Internettechnologien

Prof. Dr. Hans-Jürgen Buhl

Wintersemester 2002/03

Bergische Universität Wuppertal
Fachbereich Mathematik

Inhaltsverzeichnis

0. Einleitung

Internet

In Zeiten der weltweiten Vernetzung, der rapiden Zunahme von Zahlungen und Geschäften via WWW sind Internettechnologien von immer größerer Bedeutung.
Was aber genau bedeutet eigentlich das Wort *internet* bzw. *Internet*? Eine Suche im frei nutzbaren `On-line Dictionary of Computing` gibt Aufschluß:

Aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=internet:

---

internet

<networking>(Note: not capitalised) Any set of networks interconnected with routers. The Internet is the biggest example of an internet. (1996-09-17)

Aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=Internet:

Search Home Contents Feedback Random

Internet

<networking>(Note: capital "I"). The Internet is the largest internet (with a small "i") in the world. It is a three level hierarchy composed of backbone networks, mid-level networks, and stub networks. These include commercial (.com or .co), university (.ac or .edu) and other research networks (.org, .net) and military (.mil) networks and span many different physical networks around the world with various protocols, chiefly the Internet Protocol.

Until the advent of the World-Wide Web in 1990, the Internet was almost entirely unknown outside universities and corporate research departments and was accessed mostly via command line interfaces such as telnet and FTP. Since then it has grown to become an almost-ubiquitous aspect of modern information systems, becoming highly commercial and a widely accepted medium for all sort of customer relations such as advertising, brand building, and online sales and services. Its original spirit of cooperation and freedom have, to a great extent, survived this explosive transformation with the result that the vast majority of information available on the Internet is free of charge.

While the web (primarily in the form of HTML and HTTP) is the best known aspect of the Internet, there are many other protocols in use, supporting applications such as electronic mail, Usenet, chat, remote login, and file transfer.

There were 20,242 unique commercial domains registered with InterNIC in September 1994, 10% more than in August 1994. In 1996 there were over 100 Internet access providers in the US and a few in the UK (e.g. the BBC Networking Club, Demon, PIPEX).

There are several bodies associated with the running of the Internet, including the Internet Architecture Board, the Internet Assigned Numbers Authority, the Internet Engineering and Planning Group, Internet Engineering Steering Group, and the Internet Society.

See also NYsernet, EUNet.

http://www.openmarket.com/intindex - statistics about the Internet.

(2000-02-21)

Eine Möglichkeit der Internetnutzung ist der Austausch von (elektronischen) Nachrichten: email.

Was für eine Gaphik?

Leider wird die email-Nutzung heute sehr stark gestört durch

SPAM — Eine Plage im Internet

Unter SPAM versteht man im „elektronischen Post“-Bereich die Versendung unerwünschter, unangeforderter Massenwurfsendungen (meist Werbung zweifelhafter Herkunft und oft auch zweifelhaften Inhalts). http://dict.leo.org?search=spam übersetzt

2 Treffer für 'spam'

ENGLISCH	**DEUTSCH**
Spam©[Amer.]	das Frühstücksfleisch
spam [comp.]	elektronisches Äquivalent unerwünschter Wurfsendungen

Abbildung 0.1.: Quelle: http://dict.leo.org?search=spam

und http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam erläutert

spam

1. <messaging> (From Hormel's Spiced Ham, via the Monty Python "Spam" song) To post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists, or other messaging system in deliberate or accidental violation of netiquette.

It is possible to spam a newsgroup with one well- (or ill-) planned message, e.g. asking "What do you think of abortion?" on soc.women. This can be done by cross-posting, e.g. any message which is crossposted to alt.rush-limbaugh and alt.politics.homosexuality will almost inevitably spam both groups. (Compare troll and flame bait).

Posting a message to a significant proportion of all newsgroups is a sure way to spam Usenet and become an object of almost universal hatred. Canter and Siegel spammed the net with their Green card post.

If you see an article which you think is a deliberate spam, DO NOT post a follow-up - doing so will only contribute to the general annoyance. Send a polite message to the poster by private e-mail and CC it to "postmaster" at the same address. Bear in mind that the posting's origin might have been forged or the apparent sender's account might have been used by someone else without his permission.

The word was coined as the winning entry in a 1937 competition to choose a name for Hormel Foods Corporation's "spiced meat" (now officially known as "SPAM luncheon meat"). Correspondant Bob White claims the modern use of the term predates Monty Python by at least ten years. He cites an editor for the Dallas Times Herald describing Public Relations as "throwing a can of spam into an electric fan just to see if any of it would stick to the unwary passersby."

Usenet newsgroup: news.admin.net-abuse.

See also http://www.nightflight.com/foldoc-bin/foldoc.cgi?netiquette

2. (A narrowing of sense 1, above) To indiscrimately send large amounts of unsolicited e-mail meant to promote a product or service. Spam in this sense is sort of like the electronic equivalent of junk mail sent to „Occupant".

In the 1990s, with the rise in commercial awareness of the net, there are actually scumbags who offer spamming as a „service" to companies wishing to advertise on the net. They do this by mailing to collections of e-mail addresses, Usenet news, or mailing lists. Such practises have caused outrage and aggressive reaction by many net users against the individuals concerned

Abbildung 0.2.: Quelle: http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam

SPAM-Nachrichten sehen im allgemeinen folgendermaßen aus:

```
Received: from [217.223.62.15] (helo=web.com)
by mx09.web.de with smtp (WEB.DE(Exim) 4.93 #56)
id 18L4iM-0001M6-00; Sun, 08 Dec 2002 17:55:34 +0100
Message-ID: <000c63e43c8e$1361a2a2$2dd66ac6@dyssus>
From: "Steffi" <steffivf406@web.com>
To: Markus
Subject: Ich habe Dich vermisst!
Date: Mon, 09 Dec 2002 01:27:32 -0900
Sender: steffivf406@web.com

Hallo,
jemand der sich in dich verliebt hat aber sich nicht traut es dir persönlich zu
sagen hat eine Foto Nachricht für dich hinterlassen.

Wenn du wissen willst wer dir eine Nachricht hinterlassen hat, so gehe auf unsere
Seite und wähle die Nachricht mit der Nummer Pt-224885 und benutze das Kennwort:
Pt-224live

Solltest du unsere Livesoftware noch nicht installiert haben, kannst du das jetzt
machen indem du auf folgenden Link klickst:

http://213.76.131.85/?account=dkm-10129&layout=layoutdp4&land=de&exename=live-software

Du wirst dann automatisch in unseren Mitgliederbereich geleitet.

Viel Spaß

SH Partnervermittlung



WERBUNG
==
JETZT NEU: Private Kontakte aus Deiner Stadt
http://66.46.145.36/members/testzugang01/
==
```

Abbildung 0.3.: SPAM-Nachrichten: Werbung

```
Return-Path: <m_bundu1@rediffmail.com>
Delivered-To:
Received: (qmail 29004 invoked by uid 4216); 8 Dec 2002 15:07:56 -0000
Received: from unknown (HELO 218.5.135.42) (218.5.135.42)
  by mail.telebel.de with SMTP; 8 Dec 2002 15:07:56 -0000
Received: from rly-xl04.mx.aol.com ([161.143.46.72]) by m10.grp.snv.yahoo.com with QMQP;
          Dec, 08 2002 6:43:00 AM -0700
Received: from 213.54.67.154 ([213.54.67.154]) by sparc.isl.net with esmtp;
Subject: Assistance
Sender: Michael Bundu <m_bundu1@rediffmail.com>

FROM: COL. MICHAEL BUNDU.
DEMOCRATIC REPUBLIC OF CONGO.
Tel No: Your country Intl. access code +8821652098236
email : mik_bundu1@rediffmail.com
Dear Sir/Madam


SEEKING YOUR IMMEDIATE ASSISTANCE.

Please permit me to make your acquaintance in so informal a manner. This is necessitated
by my urgent need to reach a dependable and trust worthy foreign partner. This request may
seem strange and unsolicited but I crave your indulgence and pray that you view it seriously.
My name is COL. MICHAEL BUNDU of the Democratic Republic of Congo and one of the close
aides to the former President of the Democratic Republic of Congo LAURENT KABILA of blessed
memory, may his soul rest in peace.

Due to the military campaign of LAURENT KABILA to force out the rebels in my country, I
and some of my colleagues were instructed by Late President Kabila to go abroad to purchase
arms and ammunition worth of Twenty Million, Five Hundred Thousand United States Dollars
only (US$20,500,000.00) to fight the rebel group. We were then given this money privately by
the then President, LAURENT KABILA, without the knowledge of other Cabinet Members. But
when President Kabila was killed in a bloody shoot-out by one of his bodyguards a day before
we were schedule to travel out of Congo, We immediately decided to put the funds into a private
security company here in Congo for safe keeping. The security of the said amount is presently
being threatened here following the arrest and seizure of properties of Col. Rasheidi Karesava
(One of the aides to Laurent Kabila) a tribesman, and some other Military Personnel from our
same tribe, by the new President of the Democratic Republic of Congo, the son of late President
Laurent Kabila, Joseph Kabila.
...
```

Abbildung 0.4.: SPAM-Nachrichten: Bitte um Unterstützung

Häufig sind sie noch darüber hinaus falsch codiert oder aber mit unsinnigen Zeitangaben der Versendung versehen. Auf jeden Fall stimmt die Absendeadresse nicht.

```
Return-Path: <Marshamaxi@id.ru>
Delivered-To:
Received: (qmail 1197 invoked by uid 4216); 8 Dec 2002 16:11:46 -0000
Received: from unknown (HELO yuwpd) (200.160.248.74)
  by mail.telebel.de with SMTP; 8 Dec 2002 16:11:46 -0000
From: Elena Palik <Marshamaxi@id.ru>
To:
Subject: Information sven.b1
Date: Sun, 08 Dec 2002 07:10:44 -0500
Mime-Version: 1.0
Message-Id: <aounwrravnxv@id.ru>

PEhUTUw+PFAgQUxJRO49Q0VOVEVSPjxGT05UICBTSVpFPTYgUFRTSVpFPTI0PjxCPnN2ZW4u
YjEsPEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iI2ZmMDAwMCIgQkFDSz0iI2ZmZmZmZiIg
c3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJWkU9MjQgRkFN
SUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48VT5Zb3UgaGF2ZSBiZWVu
IGFwcHJvdmVkLjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiNmZjAwMDAiIEJBQOs9IiNm
ZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTUgUFRTSVpF
PTE4IEZBTUlMWT0iUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORz0iMCI+PC9VPkNhc2gg
R3JhbnQgQW1vdW50OjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiMwMDAwZmYiIEJBQOs9
IiNmZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTcgUFRT
SVpFPTM2IEZBTUlMWT0iUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORz0iMCI+JDEwLDAw
MC0kNSwwMDAsMDAwPEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iIzAwMDAwMCIgQkFDSz0i
I2ZmZmZmZiIgc3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJ
WkU9MjQgRkFNSUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48ST48VT5E
aWQgWW91IEtub3c/PEJSPgOKPC9GTO5UPjxGTO5UICBDTOxPUj0iIzAwMDAwMCIgQkFDSz0i
I2ZmZmZmZiIgc3R5bGU9IkJBQOtHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NSBQVFNJ
WkU9MTggRkFNSUxZPSJTQU5TUOVSSUYiIEZBQOU9IkFyaWFsIiBMQU5HPSIwIj48LOI+PC9J
```

Abbildung 0.5.: SPAM-Nachrichten: unbrauchbar, falsch codiert

Leider wird erst jetzt sehr zögerlich etwas vom Gesetzgeber und der Rechtssprechung gegen SPAM unternommen:

US-Urteil gegen Spam-Versender

Über 98.000 US-Dollar soll der US-Amerikaner Jason Heckel für das Versenden von Spam-Mails bezahlen. Er verlor das Berufungsverfahren vor dem obersten Gericht des Staates Washington. Zuvor hatte ein Richter eine einzige E-Mail als ausreichenden Beweis für Heckels illegale Spam-Aktivitäten gewertet. Die Anklage warf Heckel vor, seit 1998 zwischen 100.000 und einer Million unerwünschte Werbesendungen pro Woche verschickt zu haben.

Die eigentliche Strafe von 2000 US-Dollar dürfte Heckel dabei kalt lassen. Schließlich soll er jahrelang pro Monat dreißig bis fünfzig Exemplare seiner 46-seitigen Online-Broschüre "How to Profit from the Internet" verkauft haben, für die er in den Mails geworben hat. Doch zusätzlich muss er nun auch Gerichtskosten von über 96.000 US-Dollar tragen. Heckels Anwalt kündigte an, das Urteil anzufechten. Gelingt ihm dies nicht, dürfte es in den USA als Präzedenzfall eine ganze Welle von Klagen gegen Spam-Versender nach sich ziehen.

Washington erließ 1998 als erster US-Bundesstaat ein E-Mail-Gesetz. Es stellt Werbe-Mails mit irreführendem Inhalt oder einer Absenderadresse, auf die man nicht antworten kann, unter Strafe. Inzwischen haben aber auch andere US-Staaten ähnliche Gesetze erlassen. Das nährt die Hoffnung, dass in den USA, von wo auch sehr viele Spam-Mails nach Deutschland kommen, bald gegen die Verursacher der Plage vorgegangen wird.

Mit der Internet-Seuche Spam befasst sich c't in der aktuellen Ausgabe 22/02 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (ad/c't)

Abbildung 0.6.: Quelle: heise online
`http://www.heise.de/newsticker/data/ad-20.10.02-002/`

Man beachte dabei, dass viele SPAM-Nachrichten auch HTML-Code verwenden. Dieser HTML-Code ist aber alles andere als sicher einzuschätzen, da auf dem eigenen Rechner Skripte ausgeführt werden und somit unter anderem Viren in das System eindringen können.
Gerade Newsreader wie Microsoft Outlook (Express) sind dabei besonders anfällig, da sie sich in den neueren Versionen nur noch schwer sicher konfigurieren lassen.
Bei diesen Newsreadern ist es wichtig,

1. die Vorschau zu deaktivieren (denn auch diese führt Skripte aus),
2. kein Öffnen von Nachrichten zweifelhaften Inhalts durchführen.

Gerade im Zusammenhang mit Windows-Systemen ergeben sich daneben immer häufiger Probleme mit sogenannten Dialern, d.h. Programmen, welche im Hintergrund teure 0190-Telefonnummern anwählen:

Bundesregierung will besseren Dialer- und Spam-Schutz

Das Verbraucherschutzministerium dringt auf ein schärferes Vorgehen gegen die Dialer-Mafia. „Wir sehen die 0190-Problematik als einen Schwerpunkt dieser Legislaturperiode“, erklärte Georg Starke, Leiter des Referats für den wirtschaftlichen Schutz der Verbraucher im Hause von Ministerin Renate Künast, am heutigen Donnerstag am Rande einer Konferenz zur europaweiten Harmonisierung des Wettbewerbsrechts in Berlin. Die zweite Änderung der Telekommunikations-Verbraucherschutzverordnung, die Netzbetreiber zum Einrichten kostenloser Service-Nummern verpflichtet und von vielen Seiten als unzweckmäßig kritisiert wurde, sei nur „ein erster Schritt“ gewesen. Weiter gehende Schutzmaßnahmen sollen laut Starke in die anstehende und von der Branche mit Spannung erwartete Novelle des Telekommunikationsgesetzes (TKG) einfließen, für die das Wirtschaftsministerium federführend verantwortlich ist.

Wie groß das Problem mit der Abzocke über 0190-Dialer im Internet oder der Werbespam für 0190-Nummern per SMS und E-Mail ist, erfährt das Verbraucherministerium ständig am eigenen Leib. „Wir erhalten täglich unzählige Eingaben und Beschwerden zu diesem Thema“, sagte Starke. „Sie pflastern uns den Schreibtisch zu.“ Momentan prüfe sein Haus noch zusammen mit dem Wirtschafts- und Justizressort, wie der Missbrauch effektiv einzudämmen ist. Konkret kann sich der Ministerialbeamte vorstellen, „verstärkt die Regulierungsbehörde für Telekommunikation und Post in die Verantwortung zu nehmen“ und so den schwarzen Schafen unter den Anbietern zu Leibe zu rücken. Bisher sind diese von den Netzbetreibern oft nur schwer zu ermitteln; eine effektive Datenbank mit einer Übersicht über die einzelnen 0190-Dienstleister existiert nicht.

Auch im Bereich E-Mail-Spam sieht Starke Handlungsbedarf. „Bisher sind die ungewünschten Werbezusendungen nicht im Telekommunikationsgesetz erfasst“, bemängelt der Regierungsvertreter. Auch hier will das Verbraucherschutzministerium im Laufe der TKG-Novelle nachbessern. Ein großes Problem sieht Ursula Pachl vom Bureau Européen des Unions de Consommateurs, dem Dachverband der europäischen Verbraucherschutzorganisationen, allerdings nach wie vor bei internationalen Spam-Versendern, hauptsächlich aus den USA. Mit den Partnerschaftsverbänden jenseits des Atlantiks arbeite ihre Institution an einer Lösung. Über „Selbstregulierungsmaßnahmen“ der Wirtschaft gehen die Überlegungen bislang aber nicht hinaus.

Für die deutschen Wahrer der Konsumentenrechte ist die gesamte Thematik Spam und 0190-Nummern im vergangenen Jahr zum Dauerärgernis geworden. „Wir erleben einen zunehmenden Wildwuchs in der Werbung, der sich vor allem durch die Neuen Medien ergibt“, sagt Edda Müller, Vorstand Verbraucherzentrale Bundesverband (VZBV). Immer mehr Firmen würden teure 0190-Nummern verwenden, um bei den Verbrauchern „in wettbewerbswidriger Weise abzukassieren“. Zahlreiche Fälle seien aus der Gewinnspielwerbung bekannt oder im Zusammenhang des vermeintlichen „Abbestellens“ von unerwünschten kommerziellen Faxen.

Abbildung 0.7.: Quelle: heise online
http://www.heise.de/newsticker/data/jk-31.10.02-006/

Der Konsument sei dagegen größtenteils machtlos, da sich die Möglichkeiten für Abmahnungen und Unterlassungserklärungen im Gesetz gegen den unlauteren Wettbewerb (UWG) als „zahnlos“ erweisen hätten. Selbst wenn eine Firma eindeutig eines Verstoßes gegen das UWG überführt worden sei, könnten die betroffenen Verbraucher keine Schadensersatzansprüche einklagen. Eine entsprechende Vorkehrung wollen die Verbraucherschützer nun aber im Rahmen der in Brüssel in den nächsten Wochen anstehenden Verhandlungen zur Harmonisierung des europäischen Wettbewerbrechts und des Grundbuchs zum Verbraucherschutz für alle Mitgliedsländer fordern. Eine „Strohmannklausel“ soll ferner verhindern, dass zwielichtige Anbieter unter Postfachadressen auf dem Markt auftreten können.

Mit der Internet-Seuche Spam befasst sich c’t in der Ausgabe 22/2002 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (Stefan Krempl) / (jk/c’t)

Abbildung 0.8.: Quelle: heise online Fortsetzung
`http://www.heise.de/newsticker/data/jk-31.10.02-006/`

Regierung legt Gesetzentwurf gegen 0190-Missbrauch vor

Die Bundesregierung hat einen ersten Referentenentwurf für das neue „Gesetz zur Bekämpfung des Missbrauchs von Mehrwertdiensterufnummern“ vorgelegt. Kernstück ist die geplante Änderung des Telekommunikationsgesetzes (TKG). Ein neuer Paragraf 43a soll jeden Anbieter, der eine 0190- oder 0136-0138-Nummer zur Nutzung überlassen bekommen hat, dazu verpflichten, eine ladungsfähige Anschrift bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) zu hinterlegen.

Die RegTP selbst soll diese Angaben in Form einer Datenbank im Internet der Öffentlichkeit zugänglich machen. Außerdem soll jedermann einen Anspruch darauf haben, die Daten telefonisch erfragen zu können. Bei Verstoß gegen die Meldepflicht „kann die Zuteilung der Rufnummer durch die Regulierungsbehörde widerrufen werden“, heißt es im Gesetzentwurf. Von weiteren Sanktionierungsmaßnahmen wie etwa der Verhängung eines Bußgeldes findet sich, anders als noch im Konzeptpapier, nichts mehr im Gesetzentwurf.

Bei der Preiskappungsgrenze ist das Bundesministerium für Wirtschaft und Arbeit (BMWA) dagegen sogar noch weiter gegangen: Die Kosten für eine über frei tarifierbare Rufnummern abgerechnete Einwahl sollen demnach 30 Euro künftig nicht überschreiten dürfen. Vorgesehen waren hier zunächst 120 Euro pro Anruf. Wird entsprechend der Länge der Verbindung abgerechnet, soll das Entgelt auf zwei Euro pro Minute begrenzt werden. Abgerechnet werden soll mit einem Takt von einer Länge von maximal 60 Sekunden.

Hintergründe, erste Reaktionen und Einschätzungen zu dem Gesetzentwurf gegen 0190-Missbrauch finden sich im Artikel auf c’t aktuell:

Erster Gesetzentwurf gegen 0190-Missbrauch
`http://www.heise.de/ct/aktuell/data/hob-18.12.02-000/`

(hob/c’t)

Abbildung 0.9.: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-18.12.02-001/`

Spam auf dem gerichtlichen Prüfstand

Der Heise-Zeitschriften-Verlag, der die Zeitschriften iX und c't, das Online-Magazin Telepolis und den Newsdienst auf heise online herausgibt, klagt vor dem Amtsgericht Hannover gegen die Firma Online-Marketing Albrecht, nachdem diese Verlagsmitarbeiter trotz einer Unterlassungsaufforderung weiterhin mit Spam-E-Mails bombardiert hatte. Dabei beruft sich der Verlag unter anderem auf die neue EU-Datenschutzrichtlinie, in der für E-Mail-Werbung ein klares „Opt-in" bestimmt wird. Diese Richtlinie ist bis zum 31. Oktober 2003 in nationale Gesetzgebung umzusetzen, sollte aber bereits jetzt Einfluss auf die deutsche Rechtsprechung haben.

Unter dem Namen „emailfuchs" versendet Bernd Albrecht in Wellen unverlangt Werbe-E-Mails an deutsche Adressen. In den Newslettern wird für Webshops, beispielsweise einen Berufsbekleider und einen Uhrenhändler, geworben. Als auch Mitarbeiter von heise online solche E-Mails erhalten hatten, forderte Heise Online-Marketing-Albrecht unter Fristsetzung auf, den unerbetenen Versand solcher Werbe-Mails zu unterlassen. Kurz danach liefen erneut Albrecht-Newsletter bei uns auf. Anstatt die entsprechende strafbewehrte Unterlassungserklärung zu unterschreiben und die Adressen des Verlages aus seinem Verteiler zu streichen, konterte Albrecht mit harsch formulierten E-Mails an den Verlag.

Der überzeugte Spammer hält es für rechtmäßig, unverlangte Werbe-E-Mails zuzusenden. Und: „Sie werden es nicht schaffen, unseren kostengüstigen und schnellen Newsletter-Versand an Millionen Leser zu blockieren", gab er sich kampfbereit. „Denken Sie daran, dass unsere Auflage weit höher ist als ihre", schrieb Albrecht und sprach von einer Pressekampagne mehrerer Verlage gegen ihn. Albrecht rechtfertigte sein Tun unter anderem unter ökologischen Gesichtspunkten: „Im Gegensatz zu den Printmedien müssen für unsere Informationen keine Bäume vernichtet werden, um eine Zeitung mit viel Werbung drucken zu müssen."

Nach Ansicht von Joerg Heidrich, Justiziar des Heise-Verlags, hat Albrecht freilich wenig Chancen, sein zweifelhaftes Anliegen vor Gericht durchzusetzen. Bis auf wenige Ausnahmen sei man inzwischen in Rechtssprechung und juristischer Literatur einhellig der Meinung, dass die unerwünschte und unaufgeforderte Zusendung von E-Mails rechtswidrig sei. Das Versenden solcher Nachrichten gegenüber Privatpersonen gilt dabei meist als Verletzung des allgemeinen Persönlichkeitsrechts des Betroffenen.

Unternehmen und Gewerbetreibende können sich auf einen Eingriff in den sogenannten „eingerichteten und ausgeübten Gewerbebetrieb" nach §§823, 1004 BGB berufen und ebenfalls Unterlassung verlangen. Ist der Empfänger der Spam-Mail darüber hinaus noch in einem ähnlichen Bereich gewerblich tätig wie der Versender, so steht ihm zusätzlich ein wettbewerbsrechtlicher Unterlassungsanspruch aus §1 UWG zu. Ein Anspruch auf Schadensersatz bei den Empfängern besteht dagegen nach bisheriger Rechtsprechung nicht. Insbesondere aufgrund der neuen EU-Richtlinie, die hinsichtlich unverlangter Werbezusendungen erstmals ein klares Verbot ausspricht, sieht Heidrich sehr gute Aussichten für die eingereichte Klage. (hob/c't)

Abbildung 0.10.: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-04.12.02-000/`

Was tun gegen Spam(`http://spam.trash.net/was.shtml`)?

Unter http://spam.trash.net/tun.shtml ist erläutert, wie Sie Spam in Zukunft vermeiden können, was Sie tun können, wenn Sie bereits spam erhalten haben, ...

- Auf keine Fall sollten Sie den Aufforderungen der Spam-Nachrichten nachkommen.
- Die Spam-Nachrichten sollten sofort gelöscht werden. Bei nur wenigen Nachrichten reicht oft noch das manuelle Löschen.
- Da die Spam-Mails immer mit neuen Absenderadressen auftauchen, helfen Einträge in lokale Filterlisten oft sehr wenig. Bei der Filterung nach Stichworten (z.B. Sex, Porn, etc.) werden leider auch gerne reguläre e-mails ausgefiltert. ...

Filtern im Netscape-Communicator:

- Eine Netscape Filterbeschreibung finden Sie unter
  (http://www.pvc.maricopa.edu/cc/training/faqs/memo/filters.htm.
- Für Outlook Express vergleiche diese Seite http://www.inboxprotector.com/.

Weitere Informationen finden Sie zum Beispiel unter:

- http://www.antispam.de/
- Information zum Thema Spam
  (`http://spam.trash.net/index.shtml`)
- DFN-CERT Informationsbulletin Spam
  (`http://www.cert.dfn.de/infoserv/dib/dib-9901.html`)
- Ratgeber Kampf gegen Spam
  (`http://www.wienerzeitung.at/aktuell/2001/antispam/default.htm`)
- HRZ-Anti-Spam an der BU Wuppertal
  (`http://w3.uni-wuppertal.de/hrz/dienste/netz/email/spam.html`)
- Junk Mail und SPAM
  (`http://w3.uni-wuppertal.de/hrz/infos/hrz-info/hrz-info-9806/node16.html`)
- Spam (Auflistung von anderen Spam-Seiten)
  (`http://directory.google.com/Top/Computers/Internet/Abuse/Spam/`)
- Reading Email Headers
  (`http://www.stopspam.org/email/headers/headers.html`)

- Uni Bremen: Maßnahmen gegen SPAM
  (`http://www.zfn.uni-bremen.de/zfn/dienste/mail/anti-spam.php3`)
- http://www.schnappmatik.de/TFFFFF/
- Uni Köln: Electronix Mail am RRZK: Spam
  (`http://www.uni-koeln.de/rrzk/mail/spam/`)
- Uni Köln: Spamassassin am RRZK
  (`http://www.uni-koeln.de/rrzk/mail/spam/spamassassin.html`)

Gericht untersagt den Versand unverlangter Newsletter-Aktivierungsmails

Nach den Anbietern von Grußkarten könnte es nun auch den Versendern von Online-Newslettern an den Kragen gehen. Nach Auffassung des Landgerichts Berlin stellt die unerwünschte Übersendung einer Newsletter-Anmeldung per E-Mail eine unzulässige Werbung dar.

Der Antragsteller des Beschlusses vom 19. September 2002 hatte eine E-Mail erhalten, in der er aufgefordert wurde, einen Aktivierungslink anzuklicken, um in einen Newsletter-Verteiler aufgenommen zu werden. Sofern er dies nicht wolle, solle er die Mail einfach löschen. Hierin sah der Antragsteller unerwünschte Werbung und beantragte den Erlass einer einstweiligen Verfügung gegen den Betreiber des Informationsservices.

Das Landgericht bestätigte in seiner Entscheidung nochmals die mittlerweile herrschende Auffassung, dass es sich bei dem unaufgeforderten Zusenden einer E-Mail mit Werbeinhalten gegenüber Gewerbetreibenden um einen unzulässigen Eingriff in den Gewerbebetrieb handelt. Privatpersonen steht unter den Gesichtspunkten des allgemeinen Persönlichkeitsrechts gegen den Versender der Mail ebenfalls ein Unterlassungsanspruch nach §§1004, 823 Abs. 1 BGB zu.

Die Einwendung des Newsletter-Betreibers, der Antragsteller hätte die Eintragung für die Mailingliste selbst vorgenommen, ließ das Gericht nicht gelten. Nachweispflichtig für die Eintragung in eine Liste sei stets der Betreiber des Angebotes. Diesen Beweis konnte der Anbieter jedoch nicht führen. Der Beschluss ist unter Juristen umstritten. Die der Entscheidung zugrundeliegende Art des Opt-In-Verfahrens bei der Anmeldung zum Bezug eines Newsletters ist im Internet weit verbreitet und galt bisher als rechtlich unbedenklich. (Joerg Heidrich) / (em/c't)

Abbildung 0.11.: Quelle: heise online
`http://www.heise.de/newsticker/data/em-02.11.02-000`

Spam-Versender muss sieben Millionen Dollar zahlen

AOL ist vor einem Gericht in Virginia ein wegweisendes Kunststück gelungen: Erfolgreich klagte das Unternehmen einen pornografischen Spam-Versender in den Bankrott. Das Urteil, hoffen Millionen, könnte Schule machen.

CN Productions kennt niemand, und doch haben Millionen Internet-Nutzer schon Post des Unternehmens im E-Mail-Empfangsordner gehabt. CN machte seine Profite mit Spam, unverlangt zugesandten Werbebotschaften. Das Unternehmen des bereits 1999 einschlägig verurteilten Jay Nelson gehörte zu den Pionieren des wohl meistgehassten Geschäftszweiges im Internet: pornografische Massenmailings.

Zum wohl endgültigen Verhängnis wurde Nelsons Firma nun ein Gesetz des US-Staates Virginia, das als Muster für den zunehmend härter geführten juristischen Kampf gegen die Müllversender gilt: Wegen Verstoßes gegen Auflagen des ersten Urteils wurde CN Productions zur Zahlung von sieben Millionen Dollar an AOL als geschädigtes Unternehmen verurteilt. Für den Pornowerber ist das der Ruin, und doch ist es fast ein mildes Urteil: Das Gesetz des Staates Virginia sieht Geldstrafen von bis zu 25.000 Dollar für einen Spambrief vor. Davon verschickte CN Productions allein an AOL-Adressen mehrere Milliarden.

Für AOL ist das ein wichtiger Sieg, von dem das Unternehmen erhofft, dass er Signalwirkung haben möge. AOL litt über Jahre unter dem Ruf, einerseits Heimat von Spam-Versendern zu sein, anderseits die eigenen User nicht davor schützen zu können.

Das Problem sind die E-Mail-Verzeichnisse von AOL, die von Spamern immer wieder gern „abgefischt“ werden: Mehr verifiziert gültige Adressen lassen sich kaum auf einen Schlag besorgen. Nutzer von AOL oder auch des Instant Messenger AIM konnten ein Lied davon singen: Es rappelte im Postfach. Heute dagegen liegt das AOL-Spam-Aufkommen sogar unter dem Durchschnitt. Der liegt - je nach Schätzung - mittlerweile bei 25 bis 50 Prozent.

AOL geht seit spätestens 1998 vehement gegen Spamer und ihre Aussendungen vor: „Wir haben die Schnauze so voll davon wie unsere Kunden“, sagte damals AOL-Chef Steve Case - und topfte ein Programm von Gegenmaßnahmen ein, die von Filtern über Rausschmisse und gerichtliche Klagen bis hin zu öffentlichen Prangern reichte. Schon 1998 landete CN Productions auf der AOL-Liste der zehn „meistgesuchten Spamer“. Vier Jahre später hat AOL seinen Peiniger erlegt, das Kopfgeld kassiert.

Abbildung 0.12.: Quelle: Spiegel Online

Internet, Extranet, VPNs

Intranet, Extranet, Internet als Intranet, VPNs

Bitte klären Sie die obigen Begriffe mit Hilfe von FOLDOC (`http://www.nightflight.com/foldoc-bin/foldoc.cgi`).

Eine Webfirmenpräsentation

Das Web stellt vielfältige Informationen benutzerfreundlich zur Verfügung.
Wir wollen uns typische Inhalte einer „Firmenpräsentation“ an Hand der Webseiten des Fachbereichs Mathematik der Universität Wuppertal genauer ansehen:
Wichtig ist neben einer klar gegliederten Webangebotsübersicht das Impressum, bestehend aus einem email-Link

`mailto:webmaster@math.uni-wuppertal.de`,

sowie der Postadresse inklusive Telefon-, Fax- und email-Adresse.

Impressum einer Homepage muss gut auffindbar sein

Das Impressum auf einer Homepage muss gut auffindbar und schnell zu erkennen sein. Das geht aus einem Beschluss des Landgerichts Hamburg hervor (Az.: 416 O 94/02), über den die Zeitschrift Verbraucher und Recht in der Ausgabe 11/2002 berichtet. So müsse das nach Paragraf 6 des Teledienstegesetzes vorgeschriebene Impressum auf der Startseite auch eindeutig gekennzeichnet werden.

In dem verhandelten Fall hatte ein Anbieter von Edutainment-Software das Impressum auf seiner Homepage unter dem Unterpunkt „Backstage“ geführt. Dagegen hatte ein Konkurrenzunternehmen Beschwerde eingelegt mit der Begründung, die Bezeichnung aus der Bühnensprache sei nicht allgemein geläufig. Der Rechtsstreit wurde beigelegt, nachdem das beklagte Unternehmen sich verpflichtete, die Angaben zu Namen und Anschrift des Anbieters künftig als „Impressum/Infos“ zu kennzeichnen.
(dpa) / (anw/c’t)

Abbildung 0.13.: Quelle: heise online
`http://www.heise.de/newsticker/data/anw-21.11.02-003`

Verstoß gegen Web-Impressumspflicht wettbewerbswidrig

Ein Verstoß gegen die Kennzeichnungspflicht auf Websites nach §§3, 6 des Teledienstegesetzes (TDG) ist wettbewerbswidrig im Sinne der §§1 und 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Dies entschied das Landgericht Düsseldorf nach Berichten von Jur-Text und erließ am 7. und 25. November zwei entsprechende einstweilige Verfügungen (Az. 34 O 172/02, Az. 34 O 188/02).

Die Frage, ob die Regelungen des neuen TDG einen Verstoß gegen Wettbewerbsrecht begründen können, war bislang zwischen Juristen umstritten. Die 12. Kammer des Landgerichts Düsseldorf (Az. 12 O 311/01) sowie das Landgericht Hamburg (Az. 312 O 512/00) hatten eine solche Haftung noch mit der Begründung abgelehnt, die Regelungen des TDG über die Impressumspflicht stellten eine reine Ordnungsvorschrift da, die keinen wettbewerbsrechtlichen Charakter habe. Diese Entscheidungen bezogen sich jedoch noch auf das alte TDG, in dem die Impressumspflichten wesentlich weniger umfangreich festgelegt waren.

Nach Ansicht der Kammer für Handelssachen des Landgerichts Düsseldorf dienen die neugestalteten Vorschriften des TDG jedoch dem Kunden- und Mitbewerberschutz. Ein Verstoß gegen die Regelungen unterfällt demnach als „Vorsprung durch Rechtsbruch“ dem UWG. Nach Auskunft von Rechtsanwalt Tim Geißler war in einem der vorliegenden Fälle ein Impressum zwar als „Kontakt“ grundsätzlich vorhanden, es fehlten jedoch die ordnungsgemäße Bezeichnung des Unternehmens, die Angabe des Geschäftsführers, die notwendigen Angaben zur Handelsregistereintragung sowie die Angabe der Umsatzsteueridentifikationsnummer, die in § 6 TDG festgelegt sind. Ob gegen die Beschlüsse Rechtsmittel eingelegt werden, steht derzeit noch nicht fest.

Die Neuregelung des der Kennzeichnungspflichten des TDG war in den vergangenen Monaten die Grundlage für zahlreiche, zum Teil äußerst fragwürdige Serienabmahnungen. Jüngst hatte das LG Hamburg bereits eine auf einem Verstoß des TDG beruhende Abmahnung bestätigt. Website-Betreiber sind in jedem Fall gut beraten, ihre Online-Präsenz noch einmal kritisch auf eine korrekte Kennzeichnung zu überprüfen. (Joerg Heidrich) / (jk/c't)

Abbildung 0.14.: Quelle: heise online
`http://www.heise.de/newsticker/data/jk-26.11.02-005`

Daneben ist die Verfügbarkeit einer lokalen „Suchmaschine“ für den Inhalt des Firmen-Webauftritts bei einem größeren Informationsangebot schon fast Usus.

Ein Bereich der Homepage für (aktuelle) Neuigkeiten (eventuell durch dynamische Effekte hervorgehoben) solle nicht zu groß sein. Schließlich ist die Angabe des Datums der letzten Änderung der Seite sehr empfehlenswert. Dies sollte automatisch aus den Modifikationsdatum der zugehörigen Datei im Filesystem des Webservers geschehen, was zum Beispiel mittels der folgenden JavaScript-Funktion geschehen kann!

Listing 1: Letzte Änderung

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
<base href="http://www.math.uni-wuppertal.de/">
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<TITLE> Testseite
</TITLE>
</HEAD>

<body bgcolor=white>

<!-- ------------------------------------------------- -->

<noscript>
 <p><h3>   This page uses Javascript. Please enable Javascript
    features in your browser.</h3>
</noscript>


<script language="JavaScript" type="text/javascript">
<!-- hide to non JavaScript browsers
function ModDate()
{
lastmod = self.document.lastModified // last modified date
while (isNaN(lastmod.substring(0,1))) { lastmod = lastmod.substring(1,100) }
// delete Mo..So
return lastmod
}

window.status='Document last modified: '+ModDate();
// -->
</script>

<p>Dies ist meine Web-Testseite!
</p>

<hr>
<p>Hans Mustermann; </p>
<script type="text/javascript">
<!-- hide to non JavaScript browsers
document.writeln('Letztes Modifikationsdatum: ', ModDate());
// -->
</script>

<a href="http://validator.w3.org/check/referer"><img border="0" src="http://www.math.
    uni-wuppertal.de/images/valid-html401.gif"
alt="W3C HTML 4.01 checked" height="31" width="88" align="right">
</a>

</body>
</html>
```

Bemerkungen:

- Web-Seiten sollten syntaktisch korrekt sein;

  vergleiche 

  .

- **Beachte:** Webseiten werden für eine Vielzahl von Lesern entwickelt nicht für bestimmte Browser! Man benutze deshalb nur solche HTML-EIgenschften, die „überall“ funktionieren.

- Der Fußbereich unter der horizontalen Linie der Fachbereichs-Homepage (`http://www.math.uni-wuppertal.de`) enthält einige Links, die früher einmal im Bereich Neuigkeiten angeboten wurden.

- Sprachvarianten (deutsch/englisch/...) können durch „Flaggen“ umschaltbar angeboten werden oder mit Hilfe des in `http 1.1` vorhandenen Inhaltsvarianten-„Verhandlungssystems“ (http://httpd.apache.org/docs/content-negotiation.html und http://www.apacheweek.com/features/negotiation) gesteuert werden.

Typische Inhalte eines Webauftritts:

Auf den Seiten des Fachbereichs Mathematik (`http://www.math.uni-wuppertal.de`) der Bergischen Universität Wuppertal (`http://www.uni-wuppertal.de`) werden folgende Informationen dargstellt:

- Selbstdarstellung
  - Organisation (Dekanat, Prüfungsämter, Fachbereichsrat, Fachschaft, ...)
  - Organisatorische Unterbereiche (Labore, Institute,...)
  - „Verwandte“ Organisationen/Organisationseinheiten
  - Tipps für Studieninteressierte
  - Tipps für Besucher/Gäste
- Personalverzeichnis
  - Listen mit Telefonnummern, email-Adressen, Web-Homepages, ...
  - email-Aliases für Verteilerlisten
  - Listen mit Rollen-Aliases (dekan, dekanat)
  - Liste der e-mail Adressen der Studenten
- Termine
- Mitteilungen/schwarzes Brett
- Dienstleistungen
  - DV-Dienstleistungen per Web für Mitglieder des FBs,... (Anforderungen von Formularen, Änderung der Daten im Personalverzeichnis, ...)
- Forschung
  - Forschungsgruppen
  - Preprints
  - Promotionen
  - Software
- Lehre
  - Studiengänge
  - Prüfungsordnungen/Studienordnungen
  - Vorlesungsverzeichnisse

  - Projekte/Praktika

- Links
  - Rechenzentrum
  - Bibliothek
  - Fachinformationszentren
  - ...

Aufgabe: Erstellen Sie ein Analogon für eine Firmenpräsentation.

Weitere Dienste im Internet:

- **e-mail mit Sondermerkmalen:**
  - normal
  - mit Vesandtvermerk (Priorität,...)
  - mit Unterschrift („Selbstbeglaubigung“)
  - verschlüsselt für ...
  - verschlüsselt für ... und mit Unterschrift
  - mit Rückschein (Empfangsbestätigung)
    - ▷ Bestätigung des Empfangs im Ziel-Emailserver
    - ▷ Bestätigung des Betrachtens im Ziel-Email-Client
  - Absenderangaben
    - ▷ `~/.signature` Text
    - ▷ `text/x-vcard` Visitenkarten
- **e-mail Adressbücher**
  - Netscape Adressbuch oder `wab` (Windows address book):
    - ▷ lokale Adressbücher
    - ▷ LDAP-Directories, z.B.

      FB7-Studenten
      `wmit00.it.math.uni-wuppertal.de`
      `ou=students,ou=math,o=uni-wuppertal,c=de`
    - ▷ Web-Gateways für LDAP-Server, z.B.

      `http://wmit00.it.math.uni-wuppertal.de:1760/ou=math,o=uni-wuppertal,c=de`

      bzw.

      `http://sites.inka.de:8002/web2ldap/` mit

      `wminf0.math.uni-wuppertal.de`
      `ou=math,o=uni-wuppertal,c=de`
- **e-mail Aliases**
  - lokal als Spitznamen (nur für User)
  - lokal als Verteilerlisten (nur für User)
  - nichtlokal für Rollennamen, Spitznamen, Verteilerlisten in `/etc/aliases` (für alle User eines Rechners bzw. nichtlokal)
  - nichtlokal auf Mailservern

- **Usenet News-Gruppen**
  - Diskussionsforen wie z.B.
    news:de.answers
    news:de.newusers.questions
    news:de.newusers.infos
    news:news.answers
    news:news.newusers.questions
    news:news.announce.newsgroups
- **Nachschlagewerke und Suchmaschinen**
  - http://www.google.com
    für die Suche nach Bildern, Dokumenten, Newsnachrichten, ...
  - http://sdb.suse.de
    als Servicedatenbank für das Suse-Linux-Betriebssystem
  - http://www.teleauskunft.de
    für Telefon- und Faxnummern
  - http://www.telekom.de
    für online verfügbare Handbücher zur T-Netbox, von Telefonanlagen, ...
  - http://www.Matheprisma.de/Module/
    für Online-Lerneinheiten zur Mathematik.
  - und viele andere mehr
- **Applikationsserver**
  - X-Window unter Unix auf einem entferneten –remote– Rechner mitbenutzen

    ```
    ssh -X rechner.de -l username
    ```

    für remote Login bzw.

    ```
    X :1 -query rechner.de -once&
    ```

    für die Benutzung des Display-Servers von rechner.de (der eigene Rechner ist nur X-Terminal)
  - Windows-Server mit Terminalserver-Software von Microsoft/Citrix

    ```
    wfcmgr&
    ```
- **Firmennetze mit dem Internet als Transportmedium**
  - VPN (virtual private net)
  - MobileIP

1. Internetnutzung

1.1. Informationsgewinnung und -austausch

1.1.1. Adressbücher

Nichtlokale Adressbücher können in Form von LDAP-Directory-Servern (Verzeichnisservern) für die automatische Adressergänzung sowohl im Netscape-Messenger als auch in Outlook/Outlook Express genutzt werden:
Dazu wird das Netscape-Adressbuch aufgerufen und z.B. der LDAP[1]-Server des Fachbereichs Mathematik der Bergischen Universität den Verzeichnisdiensten hinzugefügt:

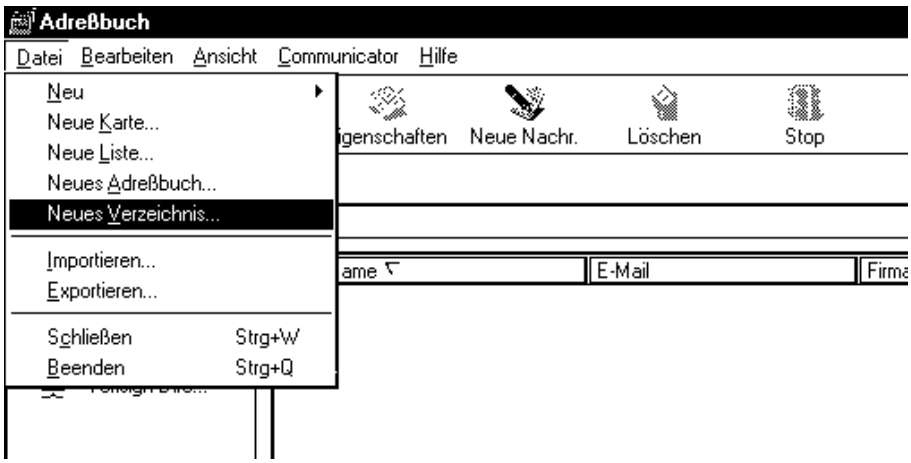


Abbildung 1.1.: LDAP-Dienste-Auruf im Netscape-Adreßbuch

Ähnlich kann und Windows `wab` (Windows adress book) aufgerufen werden und z.B. der hochschulinternen LDAP-Server des Personals der Bergischen Universität Wuppertal gemäß den Abbildungen (1.3) bis (1.6) zur Benutzung bereitgestellt werden.

[1] LDAP=light weight directory access protocol.
Ein Verzeichnisdienst ist eine Informationsdatenbank, die auf häufige Anfragen optimiert ist, jedoch nicht auf häufige Änderungen/Modifikationen,

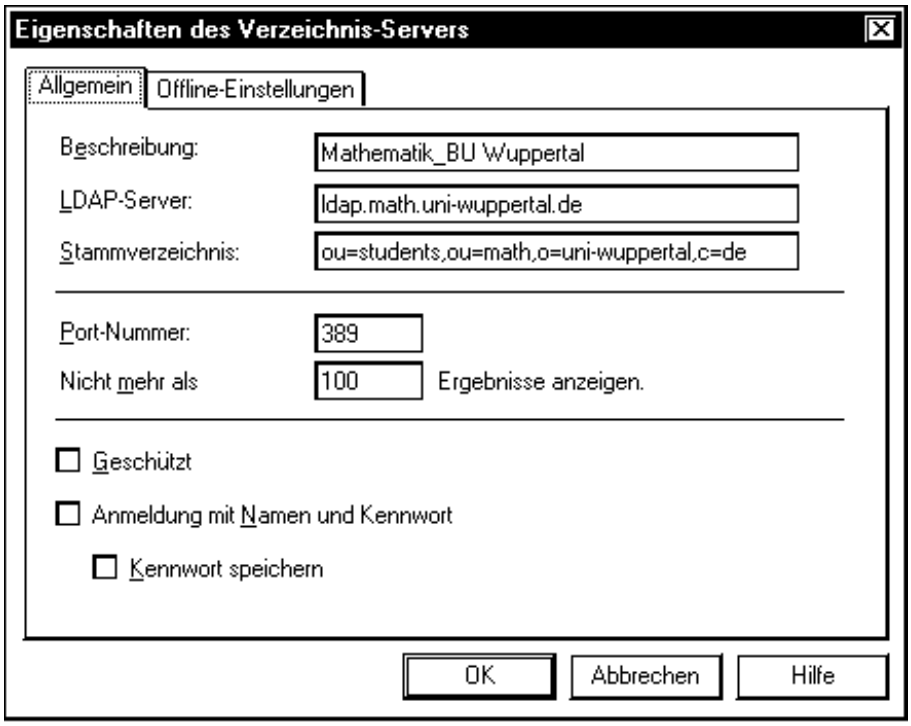


Abbildung 1.2.: LDAP-Server Einrichtung in Netscape

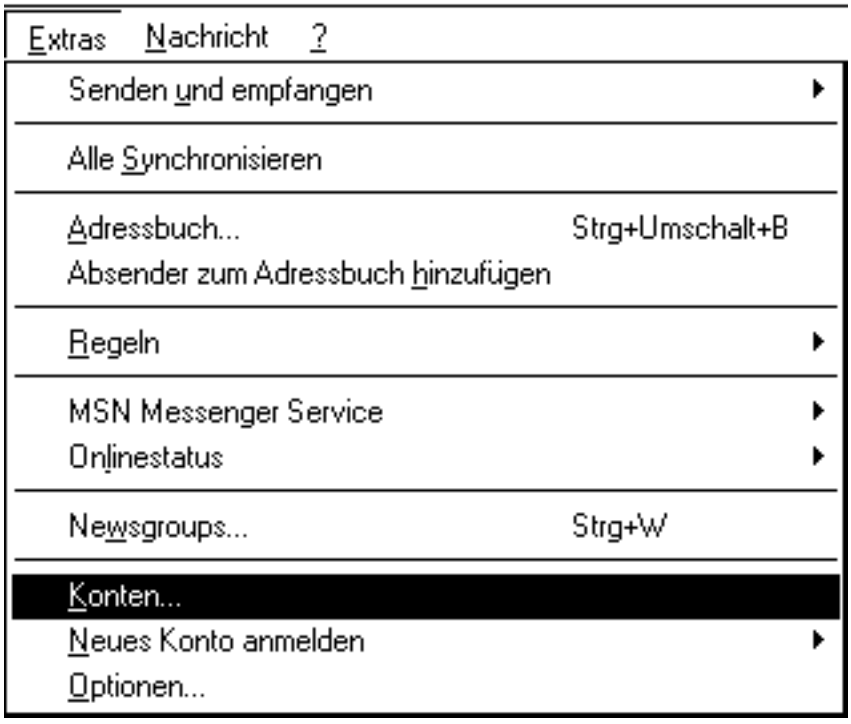


Abbildung 1.3.: LDAP-Dienste-Auruf in Outlook-Express I

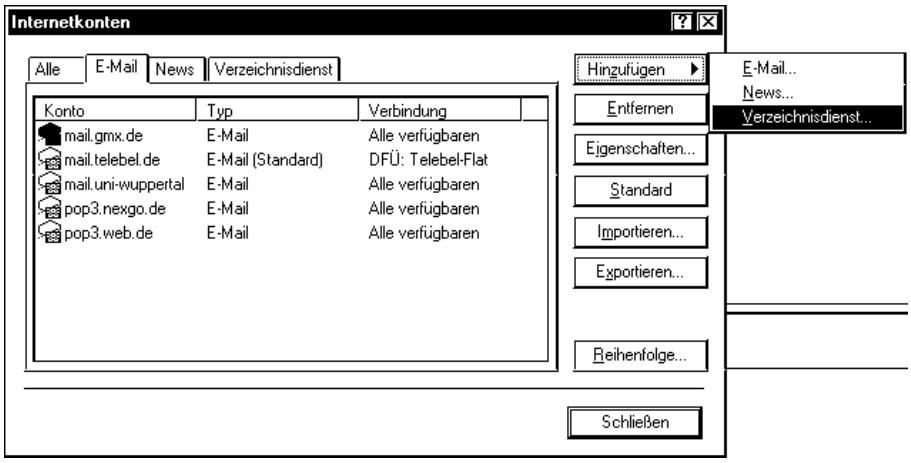


Abbildung 1.4.: LDAP-Dienste-Auruf in Outlook-Express II

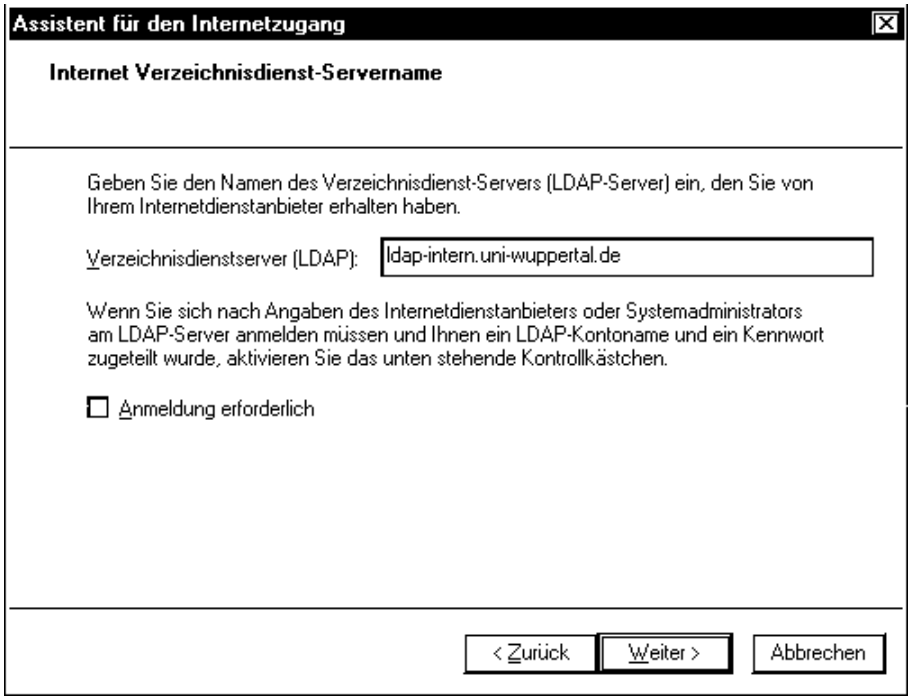


Abbildung 1.5.: LDAP-Dienste-Einrichtung in Outlook-Express I

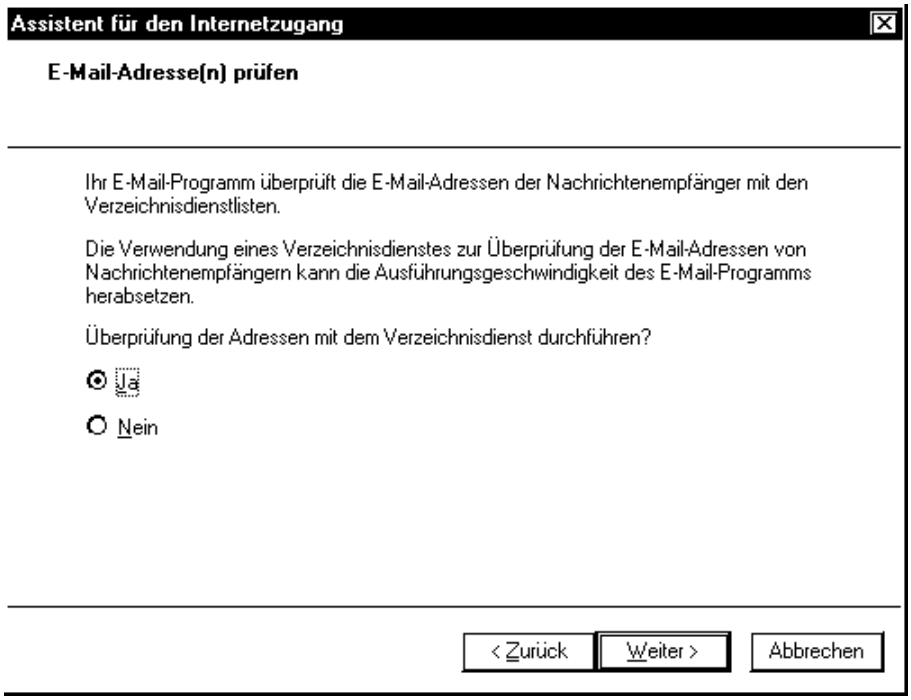


Abbildung 1.6.: LDAP-Dienste-Einrichtung in Outlook-Express II

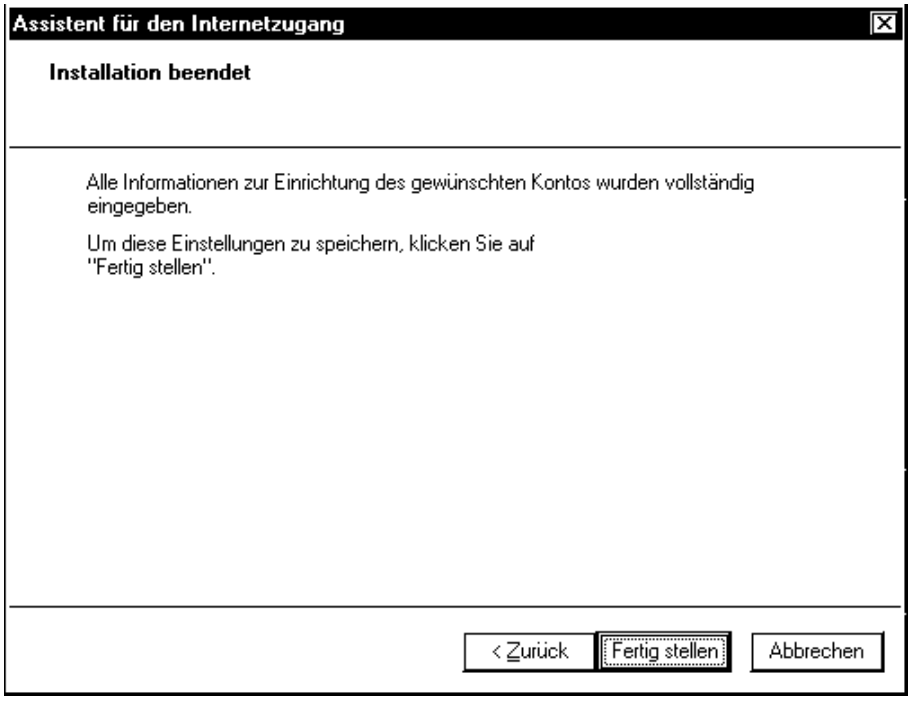


Abbildung 1.7.: LDAP-Dienste-Einrichtung in Outlook-Express III

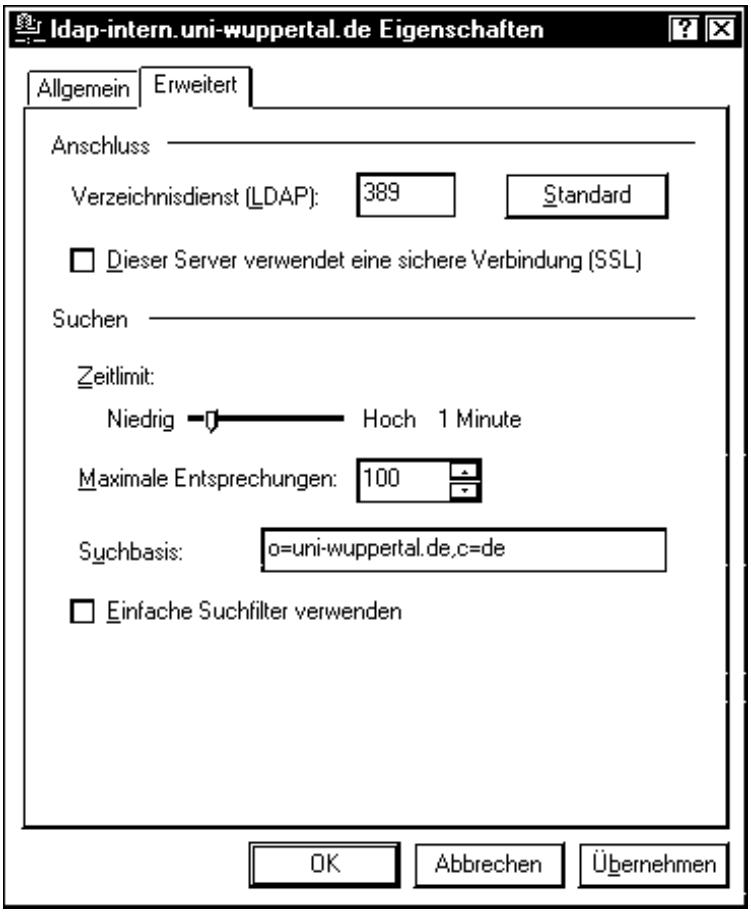


Abbildung 1.8.: LDAP-Dienste-Einrichtung in Outlook-Express IV

Durch die Suchbasis (search root) kann man „Unterabteilungen“ von Organisationen barumartig getrennt ansprechen:

Organisationsunit	ou=math
Organisation	o=uni-wuppertal
Land (country)	c=de

bzw.

ou=groups
ou=math
o=uni-wuppertal
c=de

usw.

Es gibt auch zwei verbreitete Softwareprodukte, die den Zugang zu LDAP-Servern mittels Web-Browser ermöglichen:
Eines ist web500gw:

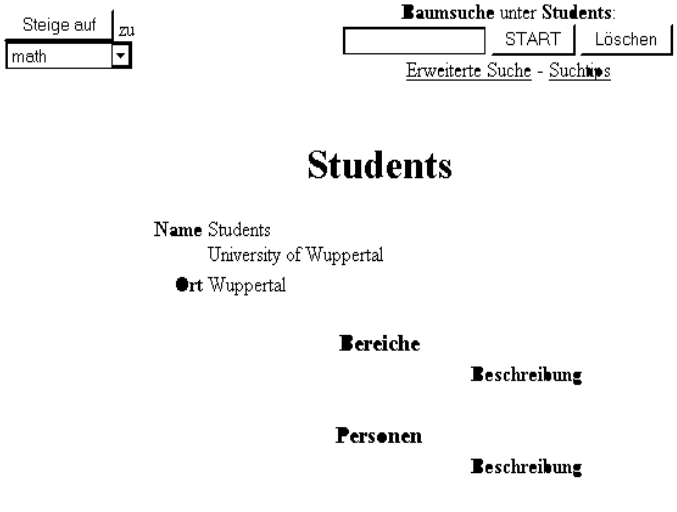


Abbildung 1.9.: web500gw
`http://wmit00.it.math.uni-wuppertal.de:1760/ou=students,ou=math, o=uni-wuppertal,c=de`

Aufgabe: Suchen Sie nach allen Studenten mit Vornamen Bernd und lassen Sie sich deren Business card (vcard) anzeigen.

Durch Anklicken des Wortes `People` bekommen Sie eine Liste aller im Adressbuch vorhandenen Einträge angezeigt.

Das andere heißt `web2ldap`. Mit diesem können Sie beispielsweise unter

`http://sites.inka.de:8002/web2ldap/`

nach dem S/MIME-Zertifikat von Herrn Feuerstein suchen. Über den Punkt `Read` kann

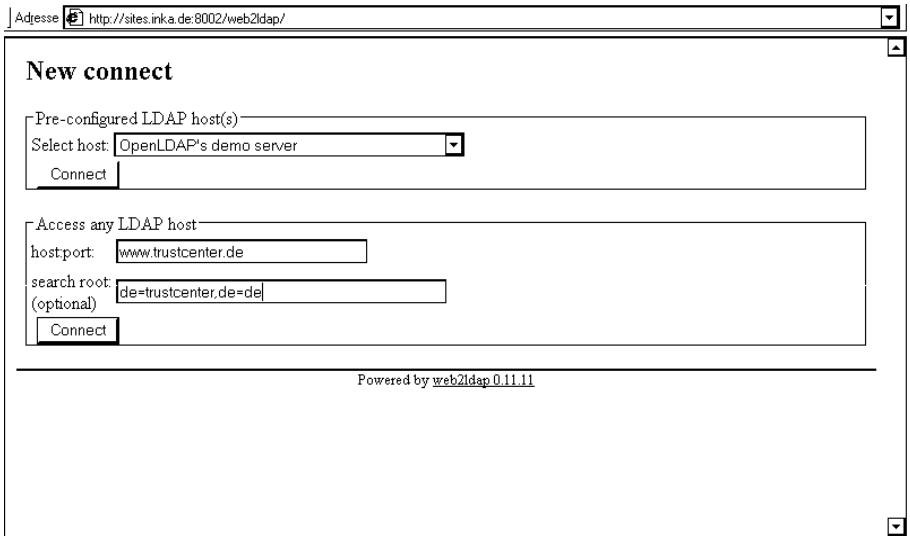


Abbildung 1.10.: web2ldap I
`http://sites.inka.de:8002/web2ldap/`

dann dort `userCertificate; binary` mittels `View` gewählt werden und damit das S/-MIME X.509v3-Zertifikat von Herrn Feuerstein erhalten werden.

Bemerkung: Die Erweiterung der Webadresse um `:1760` bzw. `:8002` sind sogenannte Port-Nummern. Über diese Nummern kann ein entsprechender Internetdienst des aufgerufenen Rechners ausgewählt werden. `http` enstpricht dabei standardmäßig dem Port 80, `https` dem Port 443[2].

[2]Vergleiche hierzu `/etc/services` auf Unix-Rechnern.

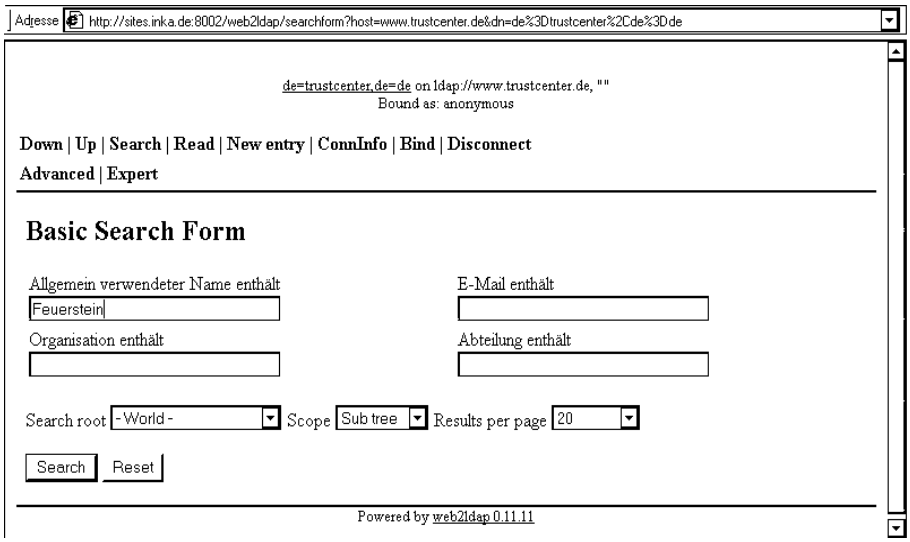


Abbildung 1.11.: web2ldap II
`http://sites.inka.de:8002/web2ldap/`

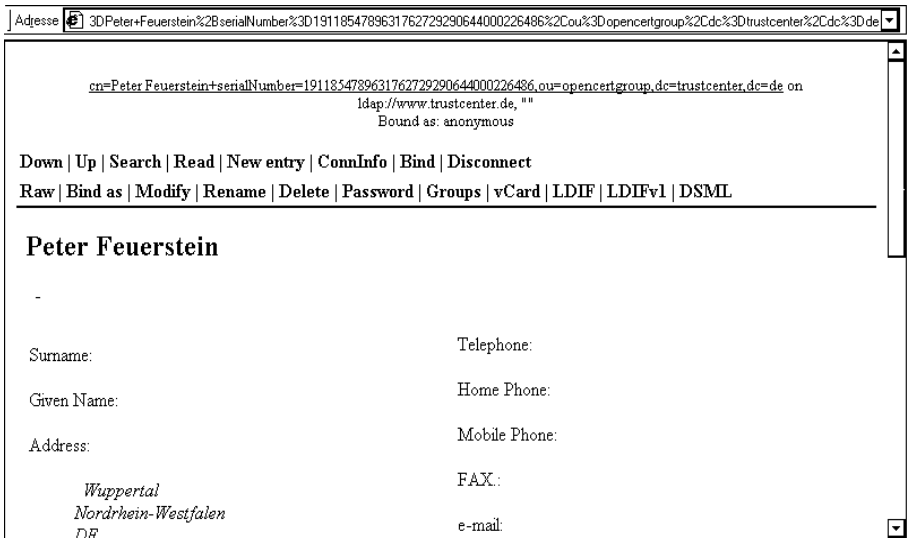


Abbildung 1.12.: web2ldap III
`http://sites.inka.de_8002/web2ldap/`

Abbildung 1.13.: web2ldap IV
`http://sites.inka.de_8002/web2ldap/`

`gq` als Bestandteil der `gnome`-Oberfläche des Linux-Betriebssystems[3] ermöglicht nicht nur eine Abfrage von LDAP-Servern sondern auch deren Verwaltung:

Abbildung 1.14.: web500gw
`http://wmit00.it.math.uni-wuppertal.de:1760/ou=students,ou=math,o=uni-wuppertal,c=de`

[3]Es ist auch unter `kde` lauffähig

1.1.2. email

Neben den in der Einleitung schon besprochenen Möglichkeiten, email mittels Netscape-Messanger bzw. Outlook/Outlook Express zu nutzen,

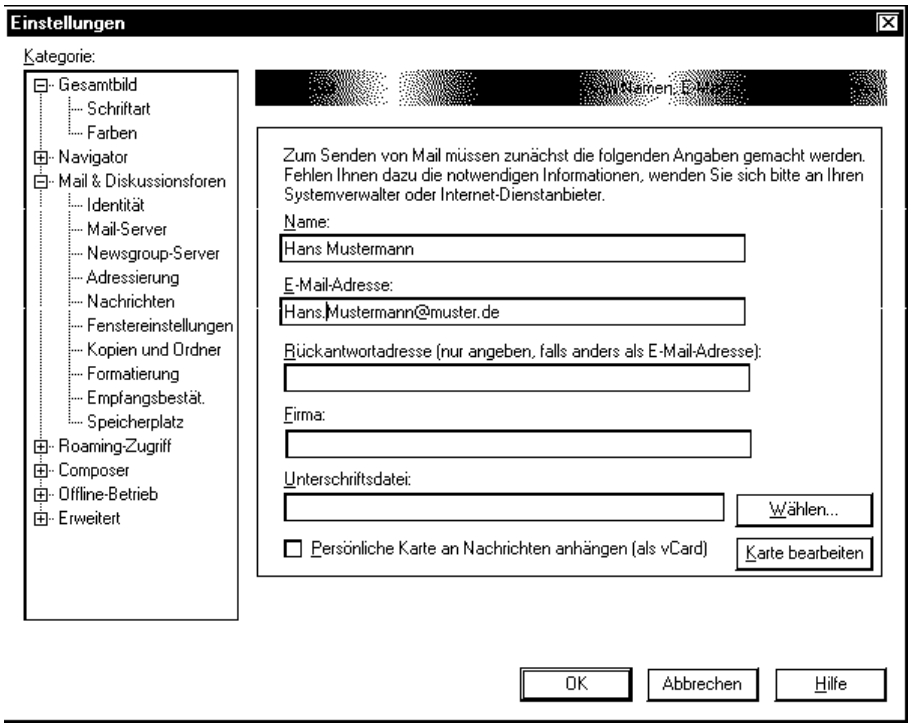


Abbildung 1.15.: email-Konfiguration im Netscape Messenger I

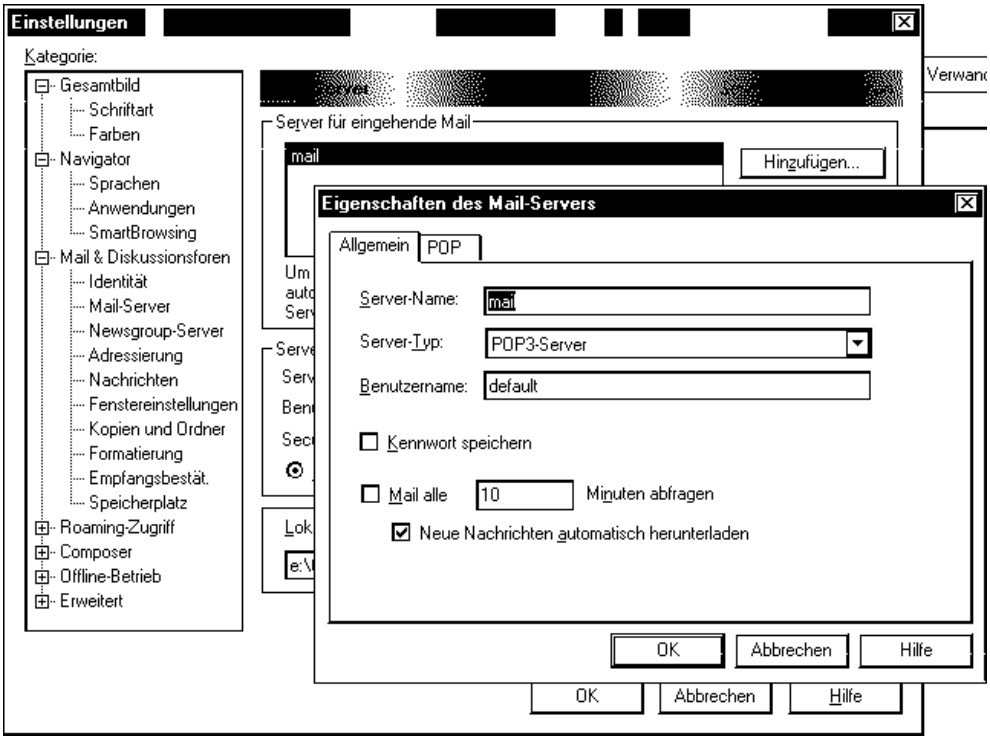


Abbildung 1.16.: email-Konfiguration im Netscape Messenger II

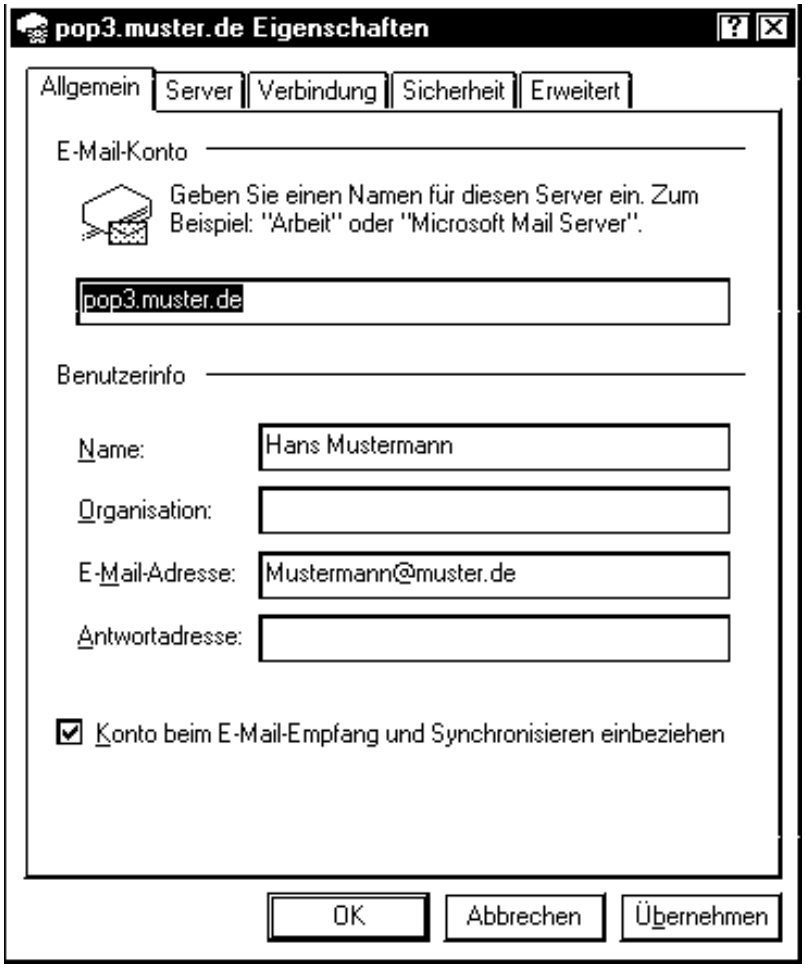


Abbildung 1.17.: email in Outlook Express

existieren auch IMAP[4]-Server mit Web-Oberfläche.

Abbildung 1.18.: email mit IMAP-Server I

Abbildung 1.19.: email mit IMAP-Server II

[4]Internet Mail Access Protocol

1.1.3. Absenderangaben, Formulare und Visitenkarten

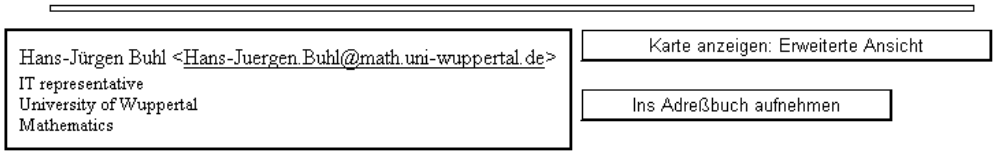
Subject: Anforderung von...
Content-type: MULTIPART/MIXED; BOUNDARY=...
X-Accepted-Language: en, de
X-Virus-Scanned: by amavisd-milter (http:/amavis.org)
References: ...
X-Priority: 1 (Highest)

Lieber Herr Mustermann,

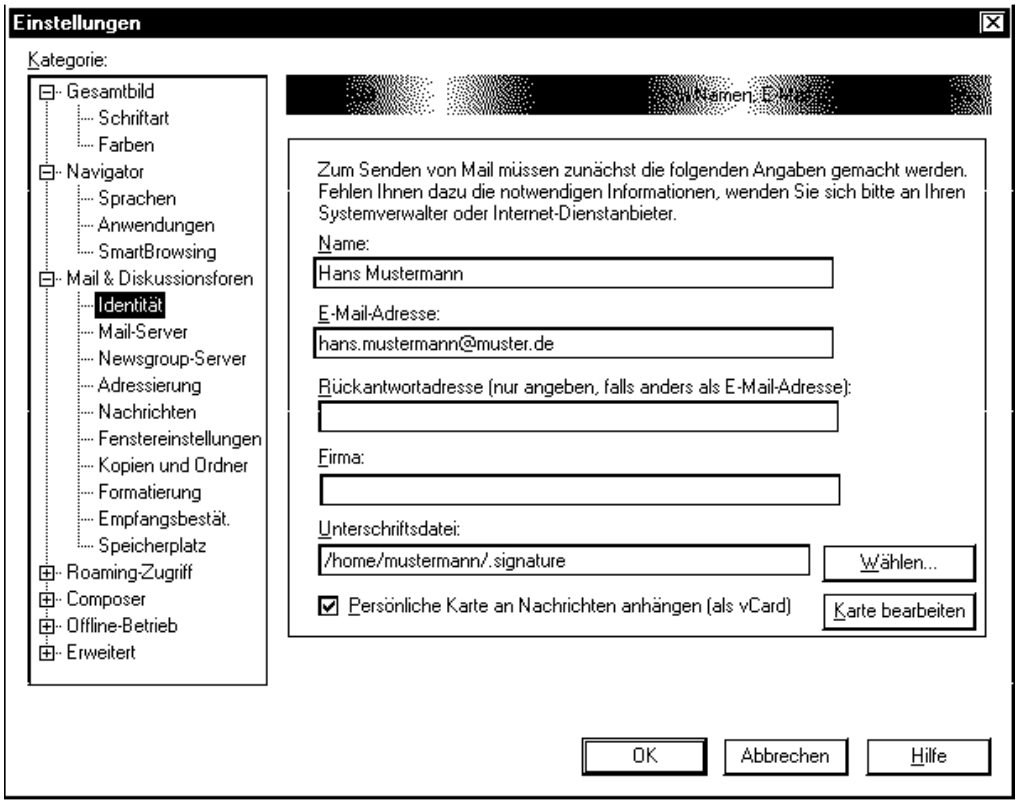
...

Gruß
Hans-Jürgen Buhl

```
--
-----------------------------------------------------------------------
Prof. Dr. Hans-Juergen Buhl University of Wuppertal
Fachbereich Mathematik & Institut fuer Angewandte Informatik
-----------------------------------------------------------------------
Phone: +49 202 2422009 Fax: +49 202 2422011
mailto: Hans-Juergen.Buhlmath.uni-wuppertal.de
WWW: http://www.math.uni-wuppertal.de/~buhl
smail: University, Gauss-Strasse 20, D-42119 Wuppertal, Germany
-----------------------------------------------------------------------
```

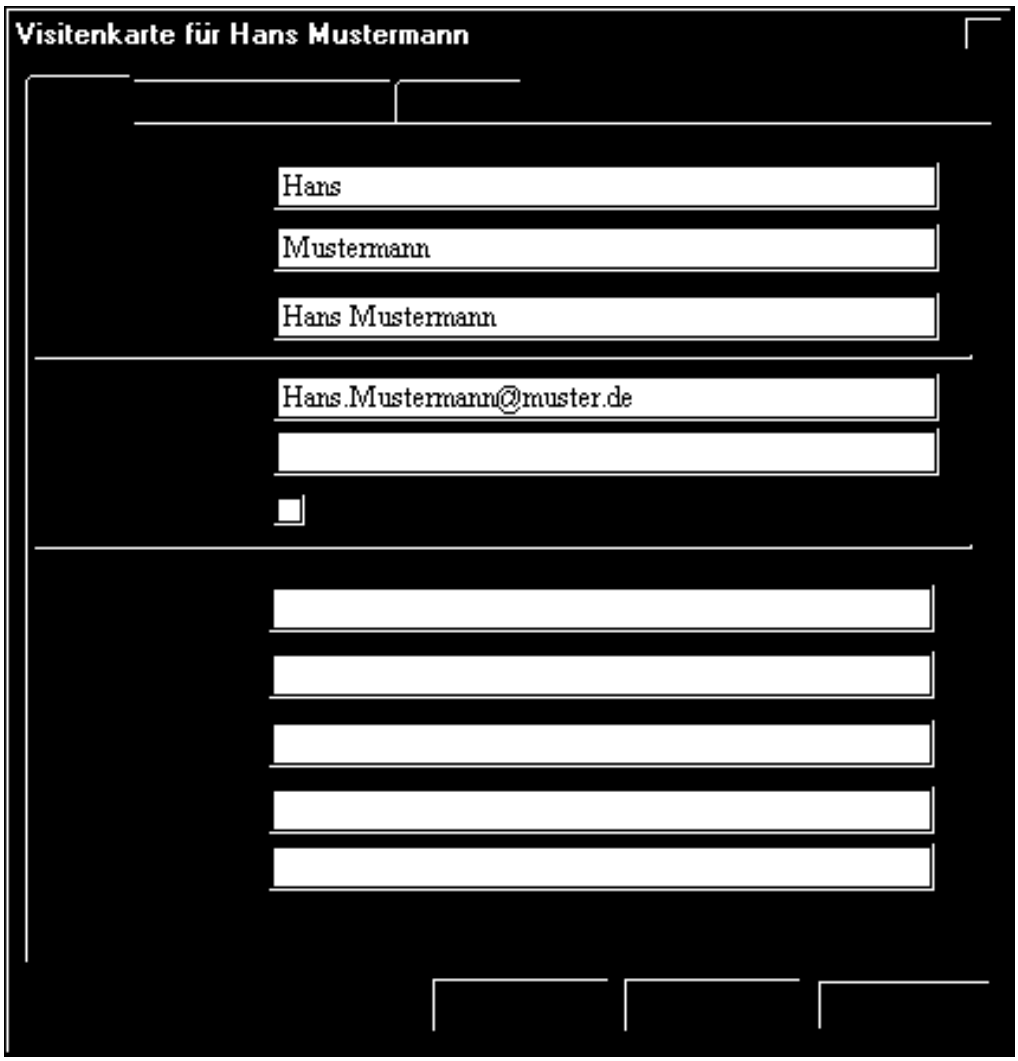


Obige email enthält zwei Arten von Absenderangaben. Die Erste, die sogenannte `signature`, wird üblicherweise als reine Textdatei von wünschenswerterweise weniger als fünf Zeilen in der Datei `$HOME/.signature` abegelegt und dann automatisch von den Kommandos `mail, mailx, ...` an jede ausgehende email angehängt. Auch Netscape kann man so konfiguerieren, dass

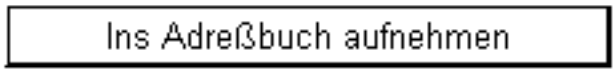


der Inhalt einer Datei (am besten ebenfalls `$HOME/.signature`) in jedem neu geöffneten Composer-Fenster im Sinne eines Default-Formulares automatisch eingefügt erscheint. Solche Absenderangaben kann jeder auch nur rein textbasiert arbeitende email-Client vernünftig anzeigen.

Eine Visitenkarte – die zweite besprochene Art von Absenderangaben – kann durch Anwählen des Punktes `Attach my personal card do messages` ebenfalls automatisch an abgehende emails angehängt werden. Solche Karten können durch KLicken auf `Edit Card` erstellt werden.



Der Empfänger einer solchen email kann dann eine solche Visitenkarten durch einfaches Klicken auf den Knopf



in sein persönliches Adressbuch übernehmen.
Vorsicht: Bitte reines ASCII ohne Umlaute benutzen, da ansonsten die Sortierungsreihenfolge des persönlichen Adressbuches durcheinanderkommen kann.
Visitenkaretn können sowohl in Netsacpe als auch in Outlook/Outlook Express genutzt werden und funktionieren auch, wenn Absender und Empfänger verschiedene email-Klienten benutzen[5]. Das liegt daran, dass für Visitenkarten der MIME[6]-Typ `text/x-vcard` benutzt wird und die Mailnachricht (body) sowie die Visitenkarte als

[5]Einige Visitenkartenfelder gehen dabei aber jeweils verlore.
[6]Multiple purpose internet mail extensions

zwei Teile einer mehrteiligen `MULTIPART/MIXED` email versendet werden. Rein textbasierte Mailreade zeigen dann auch etwa folgenden Inhalt an:

```
Sender: buhl@mail.urz.uni-wuppertal.de
Message-ID: <3E56228D.13DCD010@math.uni-wuppertal.de>
Date: Fri, 21 Feb 2003 13:58:53 +0100
From: Hans-Juergen Buhl <Hans-Juergen.Buhl@math.uni-wuppertal.de>
Organization: University of Wuppertal
X-Mailer: Mozilla 4.76 [en] (X11; U; SunOS 5.3 sun4m)
X-Accept-Language: en
MIME-Version: 1.0
To: ...
Subject: ...
References: <3E3522EB.D7B0E8D9@math.uni-wuppertal.de> <001401
    c2d9a3$9d70b0a0$492b14d5@muster>
Content-Type: multipart/mixed;
 boundary="------------B9A8CF31DD617289BA8FD894"
X-Virus-Scanned: by amavisd-milter (http://amavis.org/)

This is a multi-part message in MIME format.
--------------B9A8CF31DD617289BA8FD894
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit

...

Gruß
Hans-Jürgen Buhl

--
-----------------------------------------------------------------------
 Prof. Dr. Hans-Juergen Buhl                 University of Wuppertal
 Fachbereich Mathematik & Institut fuer Angewandte Informatik
-----------------------------------------------------------------------
 Phone:  +49 202 2422009                        Fax:   +49 202 2422011
 mailto: Hans-Juergen.Buhl@math.uni-wuppertal.de
 WWW:    http://www.math.uni-wuppertal.de/~buhl
 smail:  University, Gauss-Strasse 20, D-42119 Wuppertal, Germany
-----------------------------------------------------------------------
--------------B9A8CF31DD617289BA8FD894
Content-Type: text/x-vcard; charset=us-ascii;
 name="Hans-Juergen.Buhl.vcf"
Content-Transfer-Encoding: 7bit
Content-Description: Card for Hans-Juergen Buhl
Content-Disposition: attachment;
 filename="Hans-Juergen.Buhl.vcf"

begin:vcard
n:Buhl;Hans-Juergen
tel;fax:+49 202 2422011
tel;home:+49 202 2422003
tel;work:+49 202 2422009
x-mozilla-html:FALSE
url:http://www.math.uni-wuppertal.de/~buhl
org:University of Wuppertal;Mathematics/Computer Science
adr:;;Gauss-Strasse 20;Wuppertal;;D-42119;Germany
version:2.1
email;internet:Hans-Juergen.Buhl@math.uni-wuppertal.de
title:IT representative
note:Member of the Institute for Applied Computer Science (IAI)
x-mozilla-cpt:;26880
fn:Prof. Dr. Hans-Juergen Buhl
end:vcard

--------------B9A8CF31DD617289BA8FD894--
```

Deshalb bleibt eine Absenderangabe im Sinne der Textdatevariante `$HOME/.signature` als zweite redundante Absenderangabe solange sinnvoll, wie einige der email-Korrespondenten noch solche textbasierte email- Reader benutzen.

Bemerkung: Leider scheinen Outlook und Outlook Express auch `MULTIPART/MIXED` emails zu erzeugen, deren ersten beiden Teile ((Versand von gleichzeitig Text- und HTML-Version einer Nachricht) von Netscape als ein gemeinsamer Text-Teil interpretiert wird:

```
Message-ID: <006301c2de5b$42f2e500$08bcb9d9@pater>
From: "Hans Müller" <mueller@mueller.de>
To: "Hans Mustermann" <hans.mustermann@muster.de>
Subject: Muster
Date: Thu, 27 Feb 2003 13:25:04 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0060_01C2DE63.A3A19740"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4807.1700
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4807.1700

This is a multi-part message in MIME format.

------=_NextPart_000_0060_01C2DE63.A3A19740
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: quoted-printable

Hallo lieber Herr Mustermann,

hier ist die angeforderte Muster-Email

Viele Gr=FC=DFe


------=_NextPart_000_0060_01C2DE63.A3A19740
Content-Type: text/html;
        charset="Windows-1252"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Dwindows-1252">
<META content=3D"MSHTML 5.50.4807.2300" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY>
<DIV><FONT face=3DArial size=3D2></FONT><FONT face=3DArial =
size=3D2>Hallo lieber Herr=20
Mustermann,</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT> </DIV>
<DIV><FONT face=3DArial size=3D2>hier ist die angeforderte =
Muster-Email</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT> </DIV>
<DIV><FONT face=3DArial size=3D2>Viele Gr=FC=DFe</FONT></DIV>
<DIV> </DIV></BODY></HTML>

------=_NextPart_000_0060_01C2DE63.A3A19740--
```

1.2. Bereitstellung von Internetinhalten

1.2.1. Eigene Webseiten/HTML

1.2.2. Dynamic HTML und Javascript

1.2.3. Ausblick: Java

2. Zu sichereren Netzwerkdiensten

2.1. S/MIME

2.1.1. Unterschriften und Zertifikate

2.1.2. Codierte Mail

2.1.3. Empfangsbestätigungen

2.1.4. Quellen für öffentliche Schlüssel

2.2. PGP und Dateicodierung

PGP (Pretty Good Privacy) ist ein Verschlüsselungsprogramm für email und Dateien. Mit PGP können emails elektronisch unterschrieben (unterzeichnet/signiert) werden. PGP ist weit verbreitet und gilt mittlerweile als ein Standard der Kryptografie, da es für Privatpersonen und gemeinnützige Organisationen kostenlos ist.

2.2.1. Lokales Verschlüsseln und Entschlüsseln von Dateien

Statt des unsicheren `crypt`-Kommandos des UNIX-Betriebssystems sollte `pgp` zur Verschlüsselung/Entschlüsselung von Dateien mit sensitivem Inhalt benutzt werden.
PGP bietet zunächst sogenannte symmetrische Verschlüsselungen an, d.h. beim Verschlüsseln einer Datei wird derselben Schluessel (**Mantra**) wie bei der späteren Entschlüsselung verwendet. Es bietet sich an, als Mantra eine PassPhrase (d.h. ein nicht nur ein Wort sondern einen geeigneten Satz) zu verwenden!

Ein Beispiel:

```
% pgp -c Sieb.p
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:51 GMT

Du brauchst ein Mantra zum Verschlüsseln der Datei.
Gib das Mantra ein: <----- Eine Passphrase zur Verschluesselung nur dieser Datei
Wiederhole das Mantra: <----- Wiederholung
Einen Augenblick, bitte....
Verschlüsselte Datei: Sieb.p.pgp

% ls -al Sieb.p*
-rw-r--r-- 1 buhl inf 1680 Oct 28 1999 Sieb.p
-rw------- 1 buhl inf 655 Jun 14 18:50 Sieb.p.pgp
```

Das Entschlüsseln erfolg mittels:

```
% pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:55 GMT

Diese Datei ist konventionell verschlüsselt.

Du brauchst ein Mantra zum Entschlüsseln dieser Datei.
Gib das Mantra ein:
Einen Augenblick, bitte....
Das Mantra scheint zu stimmen.
.
Dateiname des Klartextes: Sieb.p
Die Ausgabedatei 'Sieb.p' existiert bereits. Überschreiben? (j/N) j
```

Bemerkung: „`pgp -cw Sieb.p`“ löscht nach Erzeugung von `Sieb.p.pgp` das Original `Sieb.p`.

Bemerkung: `pgp.p.pgp` ist eine Binaerdatei. Wollen Sie eine per e-mail versendbare ASCII-Datei erzeugen geht das mittels “`pgp -cwa Sieb.p`“. Die codierte Datei hat dann den Namen `Sieb.p.asc`.

2.2.2. uuencode, uudecode

Eine Möglichkeit, binäre Dateien (d.h. genauer nicht rein ASCII 7 Bit-Dateien) via email zu versenden ist, stellen `uuencode` (Unix to Unix Encode) oder das verwandte `base64` dar. Die meisten E-Mail-Clients erledigen diese Aufgabe inzwischen automatisch, sobald sie auf eine Binärdatei treffen:

> Das Internet war zunächst nicht zur Übertragung von binären Daten (Programme und andere Dateien, bei denen es sich nicht um reine Textdateien handelt) gedacht. Es ist lediglich in der Lage, Dateien zu übertragen, die aus „normalen“ Zeichen besteht (druckbare ASCII-Zeichen).
> Um diese Beschränkungen zu überwinden, wurden unter anderem das Verfahren `uuencode` entwickelt. Alle diese Ansätze, arbeiten nach dem gleichen Prinzip: Sie wandelt binäre Dateien (die ja wie bereits erwähnt nicht über das Internet verschickt werden können) in Dateien um, die nur ASCII Zeichen enthalten und somit über das Internet verschickt werden können. Dieser Vorgang ist das Kodieren (encoding). Der Empfänger der so umgewandelten Datei, kann dann den Vorgang wieder umkehren: Die reinen ASCII-Zeichen werden dann wieder in eine binäre Datei umgewandelt (also die ursprüngliche Datei).
>
> Quelle: WinZip (`http://www.winzip.de/uu00002.htm`)

Die `man`-Pages geben Aufschluss über die Verwendung der beiden Befehle (http://campuscgi.princeton.edu/man?uuencode):

NAME

uuencode, uudecode - encode a binary file, or decode its encoded representation

SYNOPSIS

```
uuencode [ source-file ] decode_pathname
uudecode [ -p ] [ encoded-file ]
```

DESCRIPTION

uuencode

uuencode converts a binary file into an encoded representation that can be sent using mail(1). It encodes the contents of source-file, or the standard input if no sourcefile argument is given. The decode_pathname argument is required. The decode_pathname is included in the encoded file's header as the name of the file into which uudecode is to place the binary (decoded) data. uuencode also includes the permission modes of source-file, (except setuid, setgid, and sticky-bits), so that decode_pathname is recreated with those same permission modes.

uudecode

uudecode reads an encoded-file, strips off any leading and trailing lines added by mailer programs, and recreates the original binary data with the filename and the mode specified in the header.

The encoded file is an ordinary portable character set text file; it can be edited by any text editor. It is best only to change the mode or decode_pathname in the header to avoid corrupting the decoded binary.

OPTIONS

uudecode

-p decode encoded-file and send it to standard output. This allows uudecode to be used in a pipeline.

OPERANDS

uuencode

The following operands are supported by uuencode:

decode_pathname

The pathname of the file into which the uudecode utility will place the decoded file. If there are characters in decode_pathname that are not in the portable filename character set the results are unspecified.

source-file

A pathname of the file to be encoded.

uudecode

The following operand is supported by uudecode:

encoded-file

The pathname of a file containing the output of uuencode.

USAGE

See largefile(5) for the description of the behavior of uuencode and uudecode when encountering files greater than or equal to 2 Gbyte (2**31 bytes).

ENVIRONMENT

See environ(5) for descriptions of the following environment variables that affect the execution of uuencode and uudecode: LC_CTYPE, LC_MESSAGES, and NLSPATH.

OUTPUT

stdout

The standard output is a text file (encoded in the character set of the current locale) that begins with the line:

`"begin/\%s/\%s\n"`, <mode>, decode_pathname and ends with the line:

`end\n`

In both cases, the lines have no preceding or trailing blank characters.

The algorithm that is used for lines in between begin and end takes three octets as input and writes four characters of output by splitting the input at six-bit intervals into four octets, containing data in the lower six bits only. These octets are converted to characters by adding a value of 0x20 to each octet, so that each octet is in the range 0x20-0x5f, and then it is assumed to represent a printable character. It then will be translated into the corresponding character codes for the codeset in use in the current locale. (For example, the octet 0x41, representing A , would be translated to A in the current codeset, such as 0xc1 if it were EBCDIC.) Where the bits of two octets are combined, the least significant bits of the first octet are shifted left and combined with the most significant bits of the second octet shifted right. Thus the three octets A, B, C are converted into the four octets:

```
0x20 + (( A >> 2 ) & 0x3F)

0x20 + (((A << 4) | ((B >> 4) & 0xF)) & 0x3F)

0x20 + (((B << 2) | ((C >> 6) & 0x3)) & 0x3F)

0x20 + (( C ) & 0x3F)
```

These octets are then translated into the local character set.

Each encoded line contains a length character, equal to the number of characters to be decoded plus 0x20 translated to the local character set as described above, followed by the encoded characters. The maximum number of octets to be encoded on each line is 45.

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

ATTRIBUTES

See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWesu

SEE ALSO

mail(1), mailx(1), uucp(1C), uux(1C), attributes(5), largefile(5)

NOTES

The encoded file's size is expanded by 35% (3 bytes become 4, plus control information), causing it to take longer to transmit than the equivalent binary.

The user on the remote system who is invoking uudecode (typically uucp) must have write permission on the file specified in the decode_pathname.

If you uuencode then uudecode a file in the same directory, you will overwrite the original file.

2.2.3. base64

Eine modernere Möglichkeit für die Übertragung von Binärdateien im Internet stellt die base64-Methode gemäß RFC 1521 dar. Die große Verbreitung dieser Methode basiert darauf. dass die Base64-Kodierung mit einem sehr eingeschränkten Alphabets von nur 64 Zeichen auskommt. Damit genügen für die Darstellung eines codierten Zeichen 6 Bit. Die Man-Page ist unter http://www.fourmilab.ch/webtools/base64/ einsehbar:

NAME

base64 - encode and decode base64 files

SYNOPSIS

`base64 [ -d / -e ] [ options ] [ infile ] [ outfile ]`

DESCRIPTION

The MIME (Multipurpose Internet Mail Extensions) specification (RFC 1341 and successors) defines a mechanism for encoding arbitrary binary information for transmission by electronic mail. Triplets of 8-bit octets are encoded as groups of four characters, each representing 6 bits of the source 24 bits. Only characters present in all variants of ASCII and EBCDIC are used, avoiding incompatibilities in other forms of encoding such as uuencode/uudecode. base64 is a command line utility which encodes and decodes files in this format. It can be used within a pipeline as an encoding or decoding filter, and is most commonly used in this manner as part of an automated mail processing system.

OPTIONS

–copyright Print copyright information. -d, –decode Decodes the input, previously created by base64, to recover the original input file. -e, –encode Encodes the input into an output text file containing its base64 encoding. -n, –noerrcheck Suppress error checking when decoding. By default, upon encountering a non white space character which does not belong to the base64 set, or discovering the input file is incorrectly padded to a multiple of four characters, base64 issues an error message and terminates processing with exit status 1. The -n option suppresses even this rudimentary error checking; invalid characters are silently ignored and the output truncated to the last three valid octets if the input is incorrectly padded. -u, –help Print how to call information and a summary of options. –version Print program version information.

EXIT STATUS

base64 returns status 0 if processing was completed without errors, 1 if an I/O error occurred or errors were detected in decoding a file which indicate it is incorrect or incomplete, and 2 if processing could not be performed at all due, for example, to a nonexistent input file.

FILES

If no infile is specified or infile is a single "-", base64 reads from standard input; if no outfile is given, or outfile is a single "-", output is sent to standard output. The input and output are processed strictly serially; consequently base64 may be used in pipelines.

BUGS

Little or no error checking is done when decoding, other than validating that the input consists of a multiple of four characters in the encoding set. This is inherent in the design of base64, which assumes transmission integrity is the responsibility of a higher-level protocol.

SEE ALSO

qprint(1), uudecode(1), uuencode(1), RFC 1341

AUTHOR

John Walker

http://www.fourmilab.ch/

2.2.4. md5

`md5`[1] (Message Digest 5) ist ein sogenannter Message Digest[2]-Algorithmus, der aus beliebigem Text eine 128-Bit lange digitale Kennung erzeugen kann, der bei minimaler Text????
`md5` wird daher auch häufig als Authentifizierungsverfahren eingesetzt.
Man-Page unter http://campuscgi.princeton.edu/man?md5

NAME

md5 - calculate a message-digest fingerprint (checksum) for a file

SYNOPSIS

```
md5 [ -t | -x | -sstring | filename(s) ]
```

DESCRIPTION

md5 takes as input a message of arbitrary length and produces as output a 128-bit ffingerprintör mmessage digestöf the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be compressedin a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

OPTIONS

The following four options may be used in any combination, except that filename(s) must be the last objects on the command line. -s string prints a checksum of the given "string".

-t runs a built-in time trial.

-x runs a built-in test script.

filename(s) prints a checksum(s) for each of the files.

SEE ALSO

sum(1)

RFC 1321 describes in detail the MD2, MD4, and MD5 messagedigest algorithms.

ACKNOWLEDGEMENTS

This program is placed in the public domain for free general use by RSA Data Security.

[1] gemäß RFC 1321
[2] Botschaften-Auszug

2.2.5. Verschlüsseln und Entschlüsseln von Dateien zum Austausch mit Anderen

Da ein symmetrisches Verschlüsselungsverfahren[3] zum Austausch von Nachrichten/Dateien/... mit anderen nicht geeignet ist, wird hier ein RSA-Verfahren mit einem Schlüsselpaar beschrieben. Dabei besteht das Schlüsselpaar aus einem geheimem nur dem Absender bekannten Schlüssel und einem öffentlichen der ganzen Welt oder doch zumindest dem Empfänger, dem Sie die Nachricht/Datei/... zugänglich machen wollen, bekannten Schlüssel)

2.2.5.1. Erzeugen eines RSA Schlüsselpaares

Ein RSA-Schlüsselpaar wird folgendermaßen erzeugt

```
% mkdir $HOME/.pgp
% pgp -kg

Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:38 GMT

Wähle die Länge Deines RSA-Schlüssels aus:
1) 512 Bits: 'einfach kommerziell', schnell,
aber nicht ganz so sicher
2) 768 Bits: 'hochgradig kommerziell', mittelmäßig schnell,
recht sicher
3) 1024 Bits: 'militärisch', langsam, jedoch maximale
Sicherheit
Auswahl (1,2,3 oder die Länge des Schlüssels in Bits [384 bis 2048]): 3

Ich erzeuge einen RSA-Schlüssel mit einem 1024-Bit-Modulus.

Du brauchst eine Benutzer-ID für Deinen öffentlichen Schlüssel. Das
übliche Format für diese Benutzer-ID ist Dein Realname,
gefolgt von Deinem Usernamen in <spitzen Klammern>, falls
Du per E-Mail erreichbar bist.
Beispiel: Helmut Kohl <BIRNE@LINK-BN.cl.sub.de>
Gib die Benutzer-ID für Deinen öffentlichen Schlüssel ein:

Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de>

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu schützen.
Dein Mantra kann jeder beliebige Satz oder Zeichenfolge sein und darf
aus vielen Worten, Leerzeichen oder anderen druckbaren
Zeichen bestehen.

Gib das Mantra ein: xxxxxx xxxxxx xxxxxxx xxxxxxxxxx xxxxxx

Wiederhole das Mantra: xxxxxx xxxxxx xxxxxxx xxxxxxxxxx xxxxxx

Beachte, daß die Schlüsselerzeugung eine zeitaufwendige Sache ist.

Wir müssen 783 zufällige Bits erzeugen. Dies wird durch Messung
der Abstände zwischen Deinen Anschlägen bewerkstelligt. Bitte gib
irgendwelchen beliebigen Text auf der Tastatur ein, bis es piepst:
783 xxxxxxxxxxxxxxx
...
.....**** ...****
```

[3] beim Verschlüsseln wird derselbe Schlüssel wie beim Entschlüsseln benutzt

```
Das Mantra ist richtig.

Einen Augenblick, bitte....

Der Schlüssel wurde mit Deiner Unterschrift beglaubigt.

Die Erzeugung des Schlüssels ist beendet.
```

Das Überprüfen des Schlüssels kann folgendermaßen geschehen:

```
% pgp -kv
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:45 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/5647284D 2000/06/14 Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de>
Es wurde ein passender Schlüssel gefunden.
```

bzw.

```
% pgp -kvv
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:45 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/5647284D 2000/06/14 Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de>
Unt 5647284D Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de>
Es wurde ein passender Schlüssel gefunden.
```

2.2.5.2. Zertifizierung des PGP-Schlüssels

Zur Erhöhung der Vertrauenswürdigkeit eines öffentlichen Schlüssels kann man diesen bei Bedarf kostenlos zertifizieren lassen. Zunächst extrahiert man diesen in ASCII-Form:

```
% pgp -kxa Nachname nachname.pub
% cat nachname.pub.asc
```

Dazu konnte bislang die Seite

https://www.trustcenter.de

des Trustcenter aufgesuchte werden und der öffentliche PGP-Schlüssel dort (kostenlos) als Class1-Privatkunde zertifiziert werden. Trustcenter hat aber diesen Dienst eingestellt, lediglich bestehende Zertifizierungen können noch verlängert werden.
Ein ähnliches Angebot für Mitglieder der Universität Münster stellt deren Zertifizierungsstelle

http://www.uni-muenster.de/WWUCA/

dar. Ein Zertifizierungsantrag geht etwa wie folgt vor sich:

Nach Aufruf einer der obigen Seiten und folgen der Anweisungen, erhält man zunächst eine mittels PGP verschlüsselte e-mail, die in eine Datei geschrieben und dann mittels „`pgp Dateiname`“ entschlüsseln werden muss (den Hinweis auf die nicht überprüfbare Unterschrift ignorieren Sie hier einfach noch!).
In der Nachricht wird man nun aufgefordert, zur Verifizierung der eigenen e-mail Adresse eine Bestätigungsmail mit fest vorgeschriebenem Inhalt an die Zertifizierungsstelle zu senden. Nachdem dies geschehen ist, erhält man eine weitere e-mail, die den zertifizierten öffentlichen Schlüssel und die öffentlichen Signierschlüssel der Zertifizierungsstelle enthält.
Den zertifizierten öffentlichen Schlüssel (und eventuell auch die Trustcenter-Schlüssel) kann man nun mittels

```
% pgp -ka Dateiname.pub
```

dem eigenen Schlüsselring hinzufügen.

2.2.6. Sichern von Dateien gegen unbefugtes Lesen (Codieren)

Um verschlüsselte Dateien beispielsweise einem Kollegen zuzusenden, wird dessen öffentlicher Schlüssel benötigt. Hat man diesen noch nicht erfahren so kann man versuchen über

http://www.pca.dfn.de/dfnpca/pgpkserv/#extract

den Schlüssel zu erhalten.

Im Besitz des Schlüssels, einer Datei `xxx.pub` mit einem Inhalt ähnlich zu

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.4

mQCNAzONkfwAAAEEANyx5XD9uAk8e3b5cQQ3WyhaeVkNadH2BPovm28ctAirF0D/
...
HLMc4crlQm2Ev8RYWzzjkGbQnzjudtUyHingfBc=
=zRXA
-----END PGP PUBLIC KEY BLOCK-----
```

sollte dieser mittels

```
% pgp -ka xxx.pub
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 07:35 GMT

Suche nach neuen Schlüsseln...
öff 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>

Überprüfung der Unterschriften...
öff 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>
Unt! 94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>


Die Datei enthält folgende Schlüssel:
1 neü(n) Schlüssel

Ein oder mehrere neue Schlüssel sind nicht ausreichend beglaubigt.
Willst Du sie selbst beglaubigen? (j/N) n
```

dem eigenen öffentlichen Schlüsselring hinzugefügt werden.

Codiert man nun die eine Datei für Holger Wirtz `<wirtz@dfn.de>`, so erreicht man dies analog zu:

```
% pgp -e Sieb.p wirtz
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:14 GMT


Verschlüsselung mit Empfänger-Schlüssel(n).

Schlüssel für Benutzer-ID "Holger Wirtz <wirtz@dfn.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 94DB4A21, erzeugt am: 1997/05/29.
```

```
WARNUNG: Da dieser öffentliche Schlüssel nicht mit einer
vertraünswürdigen Unterschrift beglaubigt ist, ist nicht
sicher, daß er wirklich zu "Holger Wirtz <wirtz@dfn.de>" gehört.

Bist Du sicher, daß Du diesen Schlüssel benutzen willst? (j/N) j
.
Verschlüsselte Datei: Sieb.p.pgp
```

Die Datei `Sieb.p.pgp` kann nun nur noch vom Besitzer des privaten Schlüssels von "`Holger Wirtz <wirtz@dfn.de>`" entschlüsselt werden:

```
% pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:15 GMT

Die Datei ist verschlüsselt. Zum Lesen wird der private
Schlüssel benötigt.

Diese Nachricht kann nur gelesen werden von:
Holger Wirtz <wirtz@dfn.de>

Dir fehlt der private Schlüssel zum Entschlüsseln dieser Datei.

Eine Übersicht der PGP-Befehle erhältst Du mit: pgp -h
Ausführlichere Hilfe findet sich in der PGP-Anleitung.
```

Soll die codierte Datei ebenfalls von uns decodiert werden können, so muss für die Verschlüsselung der eigne Name (hier: Nachname) angegeben werden:

```
% pgp -e Sieb.p wirtz Nachname
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:22 GMT


Verschlüsselung mit Empfänger-Schlüssel(n).

Schlüssel für Benutzer-ID "Holger Wirtz <wirtz@dfn.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 94DB4A21, erzeugt am: 1997/05/29.

WARNUNG: Da dieser öffentliche Schlüssel nicht mit einer
vertraünswürdigen Unterschrift beglaubigt ist, ist nicht
sicher, daß er wirklich zu
"Holger Wirtz <wirtz@dfn.de>" gehört.
Aber Du hast diesen Schlüssel trotzdem bereits benutzt...

Schlüssel für Benutzer-ID "Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de",
1024-Bit-Schlüssel, Schlüssel-ID: 5647284D, erzeugt am: 2000/06/14.
.
Verschlüsselte Datei: Sieb.p.pgp
```

Jetzt können "`Holger Wirtz <wirtz@dfn.de>`" und
"`Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de`" die Datei decodieren:

```
pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
```

```
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:27 GMT

Die Datei ist verschlüsselt. Zum Lesen wird der private
Schlüssel benötigt.

Schlüssel für Benutzer-ID "Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.
    de",
1024-Bit-Schlüssel, Schlüssel-ID: 5647284D, erzeugt am: 2000/06/14.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
Gib das Mantra ein: ...
```

mit Ihrem Nachnamen ausgeführt werden!

Bemerkung: „`pgp -ew`“ und „`pgp -ea`“, „`pgp -ewa`“ sind analog wie oben benutzbar.

2.2.7. Sichern von Dateien gegen Fälschungsversuche (Signieren)/Unterschrift

2.2.7.1. Sichern von Dateien für den lokalen Gebrauch

Beim Signieren wird nur das eigene RSA-Schlüsselpaar benötigt: Der die signierte Datei Überprüfende benötigt jedoch den öffentlichen Schlüssel des Signierenden. Signierte Dateien sind ein Mittel, Erstveröffentlichungrechte von elektronischen Publikationen, ... zu sichern - die Bibliothek der Universität Wuppertal (http://www.bib.uni-wuppertal.de benutzt zur Zeit im Wuppertaler Hochschulschriftenserver zur Sicherstellung der Authentizität der elektronischen Dokumente den MD5-Digest, wird jedoch zukünftig wahrscheinlich externe PGP-Unterschriften (die ein Datum und die Unterschrift/Signierung enthalten) benutzen. **Beispiel:**

```
MD5 für MS-DOS:
Bergische Universität - Gesamthochschule Wuppertal,

Dissertation
Hübschen,Thorsten
Lokale Fortsetzbarkeit holomorpher Abbildungen im nicht-pseudokonvexen Fall 2002

MD5 (d070201.pdf) = 60ce41e3a6d3456a9578ad85564f06fe
```

Dateien werden durch

```
% pgp -sb übung9.pdf
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:38 GMT

Für eine Unterschrift wird ein privater Schlüssel benötigt.
Da Du keine Benutzer-ID für Deinen privaten Schlüssel angegeben hast,
wird der letzte zum privaten Schlüsselbund hinzugefügte Schlüssel
benutzt.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Gib das Mantra ein:
Das Mantra ist richtig.

Einen Augenblick, bitte....
Unterschriftsdatei: übung9.pdf.sig
```

oder mittels

```
% pgp -sba übung9.pdf
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:38 GMT

Für eine Unterschrift wird ein privater Schlüssel benötigt.
Da Du keine Benutzer-ID für Deinen privaten Schlüssel angegeben hast,
wird der letzte zum privaten Schlüsselbund hinzugefügte Schlüssel
```

```
benutzt.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Gib das Mantra ein:
Das Mantra ist richtig.

Einen Augenblick, bitte....
Dateiname der Versandhülle: übung9.pdf.asc
```

signiert.

Überprüfen von signierten Dateien auf Authentizität

```
% pgp übung9.pdf.asc
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:40 GMT

Diese Datei trägt eine Unterschrift.
Zur Überprüfung wird der öffentliche Schlüssel benötigt.

Die Datei 'übung9.pdf.$00' enthält eine Unterschrift, aber keinen Text.
Der Text könnte sich in der Datei 'übung9.pdf' befinden.
.
BESTÄTIGTE Unterschrift von "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
Unterschrift erzeugt am 2000/06/15 08:38 GMT mit 1024-Bit-Schlüssel 0x8EC88425.

Unterschrift und Text sind getrennt. Es wurde keine Ausgabedatei erzeugt.
```

2.2.7.2. Sichern von Dateien gegen Fälschungsversuchen beim Austausch mit anderen

Kehren wir zu unserem Beispiel zurück, in dem wir einem Kollegene eine Datei übermitteln wollten. Der Empfänger möchte dann natürlich die Datei auf Authentizität überprüfen und benötigt dazu unseren öffentlichen Schlüssel. Er muss den Schlüssel mittels „`pgp -ka`“ seinem Schlüsselring hinzufügen. Dann kann er ebenfalls durch

```
% pgp Datei.Extension.asc
```

oder

```
% pgp Datei.Extension.sig
```

die Authentizität der übermittelten Datei überprüfen.

Codieren und Signieren von Dateien
Mittels „`pgp -sea`“ ist das Codieren mit dem Signieren kombinierbar.

2.2.8. Austausch des öffentlichen PGP-Schlüssels

2.2.8.1. per e-mail

Ein Kollege möchte eine von uns signierte Datei auf Authentizität überprüfen und bittet uns, ihm unseren öffentlichen Schlüssel zu schicken. Das kann man folgendermaßen bewerkstelligen:

```
% pgp -kxa buhl buhl.pub
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:07 GMT

Extrahieren aus dem Schlüsselbund: '/home/buhl/.pgp/pubring.pgp'
Benutzer-ID " buhl ".

Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Dateiname der Versandhülle: buhl.pub.asc

Schlüssel extrahiert in Datei 'buhl.pub.asc'.
```

Nun müssen wir ihm den Inhalt der gerade erzeugten Datei zuschicken, der folgende Gestalt haben könnte:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzk5RF4AAAEEANn+XJ7G/eqjFnpfVNrz4iwLs0x7OjIJi/ynNTOgirD5VF7k
LcH6lOPX2+gbYMneXjA4mcp453H1NihqeZEfzfT9L6ZX6HNEQguU5NgwXP3JZXDT
/WopNMaKrULckUgrJadu174DKeK4ERL34Pvc3XctM4haVUfg6obmfx2OyIQlAAUT
tEVQcm9mLiBEci4gSGFucy1KdWVyZ2VuIEJ1aGwgPEhhbnMtSnVlcmdlbi5CdWhs
```

```
QG1hdGgudW5pLXd1cHBlcnRhbC5kZT6JAJUDBRA5OURehuZ/HY7IhCUBAW8UA/9E
AfiYTATybYe3m7FXZ7VkBj/jA5IR4U+eHjJbnJtCgiVsE9wwvNbqpa6HAvI+488n
i4TlLgKHXc7Yh0A+vWYhnPpEa01HZ9At3A+0bYvL7CEGq2g1Zar/dlylHK2WxTMQ
1MLGxoM3C872yDhyqWhsWSNCuwHjgC0goTEimm11Lw==
=xPxi
-----END PGP PUBLIC KEY BLOCK-----
```

Unser Kollege erzeugt sich jetzt eine eigene Datei `buhl.pub` mit obigem Inhalt und fügt unseren öffentlichen Schlussel seinem Schlüselring hinzu:

```
% pgp -ka buhl.pub
```

Eventuell möchte er sich davon überzeugen, dass auf dem Mailwege nicht eine Verfälschung des Schlüssels erfolgte und überprüft den Fingerprint unseres Schlüssels:

```
% pgp -kvc
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:13 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/8EC88425 2000/06/03 Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>
Fingerabdruck des Schlüssels: 0D 8D 6A 80 A9 A3 4A D8 84 A8 EA 2E 92 33 A6 F6
Es wurde ein passender Schlüssel gefunden.
```

Jetzt könnte er uns per Telefon bitten, die Übereinstimmung des Fingerabdrucks zu überprüfen:

```
% pgp -kvc buhl
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:16 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':
Suche nach Benutzer-ID "buhl":

Typ Bits/ID Datum Benutzer
öff 1024/8EC88425 2000/06/03 Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>
Fingerabdruck des Schlüssels: 0D 8D 6A 80 A9 A3 4A D8 84 A8 EA 2E 92 33 A6 F6
Es wurde ein passender Schlüssel gefunden.
```

2.2.8.2. auf dem (weltweiten) PGP-Schlüssel-Server (WWW-Interface)

Auf der WWW-Seite

http://www.pca.dfn.de/dfnpca/pgpkserv/#submit

können Email-Adressen und zugehörige PGP-Schlüssel abgespeichert werden. Dazu muss nur auf der obigen Internet-Seite die e-mail Adresse sowie im Feld "`ASCII-Version Ihres Schlüssels`" den mit "`-----BEGIN PGP PUBLIC KEY BLOCK-----`" beginnenden Teil des Outputs von "`pgp -kxaf IhrName`" eingegeben werden und auf "`Absenden an den Key Server!`" geklickt werden.

2.2.9. Abfrage eines öffentlichen PGP-Schlüssels

2.2.9.1. auf dem (weltweiten) PGP-Schlüssel-Server (WWW-Interface)

Benötigen wir z.B. den öffentlichen Schlüssel von unserem Kollegen Herrn Holger Wirtz (`wirtz@dfn.de`), so können wir diesen über das oben besprochene WWW-Interface erhalten.
Dazu einfach in das Such-String-Feld der WWW-Seite

http://www.pca.dfn.de/dfnpca/pgpkserv/#extract

oder der Seite

http://www.pgp.net/pgpnet/wwwkeys.html

`Holger Wirtz` eingeben und auf den "`Suche starten!`"-Knopf drücken:

```
Public Key Server -- Index ‘‘holger wirtz ’’

Type bits/keyID Date User ID
pub 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>
pub 1024/155FD609 1995/08/21 Holger Wirtz <root@midips.snafu.de>
Holger Wirtz <wirtz@dfn.de>
Holger Wirtz <chick@midips.snafu.de>
```

Klickt man jetzt auf `wirtz@dfn.de` so erhält man

```
Public Key Server -- Get ‘‘0x94DB4A21 ’’

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.4

mQCNAzONkfwAAAEEANyx5XD9uAk8e3b5cQQ3WyhaeVkNadH2BPovm28ctAirFOD/
L3j67I5ql1v5ü129zhbcwhCvXU1u+ig3zgy+ZjXkZF9UW31bRvxUYlm+6jCnpSA
vYTODu5D19tD+FJJRDNwsfVCS396Jqx9GHsiJ0urZRHiCo2psmn58OWU20ohAAUR
tBtIb2xnZXIgV2lydHogPHdpcnR6QGRmbi5kZT6JAJUDBRAzjZH8afnw5ZTbSiEB
AVM4A/9NyNc7NLjF/t7qfc8DSKWSyxI7mTS07LrpZQMh8Zm5WcicO1QsYo7kB48m
uBGFMtAIwQo5Ea6qDCgcWzj7YqY60m3uZH/jQPS3V+wQs9lUsqdvKLdlTKn6Ouw8
mKTxyRpmF3jQ1RNkXD38cnTXyevnn0bM3kZnljecLy+Z8ceeu4kBFQMFEDOf5fmT
76X8/pPquQEBccYH/1TaA8Z+7jxnDhlJZnIj8rfs4Y3Z/EXNcv+Maw6WpCzKf61Q
kQNyYpN7+Qd0HdrgvKQ7iOqlSBJtVSnrlTduzzMYJN15K4döuIVe4dDPSNfy4P5
rkxbzZWVSQcöA/tfUks4dDCdwTLmDGmTsswFFAF2ayTRJYU+1By6Dbpn+cjFC+X
B1FPgZu2birz0KTfATkOIGFmVRjh3iOvPeNXHcCLlrQ/bEBuCgKbjJiUKHOGhy7u
S2QR4RMGlSoVFm1faXcmCTHcaTRiP/9W6rUAEgT3ufHvAXpjGebpUGhrL3fMeX2x
HLMc4crlQm2Ev8RYWzzjkGbQnzjudtUyHingfBc=
=zRXA
-----END PGP PUBLIC KEY BLOCK-----
```

(Den Fingerabdruck kann man sich über den Knopf "`Anzeige der Fingerprints`" anzeigen lassen.)

2.2.9.2. auf dem Trustcenter Zertifikat-Suchserver (WWW-Interface)

Über die WWW-Seite

https://www.trustcenter.de:443/fcgi-bin/search.cgi

oder

https://www.trustcenter.de:443/certservices/search/de/pgp_suche.htm

kann man PGP und S/MIME-Zertifikate suchen, die das Trustcenter ausgestellt hat. PGP-Zertifikate sollten in eine Datei heruntergeladen und dann mittels "`pgp -ka Dateiname`" der öffentlichen PGP-Datenbank hinzugefügt werden.

2.2.10. PGP unter Windows

2.2.10.1. Die Aegis-Shell als GUI für PGP unter Windows

Im Fachbereich Mathematik kann eine CD ausgeliehen werden, die die Binaries fur PGP und eine GUI-basierte Shell für PGP enthält.

Alternativ kann dies auch im Internet gefunden werden:

PGP (`http://www.pgp.com`)

Aegis-Shell (`http://www.aegis.com`)

Verschlüsselungs-Software PGP 8.0 ist fertig

Nachdem die ersten Beta-Versionen bereits anständig funktionierten, stellt – wie bereits angekündigt – die PGP Corporation jetzt die Final-Version von PGP 8.0 für Windows und Macintosh zum Download bereit. PGP (Pretty Good Privacy) ist die am weitesten verbreitete Verschlüsselungs-Software nach dem OpenPGP-Standard.

Für die neue Ausgabe gibt es jetzt vier Preismodelle. Nach wie vor gibt es eine Freeware-Version (`http://www.pgp.com/display.php?pageID=83`), die für die private Nutzung kostenlos ist. Dazu kommt die "Desktop Edition" für 80 US-Dollar, die die bekannte Festplattenverschlüsselung PGP Disk und Mail-Plugins bietet. Die "Enterprise Edition" kommt auf 125 US-Dollar und bietet zusätzlich ADK-Support (Additional Decryption Keys) und Komfortfunktionen für Administratoren. Die "Personal Edition" für 39 US-Dollar ist eine abgespeckte Desktop Edition, in der die Integration mit Microsoft Exchange und Lotus Notes fehlt. (pab/c't)

Abbildung 2.1.: Quelle: heise online
`http://www.heise.de/newsticker/data/pab-03.12.02-001/`

2.2.11. Dokumentation von PGP

- `man pgp`
- `more /opt/local/Sys/pgp263is/doc/pgpdoc1.txt`
- `more /opt/local/Sys/pgp263is/doc/pgpdoc2.txt`
- http://www.foebud.org/pgp/
- http://senderek.de/security/schutz.html
- Simon Garfinkel: PGP, O'Reilly, 1996

2.2.12. Quellen

- ftp://ftp.dfn.de/pub/net/mail/pgp262uis.tar.gz
- CD des FB7 mit Windows-Versionen von pgp, Aegis und ssh2.1.0
- SuSE HowTos http://www.suse.de/de/private/support/howto/index.html
- Aegis http://www.aegis.com

2.3. SSL und https

2.4. Secure Shell und sichere X-Verbindungen

2.5. xdm/kdm und Netzwerksicherheit

2.6. Virenscanner und Firewalls

3. Internet-Protokolle — technische Grundlage

3.0. Uucp und das Internet

Das Internet ist ein (das) weltweites internet, d.h. eine weltweit verteilte Ansammlung von Netzwerken, die über sogenannte Router verbunden sind.

Einen Ausschnitt dieses Netzwerkes veranschaulicht Abbildung (3.1).
Das Hochschulnetz der Uni Wuppertal ist also im DFN-Forschungsnetz mit den anderen Hochschulnetzen verbunden und das DFN-Netz ist wiederum mit anderen Netzen verbunden...

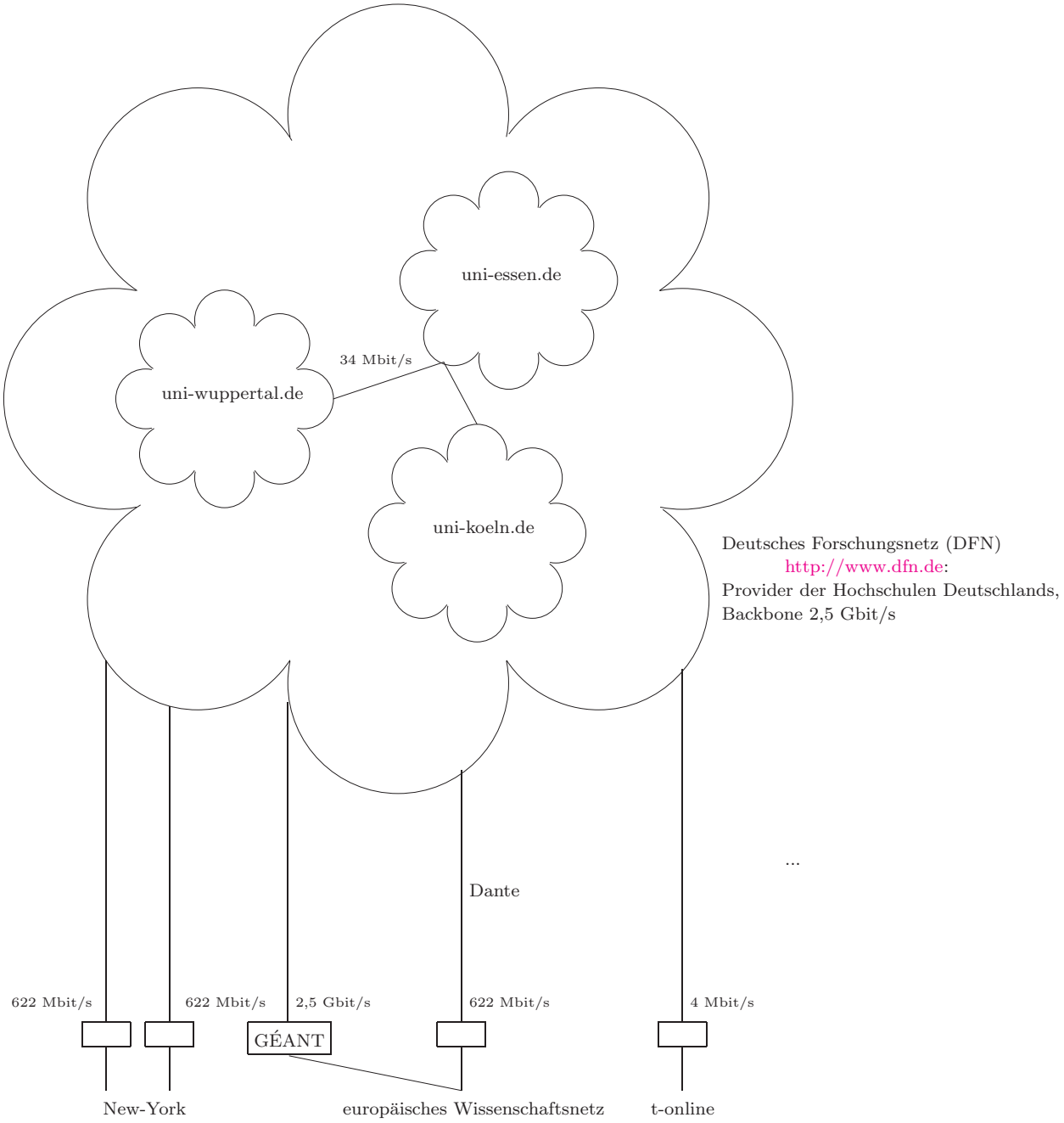
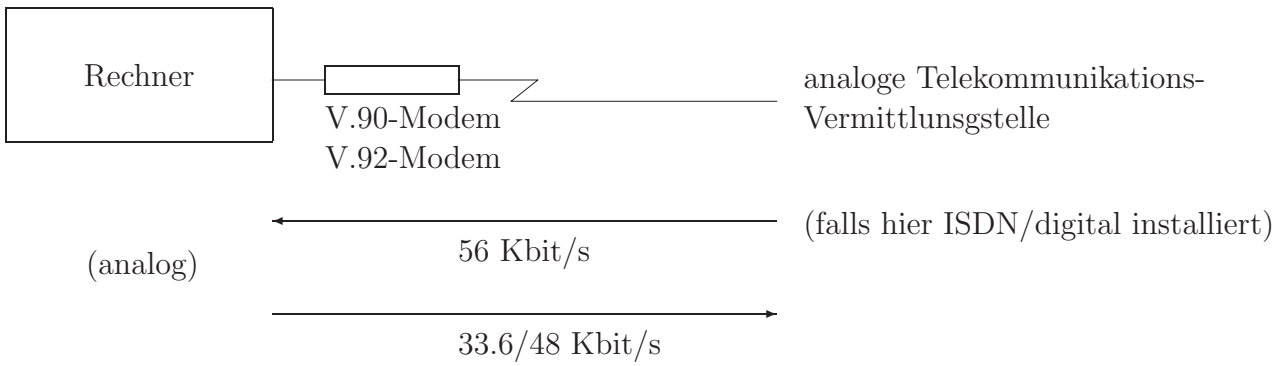


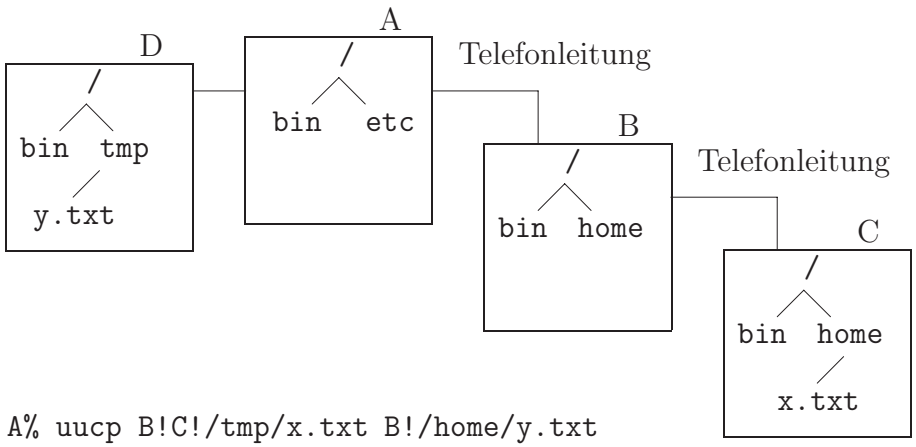
Abbildung 3.1.: G-WiN des Deutschen Forschungsnetzes

Der typische Anschluss eines einzelnen Rechners an ein nichtlokales Netzwerk:



Der Vorläufer des Internets, uucp, hat folgende Dienste bereitgestellt

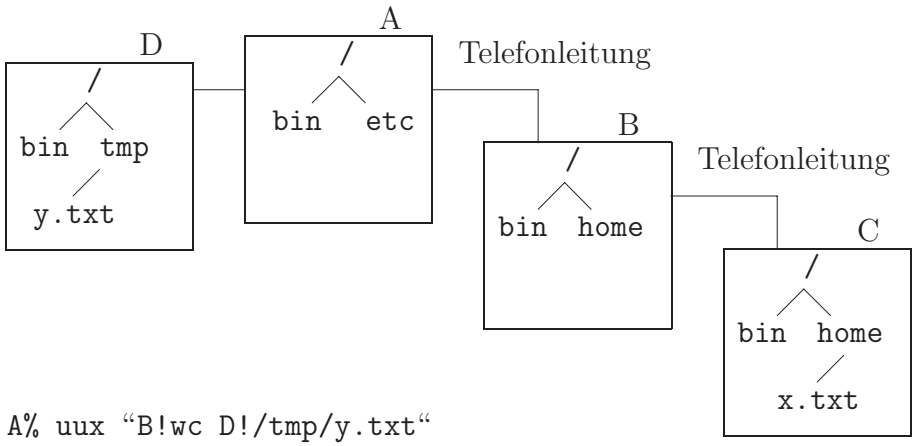
- uucp




```
A% uucp B!C!/tmp/x.txt B!/home/y.txt
```

(unix to unix copy: zum Kopieren von Dateien zwischen zwei (entfernten) Rechnern)

- uux




```
A% uux “B!wc D!/tmp/y.txt“
```

(unix to unix execute: zum Ausführen von Kommandos auf fremden Rechnern mit Dateien auf (nochmals) fremden Rechnern)

- Email

  wird relyed (stationsweise weitergereicht), benutzt uucp

- Usenet Netnews

  Diskussionsforen werden ebenfalls relyed (zur Zeit mit einem Datendurchsatz von ca. 1,1 GB/Tag)

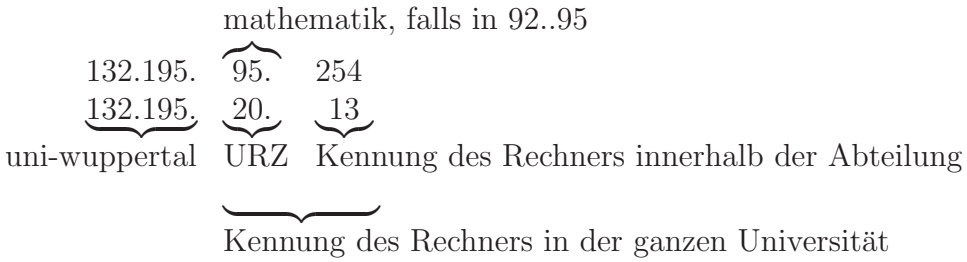
Die Lage eines Rechners (relativ zum eigenen Rechner) wird als Rechnername benutzt, dieser ist also topologieabhängig:

Jeder Zielrechner wird auf unterschiedlichen Rechnern durch einen anderen "Pfad" angesprochen. Nach einem Ausfall von nur einem Rechner, kann derselber Rechner vielleicht über einen anderen Pfad immer noch angesprochen werden, aber diesen Pfad muss man erst erfragen. Das ist im Internet nicht praktikabel, weshalb dort internetweite eindeutige Rechnernamen eingeführt wurden: die IP-Adressen.

3.1. IP-Adressen

IPv4

Beispiele von IP-Adressen:



IP-Adressen gemäß IPv4 werden mit 4*8 Bit (je 0..255) angegeben. Man unterscheidet dabei 4 verschiedene Netztypen:

A	0	$Netz_7$	$Host_{24}$
B	10	$Netz_{14}$	$Host_{16}$
C	110	$Netz_{21}$	$Host_8$
D	1110	Multicast $group_{28}$	

Damit ergeben sich dann folgende IP-Adressen in den verschiedenen Netzen

A	0.0.0.0 .. 127.255.255.255
B	128.0.0.0 .. 191.255.255.255
C	192.0.0.0 .. 223.255.255.255
D	224.0.0.0 .. 239.255.255.255

132.195.x.x ist also ein Class B Netz mit bis zu $2^{16} = 65.536$ verschiedenen Host-Adressen. Zwei Hostadressen dienen dabei für Sonderzwecke:

132.195.0.0	Netzwerkadresse für das gesamte Netzwerk
132.195.255.255	Broadcast (Damit kann ein Datenpaket an alle Rechner dieses Netzes gesendet werden.)

Weiter Sonderadressen:

Es gibt zusätzliche Adressen, die nicht international eindeutig sind. Sie werden für weitere Sonderzwecke (loopback_interface)), automatische „private“ Adressvergabe auf Windows XP-Rechnern, HP-Netzwerkdruckern,... verwendet:

A	127.0.0.1	das sogenannte loopback interface, damit wird also nur der eigene Rechner angesprochen (auch `localhost`)
B	169.254.0.0	private Netze für Apple/Microsoft (APIPA=automatic private IP addressing)
	172.16.x.x ... 172.31.x.x	für 16 private Netze reserviert, z.B. Intranet (keine Kommunikation ins Internet über diese Internetadressen)
C	192.168.0.x ... 192.168.255.x	256 private Netze

IPv6 oder auch IPng

Dieser Standard benutzt 128 Bit lange Adressen. Dies behebt den großen Mangel an IP-Adressen im Internet. Z.B.

47CD:12AB:CDEF:1234:000A:000B:000C:ABCD

Dies sind 8*16 Bit = 128 Bit = 16 Byte
Weitere Beispiele entnehmen Sie der folgenden Datei

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1 localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts

127.0.0.2       linux.local  linux
```

3.2. Subnetze und Netzmasken

Subnetze werden zur Unterteilung etwa eines Class B-Netzwerkes in kleinere Unternetze benutzt:

132.195.92.0 ... 132.195.95.255

ist ein IP-Adressbereich, der für die Rechner des Fachbereichs Mathematik benutzt wird. der Netzverkehr (inklusive Broadcasts) dieser Rechner untereinander bleibt auf diesen Teilbereich beschränkt.

Rechner z.B. im Subnetz des Fachbereichs Physik können diesen Netzverkehr nicht „mithören“, Damit wird eine höhere Netzwerksicherheit erreich. Zusätzlich belasten Datentransfers innerhalb des Mathematik-Subnetzes nicht die Netzwerkkapazität der anderen Subnetzwerke.

Zur Erzeugung von solchen Subnetzen dienen sogenannte Netzmasken:

Class	default Netzmaske
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Die Netzmaske hat denselben Aufbau wie eine IP-Adresse. Bei ihr bedeutet jede binäre Bitstelle, ob das stellengleiche Bit der IP-Adresse zur Netzwerkkennung (wenn 1) oder zur Hostkennung gehört.

Um also 132.195.92 ... 132.195.95 im selben (Sub-)Netzwerk zu platzieren muss, die Netzmaske

92_{10}	=	$0101\ 1100_2$
93_{10}	=	$0101\ 1101_2$
94_{10}	=	$0101\ 1110_2$
95_{10}	=	$0101\ 1111_2$
Maske		$1111\ 1100_2 = 252_{10}$

zu 255.255.252.0 gewählt werden.

Wenn Sie einen Rechner

132.195.83.1

mit der Netzmaske 255.255.248.0 installieren, heißt das also, dass ein Subnetzwerk mit der Netzkennung

$$132.195.83.1\ \mathrm{AND}_{\mathrm{bitweise}}\ 255.255.248.0{=}132.195.80.0$$

und der Broadcastadresse

$$132.195.83.1\ \mathrm{OR}_{\mathrm{bitweise}}\ 0.0.7.255{=}132.195.87.255$$

im Fachbereich Elektrotechnik benutzt wird. (Dabei geht 0.0.7.255 durch bitweises Komplement aus 255.255.248.0 hervor.)

Einen Ausschnitt der innerhalb der Universität Wuppertal benutzten Subnetze kann unter

http://www.hrz.uni-wuppertal.de/dienste/netz/subnetze/

gefunden werden:

Fachbereich	**Domain/ Subnetze**	**Gateway**	**Netzmaske**
FB 1 Gesellschafts- wissenschaften	gewil 132.195.1	132.195.20.201	255.255.192.0
FB 2 Geschichte, Philo- sophie, Theologie	geistwi 132.195.2	132.195.20.201	255.255.192.0
FB 3 Erziehungswissen- schaften	erziwi 132.195.3	132.195.20.201	255.255.192.0
FB 4 Sprach- und Literaturwissen- schaften	lingu 132.195.4	132.195.20.201	255.255.192.0
FB 5 Design, Kunst, Druck (Gaußstr.	kunst 132.195.5	132.195.20.201	255.255.192.0
FB 5 Computational Design (Hofaue)	kunst 132.195.65	132.195.65.254	255.255.255.0
FB 5 Design, Kunst, Druck (PKS)	kunst 132.195.68	132.195.71.253	255.255.252.0
FB 5 Kommunikations- technologie Druck (Campus Freudenberg)	kommtech 132.195.88	132.195.89.254	255.255.254.0
FB 6 Wirtschaftswissen- schaft	wiwi 132.195.6 132.195.38	132.195.20.201	255.255.192.0
FB 7 Mathematik	math 132.195.92 ⋮ 132.195.95	132.195.95.254	255.255.252.0
	⋮		

Abbildung 3.2.: Subnetzstruktur an der BU Wuppertal

3.3. Konfiguration eines (TCP/IP-)Netzwerkanschlusses

3.4. Routing

3.5. Symbolische Namen — DNS

3.6. LDAP-Adressbücher

3.6.1. Nutzung zur automatischen Adressergänzung

3.6.2. Einrichten eines LDAP-Servers: openldap/Netscape Directory Server

3.6.3. Automatische LDAP-Eintragsgenerierung

Literaturverzeichnis

1. Internet, zum Beispiel:

   http://src.doc.ic.ac.uk/bySubject/Computing

   http://www.google.de

2. Benutzerhinweise:

   - Einführung in die Benutzung der Ausbildungsrechner des Fachbereichs Mathematik
   - Ergänzende Informationen zur Benutzung der PCs im IT-Raum G.16.15
   - Benutzungsordnung für die Benutzung der Ausbildungsrechner
   - Netiquette

3. Duden Informatik, Ein Sachlexikon für Studium und Praxis, Dudenverlag, Mannheim

4. Wendy G. Lehnert: Light on the Web - Essentials to Make the 'Net Work for You, Addison-Wesley, 2002

5. W. Richard.Stevens: TCP/IP Illustrated, Volume 1, The Protocol, Addison-Wesley, Ready

Software

1. Suse Linux 8.1
2. Windows 2000 Advanced Server
3. Windows XP Professional

zum Testen und zur Durchführung der Praktikumsaufgaben benötigt (im Rahmen des MSDN-AA kostenlos für Studenten verfügbar).