlesen, wobei ich hoffe, dass bei Ihnen nicht allzu viel Schadenfreude aufkommt. Ihr Gebäude könnte ja auch bald an der Reihe sein?!

Weitere Artikel weisen auf Produkte und Praktika im Bereich Multimedia hin. Um damit den Kreis wieder zu schließen: Zum Thema „Web-Kamera“ fällt mir natürlich ein, dass ich die erste, die ich gekauft hatte, wieder zurückbringen musste: Der Treiber ließ sich prinzipiell nicht installieren, er hatte nur den richtigen Namen, der Inhalt war undefinierbar.

Manchmal fragt man sich, was „normale“ Menschen eigentlich tun, wenn ihnen solches widerfährt. Die Antwort gab der Verkäufer, der bestätigte, dass auch bei den anderen Kameras ein identischer „Treiber“ mitgeliefert worden war: „Komisch, davon habe ich doch schon 40 verkauft!“

ZIV-Aktuell

Ideen zur Weiterentwicklung der Informationsverarbeitung?

W. Held

Wir erwarten Wünsche und Anregungen unserer Nutzer.

Die Informationsverarbeitung (IV) entwickelt sich in Münster nicht von alleine weiter. Die Experten im ZIV setzen z. B. in Abstimmung mit Gremien und IV-Versorgungseinheiten ihre Ideen um. Dafür beobachten sie weltweite Trends, die Vorhaben der anderen Hochschulen und greifen auf Empfehlungen der DFG, des Wissenschaftsrats oder des Arbeitskreises der Leiter der Rechenzentren in NRW und der Fachgruppen in der Bundesrepublik zurück, die mittelfristige Entwicklungslinien aufgezeichnet haben.

Auf Anregung des IV-Lenkungsausschusses sollen diese Experten-Pläne nun ergänzt werden um Bedürfnisse der Mitglieder unserer Universität. Studierende, Wissenschaftler/innen und die nichtwissenschaftlich Bediensteten können dazu Ihre Bedürfnisse in der IV für die nächsten 2 – 3 Jahre artikulieren und in eine Themensammlung einbringen. Sie können damit Einfluss nehmen auf die Entwicklung der IV in unserer Universität und darüber hinaus, denn gute Konzepte aus Münster findet man auch an anderen Orten wieder. Die Themen können aus allen IV-Feldern kommen. Zu denken ist z. B. an organisatorische Fragen, Rechnernetze, IV-Systeme, Anwendungen, Aus- und Weiterbildung sowie Beratung.

Wenn Sie Anregungen haben, senden Sie diese bitte bis zum 19.02.2003 an mich (✆ held@uni-muenster.de). Am Freitag, 21.02.2003, 15 Uhr soll ergänzend ein persönlicher Gedankenaustausch im Seminarraum des ZIV in der Röntgenstraße 9 – 13 stattfinden. Bitte melden Sie sich dazu an.

Das cHL-Administrationssystem OpenUSS

H. L. Grob, F. Bensberg, L. Dewanto

Die Nutzung von OpenUSS im Rahmen von cHL (computerunterstützte Hochschul-Lehre) ist inzwischen so intensiv, dass eine Übernahme in den professionellen Betrieb im ZIV erfolgen muss.

Das am Institut für Wirtschaftsinformatik entwickelte Softwareprodukt OpenUSS (*Open University Support System*) unterstützt die Administration von Lehrveranstaltungen. Die Nutzung von Diskussionsforen, Archiven und Chat-Rooms bietet die Möglichkeit, Präsenzveranstaltungen durch den Internet-Support effizienter zu machen. Gefördert wurde OpenUSS im Rahmen der Initiative CampusSource, die vom Ministerium für Schule, Wissenschaft und Forschung des Landes Nordrhein-Westfalen zum Aufbau eines Virtuellen Hochschulraums NRW initiiert wurde. Das Ziel dieser Open-Source-Initiative ist es, informationstechnologische Plattformen zur Nutzung und Weiterentwicklung auf Grundlage der Lizenzbedingungen von Open Source zur Verfügung zu stellen. Die Übergabe von OpenUSS an das ZIV stellt einen weiteren Meilenstein in der Entwicklung und Nutzung von OpenUSS dar. Weitere Informationen finden sich unter http://www.openuss.de.

TeX-Update für Unix- und Windows-Systeme

W. Kaspar

Mit diesem Update werden jetzt zum ersten Mal alle vom ZIV zentral unterstützten TeX-Implementationen (einschließlich der CD für den heimischen PC) zur gleichen Zeit auf einen neuen Stand gebracht.

Auch die neue TeX-Installation basiert wieder auf der in weltweiter Zusammenarbeit produzierten TeX-Live-CD, die hier in der Version 7 (06/2002) verwendet wurde.

Wie schon bei den vorherigen Versionswechseln sollten alle bisher verfassten (La)TeX-Dokumente auch von dieser neuen Version in unveränderter Form gesetzt werden. (Auch für ganz alte LaTeX-2.09-Dokumente stehen noch die entsprechenden Aufrufe `latex209` und `nlatex209` zur Verfügung.)

Viele der bisherigen Stile und Makros wurden in ihrer Funktionalität erweitert. Es lohnt sich also, einmal in die Dokumentation der von Ihnen verwendeten Komponenten zu schauen – vielleicht entdecken Sie eine neue Funktionalität, die Sie sich schon lange gewünscht haben.

Einen Einstieg in die Dokumentationen des TeX-Systems bietet Ihnen z. B. unsere Internet-Seite `http://www.uni-muenster.de/TeXdoc/TeXdoc.html` .

Änderungen im TeX-System

Inzwischen sind fast alle Schriftfamilien, die mit TeX mitgeliefert werden, auch als Adobe-Type-1-Schriften verfügbar. Mussten bisher von diesen Schriften für unterschiedliche Druckerauflösungen passend gerasterte PK-Fonts generiert werden, so kann jetzt nur eine Type-1-Schrift für alle Auflösungen verwendet werden. Die Voreinstellung wurde deshalb so verändert, dass `dvips` jetzt standardmäßig diese Type-1-Schriften einbindet. Gerasterte PK-Fonts werden nur noch dann verwendet, wenn keine entsprechenden Type-1-Schriften vorliegen. Sie brauchen sich also jetzt bezüglich der Schriften nicht mehr um die Auflösung des jeweiligen Ausgabegerätes zu kümmern, da Type-1-Schriften erst kurz vor dem Drucken automatisch in der gerade benötigten Auflösung gerastert werden. Es gibt allerdings auch einen kleinen Nachteil, den man sich hierbei einhandelt: Die so erzeugten PostScript-Dateien werden in der Regel etwas größer, da die Type-1-Schriften mehr Platz als die PK-Fonts benötigen. Type-1-Schriften sind aber auch bei der Erzeugung von pdf-Dateien von großer Bedeutung. Nur sie gewährleisten im Gegensatz zu den gerasterten (Type-3) Schriften eine einwandfreie Bildschirm- und Druckausgabe.

Da jetzt erheblich mehr Type-1-Schriften zur Verfügung stehen, wird sich die Qualität der von `pdflatex` erzeugten pdf-Dateien in einigen Fällen deutlich verbessern. Falls Sie z. B. in Ihren Texten die so genannten Extended-Computer-Modern-Schriften (ec-Schriften) verwenden, können Sie nun ohne Zuhilfenahme des ae-Paketes gute pdf-Dateien erzeugen, da inzwischen auch alle ec-Schriften in der Type-1-Kodierung vorliegen. Es gibt deshalb kaum noch einen Grund, nicht grundsätzlich mit den Nachfolgern der Computer-Modern-Schriften (cm-Schriften), den ec-Schriften, zu arbeiten. Um sie zu verwenden, muss nur die Zeile „`\usepackage[T1]{fontenc}`“ in den Vorspann des Dokumentes eingefügt werden.

Unix-spezifische Hinweise

Das bisherige TeX-System unter Unix (Linux, AIX, Solaris, OSF/1) wird voraussichtlich zu Beginn des Sommersemesters durch die neue Version ersetzt. Als Nutzer der zentralen Unix-Systeme brauchen Sie bezüglich dieser Umstellung nichts weiter zu unternehmen. Schon jetzt können Sie vorab mit der neuen Version arbeiten, indem Sie in Ihrer Unix-Umgebung den Befehl „`. setversiontex -neu`“ eingeben. Mit „`. setversiontex -std`“ schalten Sie wieder zur Standard-Version zurück. Falls beim Arbeiten mit der neuen Version Probleme auftreten, können Sie mit dem oben beschriebenen Befehl wieder auf die alte Version zurückschalten. Bitte vergessen Sie dabei nicht, möglichst umgehend den zuständigen Ansprechpartner im ZIV über das Problem zu informieren.

Um in einer solchen Situation auch später noch auf die alte Version zugreifen zu können,

wird diese nach der Umstellung über den Befehl „`. setversiontex -alt`“ noch für einige Zeit verfügbar bleiben. Weitere Informationen zum TeX-System unter Unix finden Sie auf unseren Internet-Seiten.

Windows-spezifische Hinweise

Wenn Sie unter Windows (95/98/ME/NT/2000/XP) bisher mit dem TeX-System auf unserem zentralen Server `wwuappl2` gearbeitet haben, können Sie das neue System nutzen, indem Sie die Verknüpfungen im Verzeichnis `\\wwuappl2\w\TeX\TeXlive-Verknuepfungen` verwenden.

Sie können alle Verknüpfungen in diesem Verzeichnis auch in einen neuen Ordner Ihres Startmenüs, den Sie z. B. `texlive` nennen, kopieren und so für eine Übergangszeit wahlweise mit der alten oder neuen Version arbeiten. Wie schon unter den Unix-spezifischen Hinweisen erwähnt, informieren Sie auch hier bitte möglichst umgehend den zuständigen Ansprechpartner im ZIV, falls beim Arbeiten mit der neuen Version Probleme auftreten sollten. Haben Sie zur Zeit ein lokales TeX-System auf ihrem PC installiert, könnten Sie, ohne ihr lokales TeX zu stören, das neue TeX-System auf unserem Server einmal ausprobieren, indem Sie entweder die soeben beschriebenen Verknüpfungen benutzen oder unsere Internet-Seiten besuchen, von denen aus Sie z. B. eine spezielle TeX-Eingabeaufforderung oder eine einfache TeX-Bedienoberfläche direkt starten können. Die einzigen Voraussetzungen hierfür sind, dass ihr PC an das zentrale Rechnernetz der Universität angeschlossen ist und dass sich der Server `wwuappl2` in Ihrer Netzwerkumgebung befindet.

Falls Sie an Ihrem häuslichen Arbeitsplatz über eine schnelle Netzanbindung (wie z. B. ADSL) verfügen, können Sie auch über diese Verbindung einen ersten Test mit unserem zentralen TeX-System unternehmen. Bitte beachten Sie in diesem Fall, dass Sie in der Regel eine zusätzliche virtuelle Verbindung (VPN) zum Rechnernetz der Universität benötigen, um auf den Server `wwuappl2` zugreifen zu können.

Wenn Sie mit diesem zentralen System alle ihre TeX-Arbeiten erledigen könnten, brauchten Sie sich in Zukunft um die Beschaffung, Installation und Wartung eines TeX-Systems nicht mehr zu kümmern.

Vor allem in PC-Pools empfiehlt es sich, dieses zentral gepflegte TeX-System einem lokal installierten vorzuziehen. Für die Anpassung an die jeweilige System-Umgebung des Pools (wie z. B. der Vorgabe von Home-Verzeichnissen und Laufwerksbuchstaben) gibt es schon jetzt Einstellmöglichkeiten, die bei Bedarf aber auch noch erweitert werden können.

Für Anwender, die das zentral installierte TeX-System nicht nutzen können, steht wie bisher eine Installations-CD zur Verfügung.

Weitere Informationen zum TeX-System für Windows – insbesondere zum Übergang auf die neuen Versionen der WinTeXShell bzw. von WinEdt – finden Sie auf unseren Internet-Seiten. Diese erreichen Sie über die Leitseite des ZIV unter „Software“ in der Rubrik „Service“.

Bei Fragen und Problemen zum TeX-System wenden Sie sich bitte an mich (✆ `kaspar@uni-muenster.de`, G 0251/83-31673).

Multimedia-Praktikum „Bildgewinnung und Darstellung“

H.-W. Kisker

Jetzt geht’s los …
(Mein Lieblingslöwe, siehe TeX)

Teil 1 Das Praktikum

Für die Durchführung des Praktikums werden 5 Gruppen zu je 3 Personen gebildet (in der Vorbesprechung). Jede Gruppe beschäftigt sich einen Tag lang mit einem der fünf Themenkreise:

- Scanner und Drucker
- Dia-Scanner und Still-Video-CD
- Digitale Kamera und Bildschirmschau
- Video-Kamera und DVD
- Video-Konferenz, WebCam und Web-Seite

Am Ende der Woche hat jede Gruppe jedes Thema behandelt. Das Praktikum ist ganztägig. Vormittags werden im CIP-Pool 3 die Experimente und Messungen unter Anleitung durchgeführt. Am Nachmittag wird in selbständiger Arbeit die Dokumentation (Praktikumsbuch) gepflegt und Material für den kommenden Tag gesammelt. Hierzu werden je nach Thema entsprechende Geräte zur Verfügung gestellt.

Teil 2 Die Web-Vorlesung

Während der Praktikumswoche verbleibt keine Zeit für erläuternde Einführungen. Deshalb ist dem Praktikum eine anwesenheitsfreie Vorlesung vorgeschaltet. Unter der Adresse

`http://Winkiosk.uni-muenster.de/MMr1/Vorlesung.htm`

werden, beginnend mit dem 3. März, nach und nach Artikel erscheinen, die der Vorbereitung des Praktikums dienen. Hintergrundartikel werden hier ebenso zur Verfügung stehen wie Beschreibungen von Geräten und Arbeitsabläufen. Ich erwarte, dass die Teilnehmer des Praktikums diese Anleitungen bis zum Beginn des Praktikums durchgearbeitet haben. (✆ `kisker@uni-muenster.de`, G 31651)

Kenndaten

Anwesenheitspraktikum:	24.3. – 28.3.2003 ganztägig
Vorbereitende Web-Vorlesung:	3.3. – 21.3.2003
Web-Server (ab sofort):	`http://Winkiosk.uni-muenster.de/MMr1`
● Mailing-Liste (ab 3.3.2003):	`MMr1@uni-muenster.de`
● Vorbesprechung:	21.3.2003 um 11 Uhr im CIP-Pool 3
Ort:	Zentrum für Informationsverarbeitung Einsteinstr. 60 CIP-Pool 3
Anzahl der Teilnehmer:	15 (werden nach Anmeldung benachrichtigt)
Anmeldung über die Web-Seite:	`http://www.uni-muenster.de/ZIV/zivlehre.html`

Zum Fortgang der Baumaßnahme Einsteinstr. 60

H. Pudlatz

Ja, mach nur einen Plan
Sei nur ein großes Licht!
Und mach dann noch 'nen zweiten Plan.
Geh' n tun sie beide nicht.

Brecht:
Die Dreigroschenoper

Der Titel dieses Beitrags ist nicht doppeldeutig gemeint, obwohl solch spontane Formulierungen unterbewusste Befürchtungen eines Betroffenen zu enthüllen scheinen.

Pläne für den Ausbau des vormaligen Universitätsrechenzentrum sind bekanntlich schon drei Jahre nach der Errichtung des Gebäudes im Jahr 1967 geschmiedet worden, war das Haus doch (damals sehr großzügig) zwar für die Unterbringung des Transistorrechners Zuse Z23 konzipiert worden, aber schon für die tatsächlich darin untergebrachte IBM-Anlage System /360-50 zu klein. Wie gesagt: geplant wurde danach an einem Neu- oder Erweiterungsbau wahrlich mit über 30 Jahren lange genug, und es waren nicht nur zwei Pläne, die „nicht gingen".

Nach Übernahme der Aufgaben des ehemaligen „Staatshochbauamts II für die Universität Münster" durch den „Bau- und Liegenschaftsbetrieb NRW" (BLB) wurden die notwendigen Umbaumaßnahmen seit Anfang August 2002 endlich in die Wege geleitet (Baunummer 1480 1140). Wegen inzwischen massiv geschrumpfter Hardware war zwar der ursprüngliche Planungszweck hinfällig geworden. Das Gebäude war einfach „auf" und musste den Anforderungen eines modernen Dienstleistungsbetriebs angepasst werden.

Leider erwies sich die Realisierung der Planung als Operation „am lebenden Objekt", denn Service und Betrieb sollten trotz Umsetzung von Wänden, Auswechslung der versifften Fassadenfenster und Verlegung der Toiletten möglichst reibungslos weitergehen. Ein Fehler, den der BLB bei der Renovierung des Regierungspräsidiumsgebäudes am Domplatz dem Vernehmen nach vermeiden will: hier wird erst ein Ausweichgebäude hergerichtet.

Der aktuelle, mir bekannte Plan ging von einer Fertigstellung unserer Baumaßnahme in der 47. Kalenderwoche des vergangenen Jahres aus. Aber wer konnte im Sommer schon ahnen, dass die gelieferten neuen Fensterrahmen nicht zum vorhandenen Kern passten, die ein Versetzen der Wände im Inneren erforderlich machten. Das war aber nur einer der Gründe für die derzeitigen Verzögerungen. Warum Handwerker es nicht schaffen zügig Hand in Hand zu arbeiten, können nur diejenigen mit Achselzucken quittieren, die jemals selbst ein Haus gebaut haben. Es scheint wohl eine Art Gesetzmäßigkeit zu sein. Murphy lässt grüßen!

Blauäugig wie wir waren, haben wir – ausgehend von dem Fertigstellungstermin November 2002 – einige Lehrveranstaltungen in den renovierten ZIV-Pools angeboten, die aber leider abgesagt werden mussten, weil zu diesem Zeitpunkt die Räume nur nach Übersteigen von Bauschutt erreichbar waren, wobei irgendwo ein Lehrling im Rhythmus der Pop-Musik aus einem Kofferradio sein Werk verrichtete oder plötzlich ein Presslufthammer einsetzte – anscheinend das wichtigste Werkzeug bei der Umgestaltung eines „Altbaus", das wohl noch bis kurz vor Schlüsselübergabe benötigt werden wird.

Wir möchten um Verständnis bitten, dass die genannten Veranstaltungen nicht nachgeholt werden können, da bereits die nächsten Termine für die Ferienkurse ins Haus stehen. So können wir nur hoffen, dass wenigstens diese planmäßig abgehalten werden können.

Immerhin aber kann doch viel Positives vom Fortgang der Maßnahme berichtet werden:

- Nach Erneuerung der Fensterrahmen und der wärmeisolierenden und lichtdämmenden Fenster macht das Haus dank der farbigen Füllungen inzwischen einen un-

erwartet fröhlichen Eindruck mit einem gewissen Wiedererkennungswert: Das ZIV: ach ja, das ist doch der bunte Kasten neben dem grauen Mathematikgebäude.

- Der ZIV-Pool 4 ist inzwischen fertiggestellt, wenn auch der ZIV-Pool 1 seit Wochen auf den neuen Bodenbelag und die Verkabelung wartet.
- Die Drucker konnten wieder in den umgestalteten Maschinenraum zurück verlegt werden, und auch für einen neuen schnellen Posterdrucker ist noch genug Platz da.
- Die Ausgabefächer im Kirschbaum-Look sind (in der Nähe der Drucker!) installiert und auch für die Posterrollen sind dazu passende Behälter vorhanden.
- Die Rechner zur Netzsteuerung haben einen angemessenen Bereich im Maschinenraum erhalten, womit auch gleichzeitig die unbehinderte Wartung des Netzes möglich wird.
- Der neue Service-Schalter – für unsere Nutzer an gewohnter Stelle im Erdgeschoss untergebracht – ist nun mit einer integrierten Klingel und einer Milchglasscheibe versehen.
- Und auch im verkleinerten Maschinenraum wurde ein großes schmales Fenster für den Einfall von Tageslicht nachgerüstet. Honi soit qui mal y pense!

Der Eingangsbereich und der behindertengerechte Zugang samt vergrößertem Fahrstuhl sollen Ende Februar fertig gestellt sein. Legen wir noch ein paar Monate drauf, damit auch diese Planungsdetails ohne Hektik, aber dann hoffentlich zu aller Zufriedenheit realisiert werden können!

Einwahl in Universität und Internet: „Welche Rufnummer muss ich wählen?“

M. Speer

Das ZIV der Universität bietet seinen Kunden (teilweise in Zusammenarbeit mit anderen Netzbetreibern) eine Reihe von Möglichkeiten für die direkte, konventionelle Einwahl über analoges Modem oder ISDN in das Universitätsnetz und das Internet an. Die Unterscheidung zwischen den Einwahlangeboten erfolgt über die angewählte Rufnummer. Diese legt dabei auch die für den Nutzer entstehenden Kosten fest.

Welches der Einwahlangebote genutzt werden kann, wird in erster Linie durch den benutzten Telefonanschluss beim Kunden festgelegt. In der Regel ist man hiermit aber nicht auf die Nutzung eines bestimmten Angebotes festgelegt. Welches Angebot tatsächlich genutzt wird und welche Kosten entstehen, legt man über die angewählte Rufnummer fest. Folgende Angebote stehen zur Verfügung:

Zuerst das „Standardangebot“:

1. „Uni@home“ mit der Einwahlrufnummer **0251 / 8807750**:

   Es sei zunächst das für jeden ZIV-Kunden nutzbare Standardangebot „Uni@home“ erwähnt. Dieses Angebot kann vom Telefonanschluss eines beliebigen Telefonanbieters (Deutsche Telekom, Citykom Münster, ...) aus benutzt werden. Es ist auch keinerlei zusätzliche Registrierung, Anmeldung o. ä. erforderlich. Für die Nutzung reicht eine gewöhnliche ZIV-Benutzerkennung aus.

   Als Einwahlkosten fallen die „normalen“ Telefongebühren des Telefonanbieters an. Das bedeutet insbesondere, dass dieses Angebot an Sonn- und Feiertagen über das XXL-Angebot der Telekom kostenlos genutzt werden kann.

Nun zwei „Spezialangebote“:

2. „universitätsinterne“ Einwahl mit der Rufnummer **66**:

   Mit diesem Einwahlangebot existiert die Möglichkeit, sich von einem Telefonanschluss des Telefonnetzes der Universität aus kostenlos einzuwählen. Auch hier reicht die gewöhnliche ZIV-Benutzerkennung ohne weitere Anmeldung aus.

3. „Teleport“ mit der Einwahlrufnummer **997**:

   Dieses Einwahlangebot kommt für Anschlüsse in Wohnheimen des Studentenwerks Münster in Frage. Genutzt werden kann das Angebot nur von Teleport-Vertragskunden. Nähere Auskünfte über die Tarife für die normale Telefonie und für die Einwahl in das Universitätsnetz / Internet erfahren Sie über das Studentenwerk bzw. Teleport.

   Es sei an dieser Stelle noch einmal ausdrücklich darauf hingewiesen, dass Teleport-Kunden nicht automatisch nur die Teleport-Einwahl zur Verfügung steht und diese auch nicht technisch von der „Uni@home“-Einwahlmöglichkeit ausgeschlossen sind. Wenn man die Teleport-Einwahltarife nutzen möchte (nach derzeitigem Kenntnisstand eine Flatrate), muss man ausdrücklich die Einwahlrufnummer 997 nutzen.

Zum Abschluss ein besonders günstiges Angebot für Telekom-Anschlüsse in Münster und Umgebung:

4. „uni@home plus“ mit der Einwahlrufnummer **0193-604**:

   Von vielen Telekom-Telefonanschlüssen in Münster und Umgebung aus kann die äußerst günstige „uni@home plus“-Einwahlmöglichkeit genutzt werden. Kunden der Citykom Münster können dieses Angebot leider nicht nutzen.

   Die Details der Nutzungsvoraussetzungen findet man auf der „uni@home plus“-Homepage: `www.uni-muenster.de/ZIV/unihomeplus` . An dieser Stelle sei nur die einfache Tarifstruktur (0,91 Cent/Min. rund um die Uhr, 40 Cent monatliche Grundgebühr) bei Nutzung von einem Telekom-Telefonanschluss im Tarifbereich Münster City genannt. Außerdem hat man die Möglichkeit, durch Festlegung eines Höchstbetrags die monatlich anfallenden Kosten zu begrenzen. „uni@home plus“-Nutzer können natürlich ggf. an Sonn- und Feiertagen über das XXL-Angebot der Telekom auch kostenlos das „Uni@home“-Angebot (vgl. 1.) nutzen.

Umfangreiche weitere Information zu den Einwahlsystemen des ZIV findet man unter: `www.uni-muenster.de/ZIV/Content--NetzEinwahl.html` .

ZIV-Tutorial

Sichere E-Mail mit perMail

R. Perske

Mit perMail steht Ihnen eine vergleichsweise sehr einfache Möglichkeit zur Verfügung, Ihre E-Mails kryptografisch gegen unbefugtes Lesen und gegen (Ver-) Fälschungen zu schützen. Dieser Artikel beschreibt Ihnen Schritt für Schritt, wie Sie sich in perMail ein PGP-Schlüsselpaar erzeugen und dieses dann verwenden.

Zunehmend erwacht bei vielen Internet-Nutzern das Bewusstsein, dass es nicht richtig sein kann, wenn fast jeder die E-Mail Anderer lesen oder gar verfälschen kann, wenn jeder E-Mails unter falscher Adresse versenden kann, wenn niemand kontrollieren kann, ob eine E-Mail wirklich vom angegebenen Absender stammt usw. usf. Und es kann nicht richtig sein, wenn von jedem, der seine Privatsphäre schützt, gleich behauptet wird, er habe etwas zu verbergen. Der Schutz der Privatsphäre ist ein Grundrecht, dass es zu verteidigen gilt.

Grundsätzlich ist das Internet genau wie der Funkverkehr ein anonymer Raum. Es wird immer anonyme Teilnehmer und Störer geben, das lässt sich einfach nicht verhindern. (Üble Subjekte sollten sich dadurch nicht in Sicherheit wiegen lassen: Auch im Internet gibt es das Äquivalent der Funkpeilung zur Ortung von Störern.)

Genau wie im Funkverkehr gibt es auch im Internet Mittel und Wege, sich vor bestimmten Ungebührlichkeiten zu schützen. Das wichtigste Mittel heißt in beiden Fällen Kryptographie, dazu gehören vor allem das Verschlüsseln, aber auch das Unterschreiben von Nachrichten.

Abb. 1: Umschalten auf sicheren Zugang: Folgen Sie Schritt für Schritt den markierten Anweisungen. Falls Ihnen „Fingerprints“ angezeigt werden, können Sie diese mit denen im gleichnamigen Artikel in jedem i vergleichen.

Jeder, der die kryptographischen Möglichkeiten zum Schutz von E-Mails nutzen möchte, benötigt eine entsprechende Software: Pretty Good Privacy (PGP) oder Gnu Privacy Guard (GnuPG). (Die Alternative S/MIME ist derzeit nur für geschlossene Verkehrskreise interessant.)

Oder er nimmt perMail, denn in perMail haben wir diese Software integriert und sehr viel Mühe darauf verwendet, die Einstiegshürden abzubauen.

Sicherer Zugang zu perMail

Die gesamte Verschlüsselung von E-Mails ist witzlos, falls Sie noch den ungeschützten Zugang zu perMail verwenden; denn dann kann alles abgehört werden, was zwischen Ihnen und dem perMail-Server abläuft, insbesondere auch Ihr Passwort und das unten beschriebene Geheimnis.

Falls Sie also bislang `http://permail.uni-muenster.de` verwenden, folgen Sie bitte den zweisprachigen Anweisungen auf der Anmelde-Seite (Abb. 1), schalten Sie die Verschlüsselung ein und benutzen Sie zukünftig direkt den abhörsicheren Zugang (Abb. 2) über `https://permail.uni-muenster.de` (beachten Sie das „s“ vor dem Doppelpunkt).

Kein modernes WWW-Programm macht Ihnen beim Akzeptieren der Zertifizierungsinstanzen mehr Schwierigkeiten als eine Reihe von Rückfragen, die Sie bitte zustimmend beantworten. (Wenn Sie ganz sicher gehen wollen, vergleichen Sie die Ihnen angezeigten Fingerprints mit denen, die Sie im Artikel „Fingerprints“ in jedem i finden .) Danach werden Sie nicht nur die perMail-Server, sondern alle abhörsicheren WWW-Server der Universität Münster ohne lästige Rückfragen benutzen können.

Abb. 2: Anmelden bei sicherem Zugang

perMail kann viel mehr

Viele perMail-Nutzer verwenden perMail mit der voreingestellten Bedienoberfläche „Start“. Diese Bedienoberfläche ist bewusst sparsam ausgestattet, um Einsteiger in perMail nicht durch die Vielfalt der Möglichkeiten dieses Programms zu verwirren. Daher stehen einige der nachfolgend genannten Schaltflächen in der Oberfläche „Start“ nicht zur Verfügung.

Sobald Sie einige Male mit perMail gearbeitet haben, sollten Sie daher überlegen, auf die Bedienoberfläche „Text“ umzusteigen. Nach der Anmeldung finden Sie unten auf der Seite im grauen Bereich „Darstellung“ das Auswahlfeld „Bedienung – perMail kann viel mehr“ (Abb. 3). Wählen Sie dort den Punkt „Text – für gelegentliche Nutzer“ und bedienen Sie, falls die Seite nicht automatisch neu geladen wird, dann die Schaltfläche „Aktualisieren“ weiter rechts in diesem Bereich.

Abb. 3: Auf der Bedienoberfläche „Start“: Stellen Sie die Bedienoberfläche auf „Text“ um.

Dann erscheinen all die Schaltflächen, die weiter unten erwähnt werden und die Sie vielleicht auf Ihrem perMail-Bildschirm bisher nicht finden. Benutzen Sie die Schaltfläche „Einstellungen speichern“ (Abb. 4), damit Sie nach der nächsten Anmeldung wieder direkt in die neue Oberfläche geleitet werden.

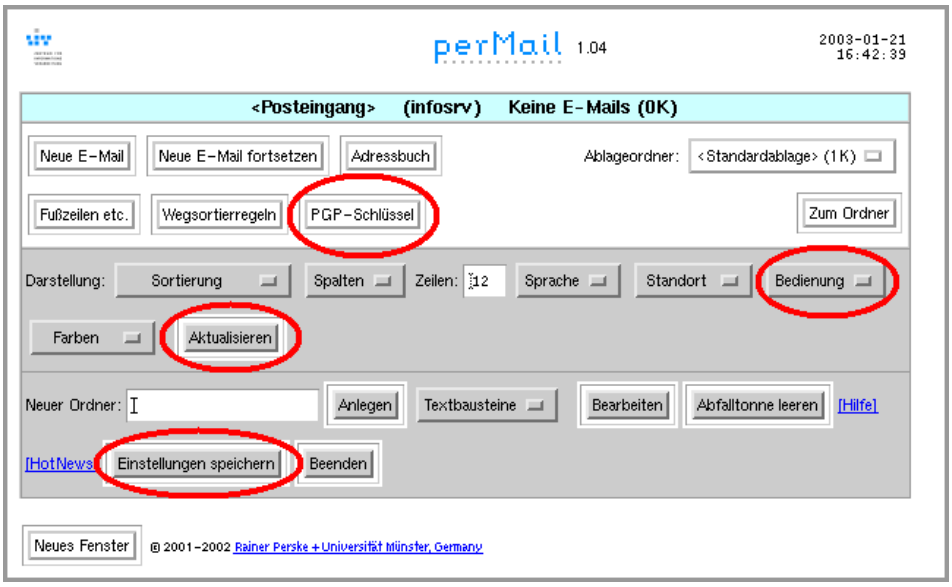


Abb. 4: Auf der Bedienoberfläche „Text“: Rufen Sie direkt die PGP-Schlüssel-Verwaltung auf oder stellen Sie vorher die Bedienoberfläche auf „Symbol“ um.

Falls Ihnen die Oberfläche „Text“ zu unübersichtlich erscheint und Sie statt mit den dicken Text-Schaltflächen lieber mit Platz sparenden Symbolen (Icons) arbeiten, schalten Sie

gleich weiter auf den Punkt „Symbol – für regelmäßige Nutzer“. Die Seite sieht dann aufgeräumter aus (Abb. 5), der Funktionsumfang ist aber der gleiche. Die Oberfläche „Symbol *“ vergrößert die Symbole. Die Bedeutung jedes einzelnen Symbols erfahren Sie, wenn Sie die Maus auf das Symbol bewegen (Ihr WWW-Programm muss dazu „ToolTips“ oder „BubbleHelp“ eingeschaltet haben), oder natürlich aus der Online-Hilfe.

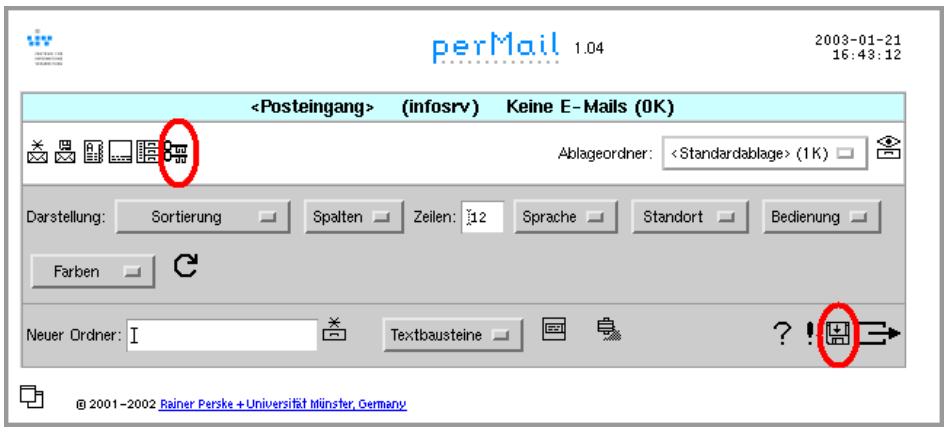


Abb. 5: Auf der Bedienoberfläche „Symbol“: Rufen Sie die PGP-Schlüssel-Verwaltung auf.

Falls Ihnen diese Oberflächen doch zu gewöhnungsbedürftig sein sollten, können Sie nach dem Erzeugen des Schlüsselpaars wieder auf „Start“ zurück schalten. Die nachfolgend beschriebenen Grundfunktionen stehen Ihnen auch dann zur Verfügung.

Das persönliche Schlüsselpaar

Um Verschlüsselung und Unterschriften zu nutzen, benötigt man ein persönliches Schlüsselpaar, bestehend aus einem geheimen und einem öffentlichen Schlüssel. Der öffentliche Schlüssel kann beliebig verbreitet werden, denn aus ihm lässt sich der geheime Schlüssel nicht ermitteln. Die beiden Schlüssel werden so eingesetzt:

- Zum Unterschreiben (Signieren) verwendet der Absender seinen eigenen geheimen Schlüssel. (Er ist der einzige, der damit unterschreiben kann.)
- Zum Überprüfen einer Unterschrift (Verifizieren) verwendet der Empfänger den öffentlichen Schlüssel des Absenders. (Das kann jeder machen, der sich den Schlüssel besorgt.)
- Zum Verschlüsseln verwendet der Absender den öffentlichen Schlüssel des Empfängers. (Das kann jeder machen, der sich den Schlüssel besorgt.)
- Zum Entschlüsseln verwendet der Empfänger seinen eigenen geheimen Schlüssel. (Er ist der einzige, der damit entschlüsseln kann.)

Daraus ergibt sich, dass der geheime Schlüssel sorgfältig geschützt werden muss, denn Unbefugte könnten damit Unterschriften fälschen oder vertrauliche Inhalte lesen.

Das Schlüsselpaar erzeugen

Damit Sie mit perMail Ihre E-Mails elektronisch unterschreiben können, benötigen Sie zuerst ein Schlüsselpaar. Um dieses zu erzeugen, bedienen Sie bitte auf der Index-Seite (Abb. 4, 5) oder der Ansicht-Seite die Schaltfläche „PGP-Schlüssel“. Sie finden die Schaltfläche im gleichen Bereich wie die Schaltfläche „Neue E-Mail“.

(Auch falls Sie schon ein eigenes Schlüsselpaar besitzen, müssen Sie diese Prozedur einmal absolvieren. Das neue Schlüsselpaar wird von perMail für sinnvoll voreingestellte Vertrauensangaben benötigt. Sie können Ihr eigenes Schlüsselpaar später trotzdem verwenden.)

Falls Sie nicht früher schon einmal PGP-Schlüssel mit perMail erzeugt haben, erscheint eine

entsprechende Fehlermeldung und dann ein großer Eingabebereich:„ Möchten Sie Ihre E-Mails verschlüsseln und elektronisch unterschreiben können?“ (Abb. 6) Bitte lesen Sie die kurzen Erläuterungen genau durch und überlegen Sie sich jetzt ein Geheimnis (auch Mantra oder Passphrase genannt). Das sollte ein längeres, äußerst sorgfältig gewähltes Passwort sein, da dieses Geheimnis das zweitschwächste Glied in der Kette zum Schutz Ihrer Daten darstellt. (Das schwächste Glied sitzt immer auf dem Stuhl vor dem Bildschirm.)

Anders als bei Login-Passwörtern verringert jede Änderung des Geheimnisses die Sicherheit, daher bietet perMail Ihnen diese Möglichkeit gar nicht erst. Sie müssen also

Abb. 6: Überlegen Sie sich ein gutes Geheimnis und starten Sie die Schlüsselgenerierung.

von Anfang an ein gutes Geheimnis wählen.

Geben Sie dieses Geheimnis in jedes der drei Eingabefelder ein („Doppelt hält besser“, aber „aller guten Dinge sind drei“) und bedienen Sie dann die Schaltfläche „Neues Schlüsselpaar erzeugen“. Danach beginnt eine Prozedur, die mehrere Minuten dauert. Den Fortschritt können Sie bei den meisten WWW-Programmen auf dem Bildschirm verfolgen (Abb. 7).

Diese Prozedur erzeugt Ihren Schlüssel mit PGP, versieht ihn ggf. auch mit Ihrem Aliasnamen, erzeugt vorsichtshalber ein Widerrufzertifikat für die Zukunft, überträgt das Schlüsselpaar nach GnuPG, importiert alle wichtigen Schlüssel der DFN-Zertifizierungsinstanzen und der ZIV-Mitarbeiter, sorgt durch Signieren und Einstellen von Vertrauensparametern für die Gültigkeit der DFN-Zertifizierungsinstanzen (dazu gehört auch die Zertifizierungsstelle der Universität Münster WWUCA) und importiert ggf. die PGP-Schlüssel, die Sie früher schon auf den zentralen Dialogservern, z. B. mit „pine“, verwendet haben. (Keine Bange, das müssen Sie sich nicht merken.)

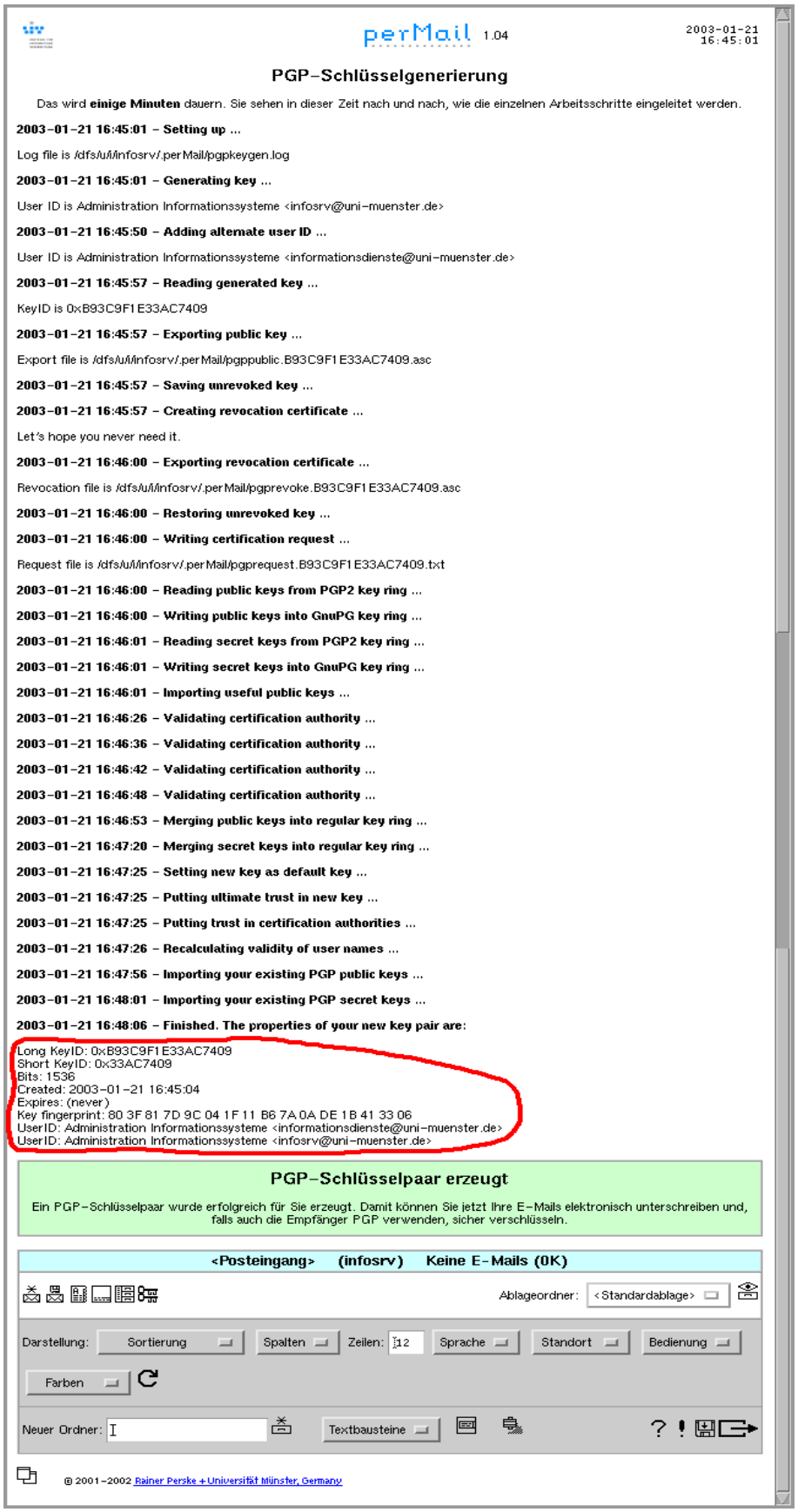


Abb. 7: Die Schlüsselgenerierung dauert einige Minuten. Notieren Sie sich danach „KeyID“, „Bits“ und „Key fingerprint“ Ihres Schlüssels.

Abschließend werden die technischen Daten Ihres Schlüssels angezeigt. Sinnvollerweise notieren Sie sich die „Short KeyID“, die Anzahl der „Bits“ (immer 1536) und den „Key fingerprint“. Mit diesen drei Angaben wird Ihr Schlüssel eindeutig identifiziert. Falls Sie einmal gefragt werden, wie die Daten Ihres Schlüssels sind, nennen Sie Ihrem Gesprächspartner diese Daten. (Die entsprechenden Daten für die Schlüssel der WWUCA finden Sie im Artikel „Fingerprints“ in jedem i .)

Das war's schon. Es erscheint wieder die Index- oder die Ansicht-Seite. Falls Sie die Schlüssel-Einstellungen kontrollieren oder gar ändern möchten, benutzen Sie noch einmal die Schaltfläche „PGP-Schlüssel“ (Abb. 4, 5). In der dann erscheinenden Liste aller Schlüssel in Ihrem Schlüsselring können Sie die Einstellungen beliebig ändern. Außerdem können Sie dort weitere Schlüsselringe importieren (auch solche mit weiteren eigenen Schlüsselpaaren) und aussuchen, welcher Ihrer Schlüssel beim Unterschreiben verwendet werden soll. Ausführlichere Erklärungen finden Sie in der Online-Hilfe.

Versenden von E-Mails

Um jemandem Ihren **Schlüssel zuzusenden**, schreiben Sie ihm am einfachsten eine E-Mail und fügen Sie den Schlüssel als Anlage bei. Dazu müssen Sie auf der Neue-E-Mail-Seite nur vor dem Absenden in der PGP-Zeile das Feld „Eigenen Schlüssel beifügen“ ankreuzen (Abb. 8).

Um eine E-Mail elektronisch zu **unterschreiben**, so dass jeder überprüfen kann, dass die E-Mail tatsächlich von Ihnen stammt und auch unterwegs nicht verfälscht wurde, müssen Sie auf der Neue-E-Mail-Seite nur vor dem Absenden Ihr Geheimnis in das Eingabefeld „PGP-Sig.“ eintragen (Abb. 8).

Um eine E-Mail zu **verschlüsseln**, benötigen Sie vorher den öffentlichen Schlüssel des Empfängers. Bei mehreren Empfängern benötigen Sie die Schlüssel aller Empfänger. Falls alle Schlüssel bereits vorliegen, müssen Sie auf der Neue-E-Mail-Seite nur vor dem Absenden in der PGP-Zeile das Auswahlfeld von „Unverschlüsselt“ auf „Verschlüsselt, nur bestätigte Schlüssel“ umstellen (Abb. 8).

Sie können auch die Auswahl „Verschlüsselt“ verwenden, dann könnte es aber passieren, dass ein Schlüssel verwendet wird, dessen Inhaber-Angabe Sie nicht überprüft haben – man könnte Ihnen also Schlüssel mit falschem Namen unterschieben. Mehr dazu folgt weiter unten.

Selbstverständlich können Sie Unterschreiben, Verschlüsseln und Schlüsselbeifügen beim Versenden miteinander kombinieren.

Genau genommen werden natürlich nicht die E-Mails als Ganzes, sondern die Teile einer E-Mail einzeln signiert bzw. verschlüsselt. Denn die Informationen im Kopf, z. B. die Adressaten, müssen natürlich auch bei verschlüsselten E-Mails lesbar bleiben. Schreiben Sie also keine vertraulichen Informationen in die Betreff-Zeile.

Empfangen von E-Mails

Falls der Text einer E-Mail unterschrieben, aber nicht verschlüsselt ist und falls der Schlüssel des Absenders bereits vorliegt, überprüft perMail auf der Ansicht-Seite (Abb. 9) die Unterschrift automatisch und zeigt das Ergebnis unterhalb des Textes an.

Um einen Teil einer E-Mail zu entschlüsseln und/oder die Unterschrift unter diesem Teil zu überprüfen, bedienen Sie auf der Ansicht-Seite unter dem jeweiligen Teil die Schaltflächen „PGP-Meldungen“ und „PGP-dekodieren“. Falls der Teil verschlüsselt ist, müssen Sie vorher in das Eingabefeld rechts daneben Ihr Geheimnis eintragen.

Die Schaltfläche „PGP-Meldungen“ zeigt Ihnen das Ergebnis der Überprüfung der Unterschrift und alle Fehler beim Entschlüsseln und Verifizieren an. Die Schaltfläche „PGP-dekodieren“ zeigt Ihnen den entschlüsselten Inhalt an. (Falls es sich beim Inhalt um

Daten für irgendeine Software, z. B. um eine Word-Datei, handelt, können Sie mit der Funktion „Speichern als ...“ Ihres WWW-Programms die entschlüsselte Datei abspeichern.

Falls Ihnen Schlüssel oder ganze Schlüsselringe zugesendet werden, bedienen Sie bitte die Schaltfläche „PGP-Schlüssel nehmen“ unter dem Teil, der den Schlüssel enthält. Dadurch wird der Schlüssel in Ihren Schlüsselring übernommen.

In der Regel werden zugesandte Schlüssel weder von Ihnen selbst noch von einer DFN-Zertifizierungsinstanz bestätigt sein. Diese können also beim oben beschriebenen Verschlüsseln vorerst nur mit der Einstellung „Verschlüsselt“, nicht aber mit „Verschlüsselt, nur bestätigte Schlüssel“ verwendet werden.

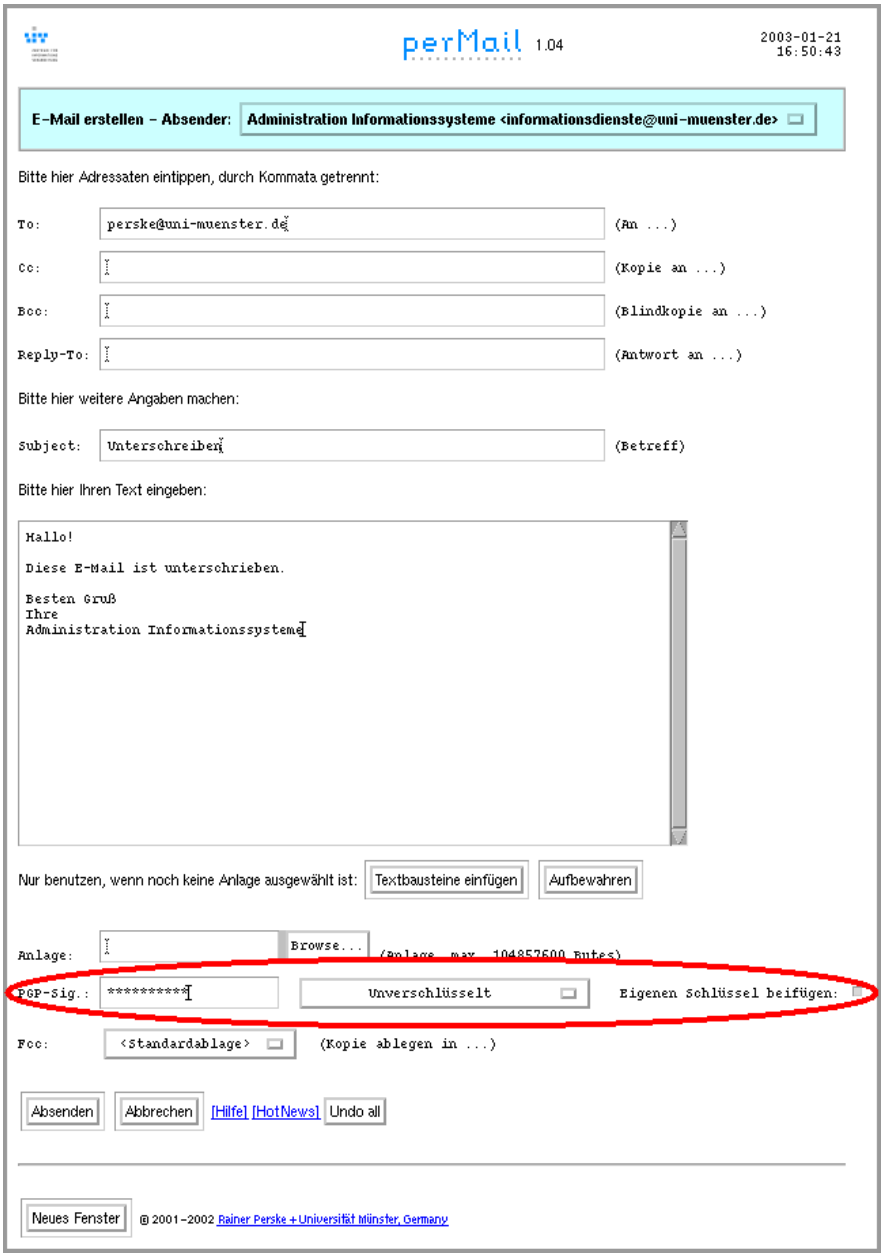


Abb. 8: Versenden einer E-Mail: Sie unterschreiben durch Eingabe Ihres Geheimnisses. Ein weiterer Mausklick genügt, um den eigenen öffentlichen Schlüssel der E-Mail beizufügen.

Falls Sie mit der Gefahr leben können, dass Ihnen ein Schlüssel mit falschem Namen untergeschoben wird, wissen Sie jetzt bereits alles, was Sie zur Benutzung der kryptographischen Möglichkeiten von perMail wissen müssen.

Bestätigen von Schlüsseln

Falls Sie jedoch vermeiden wollen, auf untergeschobene Schlüssel hereinzufallen, müssen Sie leider etwas mehr Mühe bei der Schlüsselverwaltung investieren. Aber auch hier versucht perMail es Ihnen einfach zu machen.

Zur Verwaltung der Schlüssel gibt es die PGP-Schlüssel-Seite, die Sie von der Index- und von der Ansicht-Seite aus mit der Schaltfläche „PGP-Schlüssel“ erreichen. Dort finden Sie zu jedem Schlüssel verschiedene Angaben, unter anderem die Schlüssellänge in „Bits“, die „KeyID“ in Lang- und Kurzform (die Kurzform ist einfach die rechte Hälfte der Langform), den „Fingerprint“ und die Inhaber, denen der Schlüssel angeblich gehört.

Ein Schlüssel kann durchaus mehrere Inhaber-Angaben haben. Häufig handelt es sich dabei um die gleiche Person mit unterschiedlichen E-Mail-Adressen.

In der Spalte „Gültig“ finden Sie die Angabe, ob eine Inhaber-Angabe bestätigt ist. Falls dort nur ein Fragezeichen steht, kann mit der Schaltfläche „Gültig?“ am unteren Ende der Tabelle die Gültigkeit neu berechnet werden; das kann allerdings etliche Sekunden dauern.

Falls Sie selbst bestätigen möchten, dass ein Schlüssel wirklich zu einem angegebenen Inhaber gehört, gehen Sie bitte wie folgt vor:

- Besorgen Sie sich vom Inhaber des Schlüssels die Schlüssellänge, die „KeyID“ und den „Fingerprint“. Dies darf keinesfalls per E-Mail geschehen, sondern Sie müssen anderweitig sicher stellen, dass Sie diese Informationen wirklich vom Inhaber selbst erhalten. (Zertifizierungsinstanzen verlangen in der Regel die Übergabe bei einem persönliches Treffen und die Vorlage des Personalausweises.)
- Vergleichen Sie diese Angaben sorgfältig mit den Angaben in der Schlüsseltabelle.
- Nur wenn die Angaben in allen Ziffern identisch sind, tippen Sie Ihr Geheimnis in das entsprechende Eingabefeld am unteren Ende der Tabelle. Bedienen Sie dann die Schaltfläche „Sig.“ (Signieren) in genau der Zeile mit der Inhaber-Angabe, die Sie bestätigen möchten.

Sie unterschreiben damit, dass der Schlüssel tatsächlich dem angegebenen Inhaber gehört.

Falls Sie jemand anderes um Ihre Schlüsseldaten bittet: Diese haben Sie sich oben bei der Schlüsselgenerierung notiert oder können den ersten Zeilen auf der PGP-Schlüssel-Seite entnommen werden.

Falls Sie uns und der DFN-Zertifizierungshierarchie vertrauen, ist dies jetzt wirklich alles gewesen, was Sie wissen müssen.

Vertrauen und Misstrauen

Falls Sie jedoch selbst bestimmen möchten, welchen Stellen Sie dahin gehend vertrauen, dass sie keine falschen Bestätigungen ausstellen, können Sie auch diese Einstellung auf der PGP-Schlüssel-Seite vornehmen und damit Ihr eigenes Vertrauensgeflecht zusammen stellen.

Damit eine Inhaber-Angabe eines Schlüssels als gültig angesehen wird, müssen Sie die Angabe entweder selbst bestätigt haben oder aber – jetzt wird es kompliziert – die Angabe muss von anderen Stellen bestätigt sein, wobei erstens die Schlüssel dieser anderen Stellen bereits als gültig erkannt sind und zweitens diese Stellen als vertrauenswürdig eingestuft sind. (Diese Zusammenhänge habe ich in meinen Artikeln „Kryptografische Fingerabdrücke“ und „Zertifikate für PGP-Schlüssel“ im i 3+4/1997 ausführlich beschrieben.)

Bei der Schlüsselgenerierung mit perMail werden genau diese Bestätigungen und Einstufungen bereits entsprechend den Empfehlungen der WWUCA und des ZIV vorgenommen; bei anderen Programmen müssen Sie sich selbst darum kümmern.

Auf der PGP-Schlüsselseite können Sie für jeden Schlüssel die Vertrauenswürdigkeit der Inhaber ändern oder den Schlüssel sogar vollständig deaktivieren, so dass er nicht mehr verwendet wird. Sie werden feststellen, dass Sie selbst der einzige sind, dem Sie absolut vertrauen – zumindest aus der Sicht von perMail. Die genaue Bedienung entnehmen Sie bitte der Online-Hilfe.

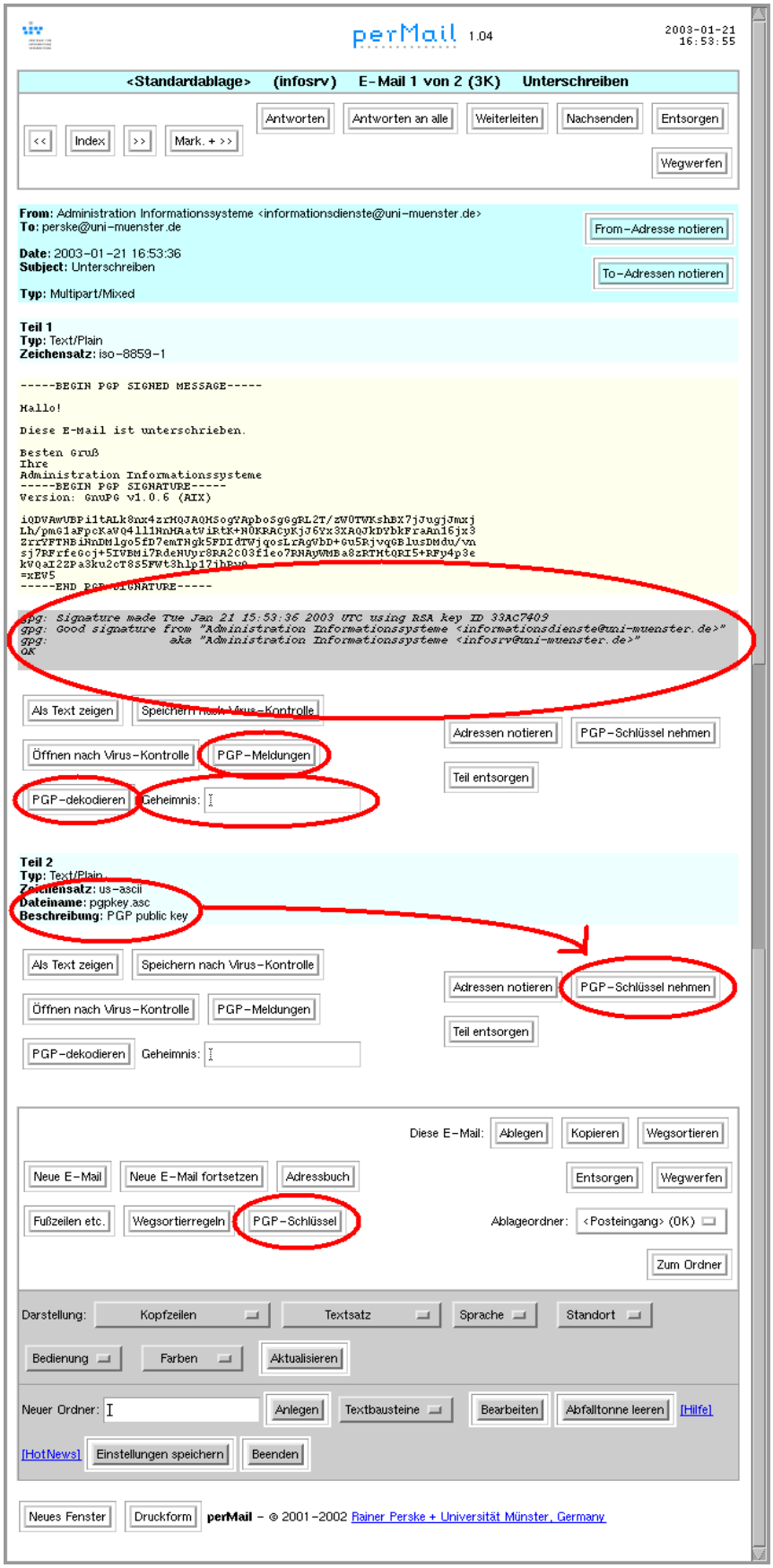


Abb. 9: Empfangen einer E-Mail: Der Zeichensalat unter dem Text enthält die Unterschrift, diese wird automatisch kontrolliert. Verschlüsselte oder signierte E-Mails können Sie nach Eintippen Ihres Geheimnisses entschlüsseln (PGP-dekodieren) und verifizieren (PGP-Meldungen). Beigefügte Schlüssel können Sie in den eigenen Schlüsselring übernehmen.

Ein Zertifikat für Ihren Schlüssel

Wenn Sie möchten, dass Ihr Schlüssel mit einer Bestätigung durch die Zertifizierungsstelle der Universität Münster (WWUCA) versehen („zertifiziert“) wird, so dass er von möglichst vielen anderen Nutzern oder auch von den Mitarbeitern des ZIV automatisch als gültig angesehen wird, dann drucken Sie bitte das Formular auf der Seite `http://www.uni-muenster.de/WWUCA/antrag-pgp-person.txt` aus und tragen Sie dort die Daten Ihres PGP-Schlüssels und Ihres Personalausweises ein.

Senden Sie dann Ihren Schlüssel per E-Mail an `ca@uni-muenster.de` und geben Sie Ihren Antrag persönlich (Ausweis nicht vergessen!) bei der WWUCA im ZIV, Röntgenstraße 9-13, ab. Um vergebliche Wege zu vermeiden, sollten Sie vorher unter 83-31590 nachfragen, ob der zuständige Mitarbeiter im Hause ist.

Den bestätigten Schlüssel erhalten Sie dann später per E-Mail. Sie müssten dann einmal mit „PGP-Schlüssel nehmen“ die Bestätigung in Ihren Schlüsselring übernehmen. Danach wird die Bestätigung bei jedem Versenden des Schlüssels automatisch mitgeschickt.

Eine E-Mail, die mit einem von der WWUCA bestätigten Schlüssel unterschrieben ist, wird vom ZIV in fast allen Fällen genauso akzeptiert wie ein eigenhändig unterschriebener Brief und in vielen Fällen sogar bevorzugt. Statt durch die WWUCA darf der Schlüssel auch durch eine andere DFN-Zertifizierungsinstanz oder durch bestimmte weitere Zertifizierungsinstanzen (c't-Zertifizierungsinitiative u. a.) bestätigt sein. Nur bei Dokumenten, die wir Dritten vorlegen müssen (Einzugsermächtigungen usw.), können wir auf die Schriftform nicht verzichten.

Etwas für den Wissensdurst

Weitere Informationen zu perMail finden Sie im i (online unter `http://www.uni-muenster.de/ZIV/inforum/` abrufbar) in folgenden Ausgaben:

- „perMail wird erwachsen“, i 2/2002
- „Neues und Tipps und Tricks zu perMail“, i 1/2002
- „Neues von perMail“, i 3/2001
- „Unsere Antwort: perMail“, i 2/2001

sowie natürlich in der Online-Hilfe unter

`http://permail.uni-muenster.de/help-de.html` (deutsch) und
`http://permail.uni-muenster.de/help-en.html` (englisch).

Wenn Sie mehr über die GnuPG, PGP, die Funktionsweise des „Web of Trust“ und die DFN-Zertifizierungshierarchie wissen möchten oder vielleicht GnuPG oder PGP auf Ihrem eigenen Rechner installieren möchten, dann starten Sie bitte mit folgenden WWW-Seiten:

- GNU Privacy Guard: `http://www.gnupg.org`
- PGP international: `http://www.pgpi.org`
- Phil Zimmermann, der PGP-Entwickler: `http://www.philzimmermann.com`
- PGP Corporation: `http://www.pgp.com`
- DFN-PCA, die Zertifizierungsinstanz für das Deutsche Forschungsnetz: `http://www.dfnpca.de`
- WWUCA, die Zertifizierungsstelle der Universität Münster: `http://www.uni-muenster.de/WWUCA/`

Spam verrät sich durch ihren Inhalt

E. Sturm

Es gibt auch Anti-Spam-Programme, die man nicht mühsam pflegen muss. Hier ein Erfahrungsbericht.

Wer irgendwo im Internet seine E-Mail-Adresse hinterlassen hat, sei es auf einer Webseite oder in einer Zuschrift an ein Diskussionsforum, hat wohl inzwischen Ärger mit unverlangt zugeschickter Reklame-E-Mail, gemeinhin Spam genannt.

Bei vielen Mail-Programmen kann man Filter einstellen, die bei bestimmten Absendern, verdächtigen Wörtern und nach anderen Kriterien neue E-Mail gleich aussondern. Wer das versucht hat, hat wohl bemerkt, dass er so mehr Arbeit hat, als wenn er Reklame-Mail selbst gelöscht hätte.

Die Idee

Interessant ist jetzt ein neuer Ansatz, der ohne eigene Pflege von Kriteriensammlungen auskommt. Zentraler Punkt ist, dass eine Mail, die Ihren Zweck erreichen will, im Text selbst Wörter verwenden muss, die verräterisch sind. Ein Antispam-Programm braucht also nur ein Wortverzeichnis aufzubauen und für jede Mail mitzuzählen, wie oft es in einer ordentlichen und wie oft es in einer Spam-Mail vorkommt, um dann auch für neue Mail Wahrscheinlichkeitsaussagen machen zu können. Die einzige Benutzerpflicht ist es, solange der Datenbestand noch relativ leer ist, ankommende Mails zu bewerten. Mit wachsender Wortanzahl wird er immer weniger gefragt, weil viele Reklame-Mails schon ungefragt gelöscht werden.

So viel zur Theorie. Da Spam erst mit einem Anti-Spam-Programm so richtig Spaß macht, habe ich mich also zuhause hingesetzt und die ganze Sache mal eben programmiert. (Das macht mir mehr Spaß, als bei fremden Programmen herauszubekommen, warum sie nicht das leisten, was sie sollen.) Dann auch im Dienst eingesetzt, zeigte das Programm tatsächlich eine beeindruckende „Intelligenz“.

Wie geht man vor?

Zunächst möchte ich auf den Algorithmus eingehen. Nachdem ich zwei Artikel im Internet (s. u.) gelesen und nicht ganz verstanden hatte, beschloss ich folgendermaßen vorzugehen:

1. In das Wortverzeichnis nehme ich auf:
   - Absender,
   - Empfänger,
   - Betreff,
   - Codierung (*Content_transfer_encoding*),
   - Inhaltstyp (*Content_type*) mit Zeichensatz sowie
   - die ersten 50 Zeilen der Mail, sofern es sich um Text handelt (also z. B. text/plain oder text/html).
2. Wenn das Programm gestartet wird, liest es von jeder Mail auf dem Server den Kopf und die ersten 50 Zeilen des Rumpfes (per POP3). Für jedes der gemäß Punkt 1 relevanten Wörter wird nun nachgeschaut, ob es schon bekannt war, und wenn ja, mit welcher Wahrscheinlichkeit Spam zu erwarten ist.
3. Als Wahrscheinlichkeit gilt nicht einfach der Quotient aus Anzahl Spam-Mail und Gesamtanzahl für dieses Wort, sondern gemäß [2] der Quotient

$$\frac{0{,}4 \; + \; \text{Anzahl\_gesamt} \; * \; W}{\text{Anzahl\_gesamt} \; + \; 1}$$

   mit

Anzahl_gesamt = Anzahl_spam + Anzahl_ok

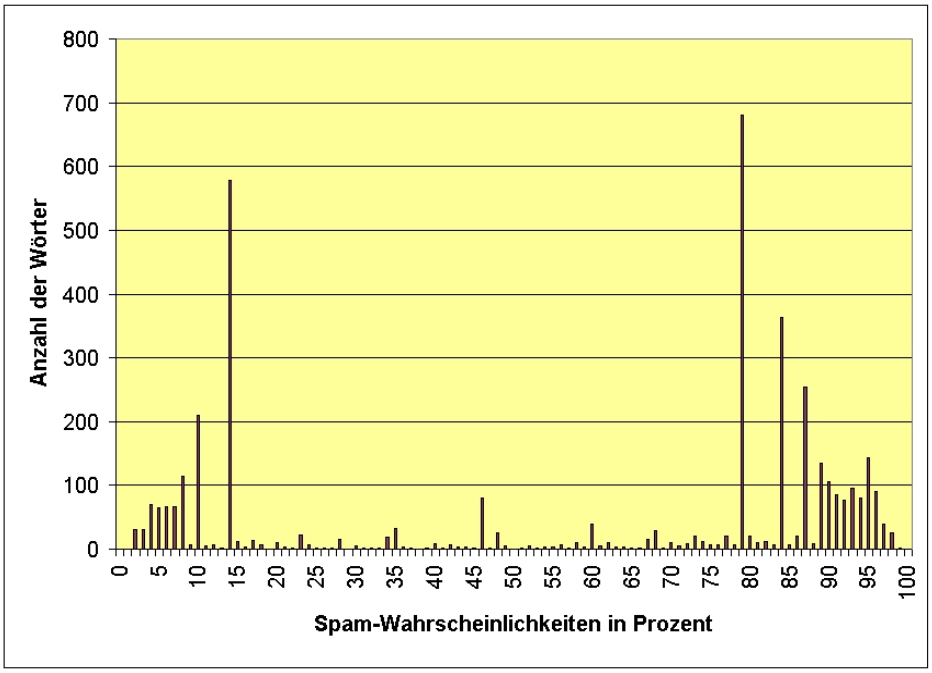
und

W = Anzahl_spam / Anzahl_gesamt.

Hierdurch wird erreicht, dass Wörter, die zum ersten Mal in einer Spam-Mail aufgetaucht sind, noch nicht mit ihrem nominellen Wert in die Berechnung eingehen. Als nominelle Werte gelten 0.99 für Spam-Mail und 0.01 für ordentliche Mail. Nach dieser Formel bekommt ein Wort, das nur zweimal in einer Spam-Mail vorkam, einen Wert von 0,78.

4. In der Mail mehrfach vorkommende Wörter werden nur einmal berücksichtigt.
5. Bei Wörtern, die länger als 16 Zeichen sind, werden die ersten acht und die letzten acht Zeichen gespeichert. Wörter mit weniger als drei Zeichen fallen unter den Tisch.
6. Als Zeichen gelten ohne Rücksicht auf Groß- und Kleinschreibung das Alphabet, die Umlaute, das Eszett, ein Punkt sowie Binde- und Schrägstrich inmitten eines Wortes – nicht zu vergessen natürlich das Dollarzeichen.
7. In die Bewertung gehen nur die 15 am meisten von 0,5 (in jeder Richtung) abweichenden Wörter ein. Aus Ihren Wahrscheinlichkeiten wird der Durchschnitt gebildet.
8. Als Spam erkannte oder bezeichnete E-Mails werden direkt auf dem Mailserver gelöscht. Mit dem eigentlichen E-Mail-Programm kann man dann weiter verfahren wie gewohnt.

Etwas unverständlich scheint eine inzwischen zu beobachtende Masche der Spam-Versender zu sein: Zwischen je zwei Buchstaben einer text/html-Mail wird ein HTML-Kommentar eingefügt. Der Leser merkt nichts davon, das Antispamprogramm findet aber kein Wort, das länger ist als ein Buchstabe. Wahrscheinlich richtet sich dieser Trick gegen Provider, die sich erst einmal wieder anpassen müssen (wie auch ich es getan habe).



Was kommt heraus?

Nach 14 Tagen waren etwa 8000 Wörter beisammen, die auf Grund ihrer trickreichen Speicherung in der Datei etwa 0,5 MB belegen. Nach einer weiteren Woche waren es 9000. Interessant sind jetzt natürlich Fragen statistischer Art:

Welche Wörter sind am häufigsten? Antwort: *bit* gefolgt von *uni-muenster.de* und *http*. Diese sind aber nicht die aussagekräftigsten. Spitzenreiter für Spam ist *here* gefolgt von *body* und *text/html*, Spitzenreiter für ordentliche Mail ist *das* gefolgt von *eberhard*. Auch *informatrbeitung* (siehe Punkt 5. oben) kommt gut weg.

Was ist noch interessant? Von 9000 Wörtern kommen 5000 nur einmal vor. 90 Wörter kommen mehr als 60-mal vor. Betrachtet man nur die Wörter, die mehr als einmal vorkommen, so fällt auf, dass der Bereich zwischen 0,15 und 0,76 nur mit etwa 500 Wörtern vertreten ist, die beiden extremen Bereiche aber mit 1200 und 2200 (siehe das Histogramm).

In der letzten Woche vor Redaktionsschluss habe ich mal mitgezählt: Von 111 empfangenen E-Mails wurden 55 korrekterweise als Spam erkannt und 52 korrekterweise als ordentlich. Lediglich 4 wurden als ordentlich angesehen, obwohl sie Spam waren, und keines wurde fälschlicherweise als Spam bewertet.

Wie geht es weiter?

Demnächst werde ich freischalten, dass ich bei Mail mit einer Spam-Wahrscheinlichkeit von weniger als 0,15 nicht mehr gefragt werde und dass Mail bei einer Spam-Wahrscheinlichkeit von mehr als 0,85 sofort gelöscht wird.

Vorerst beobachte ich noch, wie die Wortbasis wächst. Bei zwei Megabyte werde ich wohl eingreifen. Bis dahin fällt mir sicher noch ein, welche Wörter ich wegwerfen kann. (Eine Angabe, wann ein Wort zuletzt angetroffen wurde, habe ich vorsorglich mitgespeichert.)

Als Fazit kann ich sagen, dass ich nie mehr zu einem kriteriengestützten Antispam-Programm zurückkehren werde. Hoffen wir, dass die bekannten Mail-Programme bald mit Inhaltsfilter versehen werden!

[1] `http://www.paulgraham.com/spam.html`
[2] `http://radio.weblogs.com/0101454/stories/2002/09/16/spamDetection.html`

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2003)

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, G 83-31561

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse `http://www.uni-muenster.de/ZIV/Content-Lehre. html` unter „Anmelden“ zu den Veranstaltungen erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Ferienveranstaltungen sind möglich ab 13. Januar 2003.

260014 Betriebssystem Linux/Unix: Einführung und Grundlagen — Grote, M.
vom 17.02. bis 28.02.2003,
Mo-Fr 10-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260029 Publizieren mit LaTeX — Kaspar, W.
vom 17.02. bis 28.02.2003,
Mo-Fr 9-11 und 15-17 Uhr
Hörsaal: M4, Einsteinstr. 64

260033 Programmieren in Java für Fortgeschrittene — Süselbeck, B.
vom 24.03. bis 04.04.2003,
Mo-Fr 9-11 Uhr
Hörsaal: M4, Einsteinstr. 64

260048 Statistische Datenanalyse mit dem Programmsystem SPSS — Zörkendörfer, S.
vom 10.03. bis 21.03.2003,
Mo-Fr 9-11 Uhr, Übungen n.V.
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260052 Multimedia-Praktikum: Bildgewinnung und -präsentation — Kisker, H.-W.
vom 24.03. bis 28.03.2003,
Mo-Fr 9-13 Uhr, nachmittags n.V.
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260067 Systemadministration für Linux-Systeme — Hölters, J.
vom 31.03. bis 04.04.2003,
Mo-Fr 9-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

260071 Windows-Betriebssysteme: Einführung und systemtechnische Grundlagen — Kämmerer, M.
vom 07.04. bis 11.04.2003, Mo-Fr 9-17 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

Veranstaltungen in der Vorlesungszeit (Sommersemester 2003) für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, G 83-31561

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse `http://www.uni-muenster.de/ZIV/Content-Lehre. html` unter „Anmelden“ zu den Veranstaltungen erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Semesterveranstaltungen sind möglich ab 10. März 2003.

260086 Publizieren im Internet mit HTML und XML — Neukäter, B.
Mittwoch 10-12 Uhr
Hörsaal: M4, Einsteinstr. 64, Beginn: 30.04.2003

260090 Programmieren in Java — Pudlatz, H.
Dienstag 13-15 Uhr
Hörsaal: M4, Einsteinstr. 64, Beginn: 29.04.2003

260105 Objektorientiertes Programmieren in C++ — Mersch, R.
Mittwoch 12-14 Uhr
Hörsaal: M4, Einsteinstr. 64, Beginn: 30.04.2003

260110 Erstellen dynamischer Webseiten mit PHP — Sturm, E.
Freitag 11-13 Uhr
Hörsaal: M4, Einsteinstr. 64, Beginn: 02.05.2003

260124 Einführung in SQL: — Ost, St.
Ein Vergleich der SQL-Implementierungen von DB2 und MySQL
Montag 13-15 Uhr
Hörsaal: Raum 206, Röntgenstr. 9-13, Beginn: 28.04.2003

260139 Statistische Datenanalyse mit dem Programmsystem SPSS — Nienhaus, R.
Donnerstag 11-13 Uhr
Hörsaal: ZIV-Pool 2, Einsteinstr. 60, Beginn: 08.05.2003

260143 Windows Scripting für Administratoren — Winkelmann, O.
Donnerstag 14-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 24.04.2003

260158 Rechnernetze und Internet: Fortgeschrittene Themen — Richter, G./ Forsmann, A./ Kamp, M./ Speer, M./ Wessendorf, G.
Donnerstag 10-12 Uhr
Hörsaal: Raum 206, Röntgenstr. 9-13, Beginn: 08.05.2003

260162 Kolloquium des Zentrums für Informationsverarbeitung — Held, W.
Freitag 14-16 Uhr
Hörsaal: Raum 206, Röntgenstr. 11

Kommentare zu den Lehrveranstaltungen

260014 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen. Als preiswerte Windows-Alternative ist es augenblicklich in aller Munde. Die Vorlesung will in die Linux-Benutzung einführen. Sie besteht aus zwei Teilen.

Zuerst erfolgt eine an üblichen Unix-Einführungen orientierte Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle. Anschließend wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

260029 Publizieren mit LaTeX

LaTeX ist ein mächtiges und flexibles Satzsystem, das sich besonders für wissenschaftliche und technische Publikationen eignet. Der Autor kann aus einer Vielzahl von fertigen Layouts auswählen und diese seinen eigenen Vorstellungen anpassen. Mit speziellen Komponenten, z. B. zur Erzeugung von PDF- oder HTML-Dateien, können LaTeX-Publikationen für die Veröffentlichung auf CD-ROM oder im Internet vorbereitet werden. Das komplette Satzsystem ist frei erhältlich und steht praktisch auf allen verbreiteten Betriebssystemen zur Verfügung.

In dieser Veranstaltung werden die Grundkonzepte und wichtigsten Erweiterungen von LaTeX vorgestellt, u. a.

- die Komponenten des Satzsystems,
- allgemeine Dokument- und Textstrukturen,
- Formeln, Tabellen, Grafiken und
- die Erzeugung von PDF-Dokumenten,

und wie hiermit ordentlich strukturierte und typografisch ansprechende Dokumente erstellt werden können.

Die Hörer/innen sollten Grundkenntnisse im Umgang mit PCs besitzen.

LAMPORT: *Das LaTeX-Handbuch*, Addison-Wesley
ABDELHAMID: *Das Vieweg LaTeX2e-Buch*, Vieweg
DETIG: *Der LaTeX-Wegweiser*, Thomson
KOPKA: *LaTeX – Band 1: Einführung*, Addison Wesley
GOOSSEN, MITTELBACH, SAMARIN: *Der LaTeX-Begleiter*, Addison-Wesley
KLÖCKL: *LaTeX2e: Tips und Tricks*, dpunkt

260033 Programmieren in Java für Fortgeschrittene

In der Vorlesung sollen einige fortgeschrittene Konzepte der Programmiersprache Java vorgestellt werden.

Am Anfang der Lehrveranstaltung stehen Techniken zur Unterstützung der parallelen Programmierung (Multithreading) in Java. Im Anschluss daran erfolgt eine Übersicht zu I/O in Java (Streams-Konzept). Als internetbasierte Sprache bietet Java eine Reihe von Werkzeugen zur Netzwerkprogrammierung. Neben der Vorstellung der entsprechenden Grundlagen erfolgt eine Übersicht zu den darauf aufbauenden Themen wie Remote Method Invocation, Datenbankzugriff und Servlets.

Einen weiteren Themenschwerpunkt bilden schließlich neuere Konzepte zur Gestaltung grafischer Benutzeroberflächen wie Java-Beans und die Swing-Klassen.

260048, 260139 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in dieser Veranstaltung in der neuesten deutschsprachigen Version unter Windows vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

260052 Multimedia-Praktikum: Bildgewinnung und -präsentation

Das Praktikum führt in die elementaren Techniken der Bildgewinnung und deren Präsentation ein. Die Hörer/innen sollen Erfahrung im Umgang mit Flachbett-Scannern, Dia-Scannern, digitalen Kameras, Videokameras und Webcams gewinnen. Gleichzeitig wird auch die Präsentation des gewonnenen Bildmaterials als Druckausgabe, Foto-CD, Video-CD und Live-Internet-Übertragung trainiert.

Das Praktikum besteht aus zwei Teilen. Der erste Teil ist als Web-Vorlesung organisiert. Hier wird zum einen in die theoretischen Grundlagen der verschiedenen Techniken eingeführt und zum anderen werden die Experimente und Aufgaben aus Teil 2 beschrieben. Dieser Teil kann und soll von den Studierenden selbständig als Vorbereitung auf Teil 2 durchgearbeitet werden. Er wird ab Anfang März im Web zur Verfügung stehen. Der zweite Teil stellt das eigentliche Praktikum dar. Dabei wird der in Teil 1 erarbeitete Stoff vorausgesetzt. Gruppen von bis zu drei Personen beschäftigen sich jeweils mit einem Experiment. Jeder Gruppe wird jeden Tag der Woche ein neues Experiment zugeteilt.

Im Einzelnen sind folgende Experimente vorgesehen:

1. Gewinnung von gerasterten Bildern (d. h. von Druckvorlagen); Gerät: Flachbettscanner; Präsentation: Druck
2. Gewinnung von Bildern mit kontinuierlicher Farbverteilung (d. h. Fotos); Gerät: Dia-Scanner; Präsentation: Druck
3. Bildgewinnung mit einer digitalen Kamera; Gerät: Digitale Kamera; Präsentation: Still-Video-CD
4. Bildgewinnung mit Video-Kamera (d. h. Filmerstellung); Gerät: Video-Kamera; Präsentation: Video-CD
5. Bildgewinnung und Präsentation in Echtzeit (d. h. Video-Konferenz); Gerät: Webcam; Präsentation: Bildschirm

Die Experimente werden jeweils morgens unter Aufsicht in den für das Praktikum reservierten Räumen durchgeführt. An den Tagen vor den Experimenten 3 und 4 sind auch die Nachmittage mit Arbeit belegt. Den entsprechenden Gruppen werden digitale Kameras bzw. Video-Kameras ausgeliehen. Sie müssen dann selbständig die für den folgenden Tag benötigten Bilder bzw. Videos erstellen.

260067 Systemadministration für Linux-Systeme

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender/innen, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind grundlegende Kenntnisse der Unix-Kommandos und der Shell-Script-Sprache.

Die Teilnehmer/innen werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden. Ferner wird demonstriert, wie man einen speziell auf die Hardware-Ausstattung des Rechners optimierten Kernel generiert.

260071 Windows-Betriebssysteme: Einführung und systemtechnische Grundlagen

Folgende Themen sollen behandelt werden:

1. Die Bedienoberfläche von Windows: Look and Feel, Standardprogramme
2. Betriebssystemarchitektur: Dateisystem, Registry, Systemsteuerung, Dienste, Benutzerverwaltung, Zugriffsrechte, Kryptographie, Objekte
3. Kommunikationsdienste: Internet, LAN, TCP/IP, NetBios, Browser, Telnet, X, Terminal-Server-Client, Netzwerkverbindungen
4. Installation und Konfiguration: Betriebssysteme, Anwendungsprogramme, Netzkonfiguration (Ethernet, ISDN, Modem)
5. Sicherheit: Viren, Netzangriffe, Absicherung des PCs, McAfee, Personal FireWall
6. PC-Hardware: Bus-System, Plattentechnologien, Speicher, Peripherie
7. Rückblick und Ausblick: DOS, WfW, Windows'95/98/ME, Windows NT/2000, Architekturunterschiede, Stärken und Schwächen der aktuellen Versionen

260086 Publizieren im Internet mit HTML und XML

Neben den traditionellen Medien Buch, Zeitschrift, Presse, Rundfunk und Fernsehen wird das Internet zur Veröffentlichung wissenschaftlicher Erkenntnisse in Wort, Bild und Ton genutzt. Eine wichtige Grundlage für Veröffentlichungen im Internet ist die Hypertext Markup Language (HTML), mit deren Hilfe ein Geflecht von Texten, Bildern und anderen multimedialen Elementen im World Wide Web (WWW) dargestellt werden kann.

Die HTML steht im Mittelpunkt dieser Lehrveranstaltung, in der gezeigt werden soll, dass es keiner besonderen Rechner- oder Informatikkenntnisse bedarf, um Web-Seiten für das Internet zu gestalten. Voraussetzung für diese Veranstaltung sind lediglich Kenntnisse, wie sie etwa in der Vorlesung „Kommunikation und Information im Internet" vermittelt werden.

Im zweiten Teil der Veranstaltung sollen neben der HTML weitere Themen wie Webserver, CGI-Skripte, JavaScript und XML behandelt werden.

260090 Programmieren in Java

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt. Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich.

Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer/innen ohne Vorkenntnisse im Programmieren geeignet.

260105 Objektorientiertes Programmieren in C++

Objektorientierte Programmierung wird einerseits als wichtiger Schritt in Richtung ingenieurmäßige Software-Erstellung gesehen, andererseits ist sie das „natürliche" Programmier-Paradigma für einige Klassen von Anwendungen, wie z. B. grafische Oberflächen und Simulationen.

In dieser Lehrveranstaltung werden die Prinzipien der objektorientierten Programmierung vorgestellt und mit Hilfe der Programmiersprache C++ demonstriert. C++, eine Erweiterung der Programmiersprache C um objektorientierte Elemente, wurde Ende 1997 von ANSI und ISO standardisiert. Implementierungen der Sprache gibt es praktisch für alle Betriebssysteme und Rechnertypen.

In der Lehrveranstaltung werden die Programmiersprache und Teile der Standardbibliothek gemäß ISO/ANSI-Standard vorgestellt. Sie ist als weiterführende Veranstaltung konzipiert; Grundkenntnisse in C oder C++ werden vorausgesetzt.

260110 Erstellen dynamischer Webseiten mit PHP

Viele Internet-Provider bieten ihren Kunden inzwischen an, eigene Webseiten mit Hilfe von PHP dynamisch zu gestalten. PHP ist eine Programmiersprache, deren Befehle in HTML-Seiten eingebettet werden und die darüber hinaus eine Vielzahl von Unterprogrammbibliotheken mitbringt, etwa für Datenbankzugriffe, E-Mail-Verschicken und vieles mehr.

Beispiel für eine PHP-Anwendung ist ZIVprint, das Programm, mit dem man Druckdateien vorher anschauen und dann zu einem der zentralen Drucker des Zentrums für Informationsverarbeitung (ZIV) leiten kann.

In dieser Veranstaltung sollen sowohl die Elemente der Sprache als auch konkrete Projekte wie ZIVprint und ZIVlehre vorgestellt werden. Dabei wird als Datenbank MySQL näher betrachtet. Programmierkenntnisse (die Sprache ist egal) sollten vorhanden sein.

260124 Einführung in SQL: Ein Vergleich der SQL-Implementierungen von DB2 und MySQL

SQL (Structured Query Language) ist die standardisierte Schnittstelle zu relationalen Datenbanken. Mit SQL-Anweisungen werden etwa Datenbankobjekte verwaltet, Daten und Tabellen gespeichert und abgefragt, sowie Zugriffsrechte vergeben.

Die Vorlesung führt in SQL ein und vergleicht zugleich prominente Vertreter der freien und kostenpflichtigen Datenbanksysteme (MySQL und DB2) in ihren SQL-Implementierungen.

260143 Windows Scripting für Administratoren

Mit dem Windows Script Host (WSH) und der Skriptsprache Visual Basic Script lassen sich so gut wie alle wichtigen Funktionen eines Windows-Betriebssystems effizient automatisieren.

Die Vorlesung bietet eine Einführung in Visual Basic Script und das WSH-Objektmodell. Die verschiedenen WSH-Objekte ermöglichen u. a. einfachen Netzwerk- und Dateisystem-Zugriff. Weitere Themen sind die Behandlung des Active Directory Service Interfaces (ADSI) zur Benutzer- und Gruppenverwaltung innerhalb von Windows-Domänen und Beispiele für skriptgesteuerte Datenbankzugriffe mit ActiveX Data Objects (ADO).

Die Veranstaltung richtet sich an Hörer/innen mit Vorkenntnissen in Windows NT/2000.

260158 Rechnernetze und Internet: Fortgeschrittene Themen

Folgende Themen sollen behandelt werden:

1. IP-Routing-Protokolle
2. IP-Multicast
3. virtuelle Netzstrukturen: VLANs, ELANs, VPN
4. Zugangstechnologien: Modem, ISDN, ADSL
5. Sicherheit in Rechnernetzen
6. Netzwerkpolicies
7. Multimediaanwendungen in Datennetzen
8. Netzwerkmanagement
9. Ethernet-Troubleshooting
10. ATM: Asynchronous Transfer Mode

260162 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom ZIV verwendet werden.

Anhand dieser Zusammenstellung können Sie die Echtheit aller Schlüssel der Zertifizierungsstellen der Universität Münster und des DFN überprüfen, vgl. `http://www.uni-muenster.de/WWUCA/`, `http://www.dfn-pca.de` und die Übersichtsartikel in früheren i -Ausgaben.

PGP-Schlüsseldaten der WWUCA

WWUCA-Zertifizierungsschlüssel für 2002-2003:

Zertifizierungsstelle Universitaet Muenster 2002-2003
KeyID: BC811EB1, Schlüssellänge 2048 Bits, Erstellungsdatum: 2001/11/14
Key fingerprint = 28 64 01 BC F0 EF D5 BA D9 A0 86 6C 43 79 4C 1D

WWUCA-Zertifizierungsschlüssel für 2000-2001:

Zertifizierungsstelle Universitaet Muenster 2000-2001
KeyID: 313C02F5, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/03/24
Key fingerprint = 37 62 F5 E0 C2 78 76 97 53 0F 2D F2 F3 B3 27 F5

Alter Zertifizierungsschlüssel (nur durch DFN-User-CA zertifiziert):

Rainer Perske +49(251)83-31582 Certification Key
KeyID: EF750F1D, Schlüssellänge 2048 Bits, Erstellungsdatum: 1997/10/14
Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF

PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die WWUCA:

Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
KeyID: 4CB7658D, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/07/06
Key fingerprint = 38 3D 0F 16 CE FC 1F 9E B7 C3 04 B1 20 20 FC E6

PGP-Schlüsseldaten der DFN-PCA

DFN-PCA-Wurzelschlüssel für 2002-2003:

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
KeyID: F2D58DB1, Schlüssellänge 2048 Bits, Erstellungsdatum: 2001/11/20
Key fingerprint = DE 31 69 0D BC 6A E7 79 4D CD A1 B5 81 80 FE 7B

DFN-PCA-Wurzelschlüssel für 2001:

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001) <not-for-mail>
KeyID: 63EB5391, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/12/28
Key fingerprint = CF AF 6C 29 4E 57 4E 0E E8 1C BD B4 54 FD 2A AB

DFN-PCA-Wurzelschlüssel für 1999-2000:

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000) <not-for-mail>
KeyID: F7E87B9D, Schlüssellänge 2048 Bits, Erstellungsdatum: 1998/12/29
Key fingerprint = 65 70 72 74 B5 E0 3F F0 EA 7C AB E4 46 5F B8 B2

DFN-PCA-Wurzelschlüssel für 1997-1998:

DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998) <not-for-mail>
KeyID: 35DBF565, Schlüssellänge 2048 Bits, Erstellungsdatum: 1997/04/16
Key fingerprint = 09 7C 09 19 D3 C3 86 DC 7A 30 15 11 12 95 8D E3

PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die DFN-PCA:

DFN-PCA, ENCRYPTION KEY <dfnpca@pca.dfn.de>
KeyID: E77ADB85, Schlüssellänge 2048 Bits, Erstellungsdatum: 1998/04/21
Key fingerprint = 48 BE 74 79 7F 5D BD 4C 65 2B 98 53 DD 5A 03 05

Alle Angaben zur DFN-PCA ohne Gewähr.

X.509-Zertifikatdaten der WWUCA

WWUCA-Zertifikat für 2002-2003 plus 2 Jahre:

Serial Number: 1774668 (0x1b144c)
Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Validity
Not Before: Jan 1 00:00:00 2002 GMT
Not After : Dec 31 23:59:59 2005 GMT
Subject: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
Fingerprints:
MD5: a4:31:ad:41:d8:f2:18:56:4e:31:cc:69:71:e6:17:4f
SHA1: 69:45:20:ca:1a:fe:5c:fa:6c:37:52:eb:b7:72:b0:54:90:ec:d9:79

WWUCA-Zertifikat für 2000-2001:

Serial Number: 16 (0x10)
Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
Validity
Not Before: Jun 5 15:35:24 2000 GMT
Not After : Jun 5 15:35:24 2002 GMT
Subject: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2000-2001/Email=ca@uni-muenster.de
Fingerprints:
MD5: da:e3:e2:5d:bc:93:ef:03:37:96:4e:25:c1:ab:2b:d1
SHA1: a7:64:55:75:e0:ad:9a:2c:0c:b4:c8:ed:be:e0:bf:d4:72:6c:5c:b2

X.509-Zertifikatdaten der DFN-PCA

DFN-PCA-Wurzelzertifikat für 2002-2005 plus 4 Jahre:

Serial Number: 1429501 (0x15cffd)
Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Validity
Not Before: Dec 1 12:11:16 2001 GMT
Not After : Jan 31 12:11:16 2010 GMT
Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Fingerprints:
MD5: 3e:1f:9e:e6:4c:6e:f0:22:08:25:da:91:23:08:05:03
SHA1: 8e:24:22:c6:7e:6c:86:c8:90:dd:f6:9d:f5:a1:dd:11:c4:c5:ea:81

DFN-PCA-Wurzelzertifikat für 1998-2001:

Serial Number: 1 (0x1)
Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
Validity
Not Before: Oct 29 18:03:10 1998 GMT
Not After : Dec 31 18:03:10 2001 GMT
Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
Fingerprints:
MD5: 45:bb:9b:c8:8a:a4:84:8b:2d:a0:08:8f:9e:b6:b8:10
SHA1: df:a5:6f:b5:fc:41:e3:a8:92:1f:77:ad:16:22:ee:fd:91:52:a5:ad

Alle Angaben zur DFN-PCA ohne Gewähr.

Liebe Leserin, lieber Leser,

wenn Sie i regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von i nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion i

~ Ich bitte um Aufnahme in den Verteiler.
~ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
~ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

_____

~ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

An die
Redaktion i
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)
Ich bin damit einverstanden, dass diese Angaben in der i -Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift