Inforz April 2006

Inforz

Zeitschrift der Studierenden der Informatik
der TU Darmstadt

April 2006

ISSN: 1614-4295

Liebe Studierende,

das Sommersemester 2006 ist da. Sommer, Sonne, Sonnenschein? Zumindest draußen. Doch auch drinnen, im Internet?

Der Überwachungsstaat breitet sich aus und alles wird digital. Es wird der biometrische Reisepass und die elektronische Gesundheitskarte eingeführt. Mit der letzteren haben wir uns auseinandergesetzt und ihre Funktionsweise und Risiken durchleuchtet. Und kann man sich trotz Überwachung noch sicher im Internet bewegen? Wir gehen der Sache auf den Grund.

Anfang des Jahres waren ein paar Schüler zu Besuch, die von Studierenden den Universitätsberieb gezeigt bekommen haben. Wer in Zukunft von Euch Lust hat, auch mal einer Schülerin oder einem Schüler das harte Studentenleben zu präsentieren darf sich gerne bei uns melden.

Wer es noch nicht gemerkt hat: dieses Jahr ist unser Jahr! Also, wenn Du Informatiker bist zumindest. Oder Mozart — der hat auch sein Jahr. Darum wird auch ein bißchen mehr Rummel gemacht als um das „Jahr der Informatik“. Trotzdem haben wir mal geschaut, was so abgeht.

Ach ja, wir haben auch wieder mal Professorenzuwachs bekommen. Alexander May ist neu und war bei uns zu Besuch in der Fachschaft.

Viel Spaß beim Lesen wünscht
Arne Pottharst und das Inforz-Team

Und natürlich gibt's noch mehr Inhalte:

Arne Potthast

Herr Professor May, wie wirft man Münzen durch das Telefon?

Prof. Alexander May ist seit November 2005 am Fachbereich Informatik im Fachgebiet „Kryptographische Protokolle“. Er tritt hier die Nachfolge von Prof. Takagi an, der einen Ruf nach Japan erhalten hat.

Was ist Ihr Forschungsgebiet?

Mein Forschungsgebiet ist Kryptographie, algorithmische Zahlentheorie, speziell RSA bei mir und Gitterreduktion. Das hört sich sehr mathematisch an, ist aber alles in der Kryptographie verankert.

Die algorithmische Zahlentheorie beschäftigt sich unter anderem damit, große Zahlen zu faktorisieren und diskrete Logarithmen effizient zu bestimmen.

Welche Lehrveranstaltungen bieten Sie dazu an?

Im Moment gibt es Public Key Kryptanalyse, das sollte man hören, wenn man schon die Einführung in die Kryptographie gehört hat, denn es ist eine weiterführende Veranstaltung und da stelle ich moderne Methoden der Kryptanalyse vor.

Es gibt auch ein Seminar im Moment über kryptographische Protokolle, so heißt übrigens auch mein Fachgebiet. Dort geht es um einfache Protokolle, wie man beispielsweise Münzen wirft übers Telefon, wie man Geheimnisse austauscht, etc.

Wie wirft man denn Münzen durchs Telefon?

Nehmen Sie an, sie wollen eine Münze werfen, obwohl sich ihr Gesprächspartner am Telefon befindet. Wenn nun A eine Münze wirft, kann B am anderen Ende das nicht überprüfen und betrogen werden. A kann ja immer behaupten: Du hast Kopf getippt, ich habe aber Zahl geworfen. Die Frage ist, wie

man es vorher festlegen kann, was A geworfen hat, ohne es dabei B zu verraten. A schickt erst eine Festlegung über die Leitung und sagt: Ich habe die Münze geworfen, aber er steckt sie sozusagen in einen Umschlag, das heißt sie ist durch eine mathematische Funktion geschützt. Dann sagt B: Ich wähle Kopf, und der Umschlag wird geöffnet und nachgeschaut, was das tatsächliche Ergebnis ist. Das wäre beispielsweise ein ganz einfaches kryptographisches Protokoll.

Wer denkt, dass Kryptographie so ein bisschen James Bond ist, täuscht sich

Was müssen die Studierenden mitbringen, wenn sie bei Ihnen Veranstaltungen hören wollen?

Das kommt natürlich ganz darauf an, welche Veranstaltung. Auf jeden Fall Interesse an der Mathematik. Mathematik ist ganz wichtig in der Kryptographie, vor allem auch in der Einführung in die Kryptographie. Wer denkt, dass Kryptographie nur so ein bisschen James Bond ist, der täuscht sich leider. Das ganze ist diskrete Mathematik und angewandte Algebra.

Es ist bei meinen derzeitigen Veranstaltungen auf jeden Fall von Vorteil, wenn man die Krypto-Einführung gehört hat. Es muss nicht unbedingt sein, ich versuche ganz bei Null anzufangen, aber das geht natürlich nicht immer. Die einfachen Kryptoverfahren wie RSA und El-Gamal mache ich im Schnellverfahren nochmal, um alle auf die selbe Notation zu bringen, weil jeder Dozent eine eigene Notation verwendet.

Wieso sind Sie ausgerechnet nach Darmstadt gekommen?

Gute Frage. Einerseits natürlich wegen der Professur, Juniorprofessuren werden nicht so viele ausgeschrieben, gerade in meinem Gebiet. Ich wollte unbedingt Kryptographie machen und da gibt es nicht so besonders viele Stellen. Daher freue ich mich, nun hier zu sein.

Das Gebiet ist ja zur Zeit ziemlich gefragt.

Das Gebiet schon, aber Stellen gibt es eben nicht viele. Der andere Aspekt war, daß die Gruppe rund um J. Buchmann hier sehr interessante Kooperationsmöglichkeiten für mich bietet. Es ist angenehm mit ihr zusammenzuarbeiten, es gibt einige Leute, die verwandte Dinge in der Forschung machen. Wir haben hier insgesamt in der Datensicherheit eine ziemlich gute Infrastruktur. Es gibt gar nicht so viele, die in Deutschland Sicherheit und Krypto machen, die Buchmann-Gruppe ist eine der bekanntesten.

Was war Ihr erster Eindruck, als Sie hier nach Darmstadt gekommen sind?

Ich war vorher schonmal hier, und zwar im alten Gebäude.

In der Alexanderstraße.

Genau. Da dachte ich damals: ach nee, nach Darmstadt willst du eigentlich nicht. In Paderborn hatten wir schöne Räume, das waren alte Forschungsgebäude von Nixdorf, der hatte sie damals der Informatik überlassen. Wir waren da nicht auf dem Campus mit den anderen sondern hatten eigene Räume, das war schon exklusiv. Da hatte jeder Teppichboden, nicht so wie hier … (lacht)

Aber ich war sehr angenehm überrascht, als ich das neue Gebäude gesehen habe. Die Vorlesungs- und Seminarräume sind sehr schön, auch die Nähe zum Herrngarten.

Ist Ihr Büro zum Herrngarten hin?

Neenee, ich glaube da braucht man eine bessere Stelle als eine Juniorprofessur, um in den Genuss zu kommen.

Was haben Sie gemacht, bevor Sie hierher gekommen sind?

Ich habe in Frankfurt Informatik studiert, das merkt man manchmal nicht, weil ich so viel Mathematik mache.

Haben Sie Mathematik als Nebenfach gemacht?

Nein, das auch nicht, ich hatte Physik, das war ein guter Ausgleichssport zur Informatik.

Nach der Diplomarbeit bin ich dann für ein halbes Jahr an die ETH Zürich gegangen. Der Betreuer meiner Dissertation ist dann nach Paderborn gegangen, so kam ich auch dorthin. In Paderborn war ich vier Jahre, ich habe promoviert und war anschließend noch von der DFG (Deutsche Forschungsgesellschaft) angestellt. Da hatte ich einen Antrag geschrieben und eine eigene Stelle erhalten.

Was war im Studium Ihr Lieblingsfach?

Ich habe am liebsten Theorie gemacht. Das ist in Frankfurt ein großer Bereich, es gibt viele Veranstaltungen dazu, beispielsweise effiziente Algorithmen, parallele Algorithmen, aber mein Faible war damals schon die Kryptographie.

Das ist in in Darmstadt allgemein nicht so beliebt, vielleicht können Sie das mit ein paar guten Vorlesungen mal auf Vordermann bringen.

Wie lange haben Sie studiert?

(lacht) Soll ich das jetzt wirklich sagen? Hmm, zwölf Semester. Ich habe gelesen, dass in Frankfurt der Schnitt am höchsten ist in ganz Deutschland: 19,x Semester, da sind aber sicherlich viele Karteileichen dabei.

Dann waren Sie ja noch gut dabei. Darmstadt hat übrigens etwa 13 Semester, da hätten Sie nicht ganz so gut abgeschnitten.

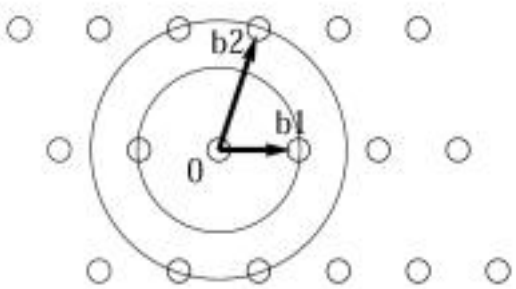
Ich hatte auch keine Lust, besonders schnell durchzukommen, dafür hat das Studium zu viel Spaß gemacht.

Was können Sie Studierenden aus Ihrer eigenen Erfahrung im Studium raten?

Immer in Übungen gehen, falls welche angeboten werden. Hier hat man eine gute Kontrolle, ob man den Stoff halbwegs verstanden hat. Wenn man schriftliche Übungen regelmäßig abgibt, hat man durch die Korrektur der Betreuer im allgemeinen ein geeignetes Feedback, welche Bereiche man sich nochmal genauer ansehen sollte.

Wie ist Ihr Verhältnis zu Studierenden? Lassen Sie Ihre Tür auf oder

Vektoren in einem Gitter. Sie dienen zum Bestimmen der Vektorbasis



Die kürzesten linear unabhängigen Vektoren

Alexander May (2)

braucht man bei Ihnen eine schriftliche Anmeldung drei Wochen vorher?

Die Tür steht offen, es kommen auch immer wieder Studierende mit Fragen zur Vorlesung und zur Übung zu mir. Meistens Donnerstags, weil Freitag morgens die Abgabe ist. Deswegen ist der Interviewtermin jetzt auch ganz günstig für mich (lacht) (es ist Donnerstag, Red.).

Sie wollen den Übungszettel zwar zwei Wochen vorher haben, machen es aber trotzdem erst am Abend vorher fertig. Aber bei uns war das damals ja auch nicht anders.

Die Besten sollten studieren dürfen, nicht die Reichsten

Finden wir sehr gut, wenn der Professor noch weiß, dass er auch mal Student war.

Bei mir ist es auch noch gar nicht so lange her.

Was sind Ihre Zukunftsvorstellungen, was wollen Sie mal werden?

Vermutlich erstmal Professor mit einer unbefristeten Stelle, aber ich weiß es noch nicht genau.

Was ich in fünf bist sechs Jahren mache, ist schwer vorherzusagen. Soweit ich verstanden habe, habe ich gar nicht die Möglichkeit hierbleiben. Die Frage ist, ob es eine Hausberufung wäre, wenn ich an der TU bleiben würde. Ich werde mich also zu gegebener Zeit auch nach anderen Unis umsehen.

Wenn Sie eine Million an Forschungsgeldern bekommen würden, was würden Sie damit machen?

Erstmal aufhören, Anträge zu schreiben.

Oder jemanden einstellen, der Anträge schreibt?

Ich würde mehrere Mitarbeiter einstellen, aber nicht zu viele, so drei bis vier wäre eine gute Gruppengröße.

Ich habe momentan das Gefühl, dass man nur dann genügend Zeit zur eigenen Forschung hat, wenn die Gruppe nicht zu groß ist. Wenn es zu viele Leute sind, ist man nur noch mit Verwalten beschäftigt. Ich möchte aber lieber mit allen Leuten zusammenarbeiten, insbesondere mit den Doktoranden. Das macht Spaß, und die Forschung gehört einfach dazu.

(überlegt) Eine Million, meine Güte, da müsste ich mir nochmal richtig Gedanken machen. Vielleicht würde ich auch was spenden an die Bibliothek und andere. Die Ausstattung hier ist ja sehr gut, da wüsste ich gar nicht, was ich noch bräuchte an Rechnern.

Theoretiker brauchen nicht so viel außer einem schnellem Rechner.

Wahrscheinlich würde ich Assistenten und Mitarbeiter einstellen und die Bibliothek ausstatten.

Und wissen Sie, was ich noch machen würde? Der Innenhof sieht scheußlich aus! (allgemeine Zustimmung, Szenenapplaus)

Da mein Fenster da raus geht, würde ich den Innenhof gerne mal erneuern. Das ist eine Schande — das Gebäude ist so schön, aber dieser Innenhof …

Ab und zu laufen da mal Architekten rum, vielleicht sehen Sie die ja, wenn sie rausschauen … denen können Sie dann Bescheid sagen. Aber im Ernst: so innerhalb des nächsten halben Jahres sollte da was geschehen, wurde uns zugesagt, die Pläne existieren schon länger.

Nächste Frage: Was halten Sie von Eliteuniversitäten?

Ein Problem ist es, dass alle in Deutschland probieren, Teile des US-Systems zu kopieren, ohne es vollständig zu kopieren. Das ist auch gut so, dass sie es nicht vollständig kopieren wollen, aber sie picken sich immer nur genau das raus, was sie haben wollen, und das ist auch der Fall bei den Eliteuniversitäten.

Arne Potthast

Man versucht Harvard zu kopieren, Berkley, Stanford und wie sie alle heißen, aber die Frage ist, ob das hier in Deutschland praktikabel ist. Ich finde es gut, dass man an allen deutschen Universitäten einen relativ hohen Standard hat, wenn man Informatik studiert, deshalb ist es für Studierende nicht unbedingt entscheidend für ihr weiteres Berufsleben, wo sie hingehen, im Moment zumindest noch. In Amerika finden Sie viele Universitäten, die einfach lausig sind. Wenn Sie dort studieren, dann bekommen Sie keinen vernünftigen Job, wenn Sie andererseits in Princeton studieren, werden sie defaultmäßig zum Staranwalt, das ist absurd.

Es gibt auch ein großes Problem mit der Finanzierung. Wenn wir Eliteuniversitäten haben, dann werden alle Studenten versuchen, da hin zu kommen, dass heißt, es wird vermutlich teuer werden, an Eliteunis zu studieren. In den USA ist es so, dass die Finanzierung des Studiums teilweise über Stipendien geregelt ist. Natürlich hat man mit den elitären Unis trotzdem das Problem, dass vorrangig die Reichen dort hinkommen, das ist sehr bedenklich. Wenn sie nicht reich sind, müssen sie viel besser als die anderen sein, dann erhalten Sie ein Stipendium. Meiner Ansicht noch sollten die Besten studieren dürfen, nicht die Reichsten.

Ich bezweifle derzeit, ob die Einführung von Eliteuniversitäten eine rundum gute Sache ist. Wenn die TU Darmstadt jetzt Eliteuni wird, wäre das natürlich sehr

gut für uns, aber insgesamt finde ich die Idee nicht gut, eine Zweiklassengesellschaft zu gründen. Ich denke, dass die deutsche Hochschullandschaft insbesondere in der Informatik auf einem sehr hohen Level ist, und da muss man sich auch nicht verstecken oder andere Systeme abkupfern. Meiner Ansicht nach sollten wir die Stärken unseres Systems weiter ausbauen, anstatt andere Systeme kopieren zu wollen.

Wie stehen Sie zu Softwarepatenten?

Das ist eine gute Frage an einen Theoretiker.

Ja, einige Kryptoalgorithmen unterliegen auch Patenten.

Ich weiß nicht, was Sie mit der Frage meinen. Bei uns in Paderborn gab es mal die Initiative, dass mehr patentiert werden soll, weil die Uni immense Gelder dadurch verliert, weil zuwenig patentiert wird. Und wenn man erst mal veröffentlich hat, kann man nicht mehr patentieren. Da liegt auch das Hauptproblem: wenn man etwas patentieren möchte, dauert das meist lange und beim Veröffentlichen muss man schnell sein, sonst hat es jemand anders schon veröffentlicht.

Aber Sie haben doch das Patent darauf.

Die Vorlaufzeit, die man aufbringen muss, um das Patent zu erhalten, ist aber leider meist sehr groß. Im Prinzip ist das Patentieren eine gute Sache, wenn man eine Idee hat, wieso sollte man sich das Geld durch die Lappen gehen lassen.

Was würden Sie tun, um den Frauenanteil zu erhöhen? Wir haben ja eine ziemlich niedrige Frauenquote, wie Sie sicherlich auch in Ihrem Studium festgestellt haben.

Ich denke, man sollte versuchen, das weitverbreitete Öffentlichkeitsklischee abzubauen, dass Informatiker weltfremde, kommunikationsunfähige Spinner sind. Gerade das mag vielleicht Frauen davor abschrecken, Informatik zu studieren. Anders kann ich mir es nicht erklären, warum die Informatik von so vielen Frauen gemieden wird.

Was ist mit der Mathematik?

In der Mathematik ist es komischerweise anders. Man sollte vermuten, dass die beiden Fächer verwandt sind, aber in Mathematik sind Frauen stark vertreten.

Vielleicht könnten Sie über Ihr Fachgebiet mit der vielen Mathematik ein bisschen Werbung machen …

Ja, das ist eine sehr gute Idee, die Mathematikerinnen … aber ich habe keine einfache Lösung, wie man mehr Frauen dazu bringt, Informatik zu studieren. In Paderborn hatten wir genau das selbe Problem, wir hatten Veranstaltungen extra für Frauen, aber das hatte keinen positiven Effekt.

Das liegt glaube ich daran, dass es ein technischer Fachbereich ist. Das ist auch ein Problem der TU selbst, die TU hat insgesamt einen niedrigen Frauenanteil.

Es ist ja auch nicht so, dass es hier frauenunfreundlich ist. Vielleicht hat man als Frau Bedenken hier zu studieren, weil man keine Kommilitoninnen hat. Ein Teufelskreis!

Bei den Theoretikern sind immer ziemlich viele Mathematiker und somit insbesondere Mathematikerinnen.

Ja, bei Prof. Buchmann ist das wohl auch so in der Kryptographie-Einführung, da ist ein überproportionaler Frauenanteil. Da könnte man daraus schließen: Mehr Theorie — mehr Frauen. Ist doch logisch.

Vielleicht bringt das der Theorie jetzt insgesamt mal einen Aufschwung …

Wenn Sie Samstagabend eine E-Mail bekommen, wie lange dauert es, bis Sie antworten?

Momentan sehr lange, bis Montagmorgen, da ich im Moment daheim keinen Netzanschluss habe. Das wird sich aber noch ändern.

Ein Informatiker ohne Internet?

Das liegt am häufigen Umziehen. Ich bin grade erst hergezogen, und Anfang Januar werde ich dann nochmal umziehen, da rentiert sich das nicht; im Moment wohne ich in Gräfenhausen.

Ich weiß allerdings nicht, ob es so sein wird, dass ich am Wochenende immer Mails beantworten will. Ich habe es auch ganz gerne, wenn ich am Wochenende was anderes mache als Informatik. Es gibt auch ein Leben außerhalb der Informatik, man kann auch mal Weggehen oder Sport machen, sonst dreht man irgendwann durch.

Noch ein paar Sätze zum Vervollständigen:

Informatik ist für mich …

… eine Wissenschaft, die Probleme algorithmisch löst.

Mathematik ist für mich …

… sehr elegant und eine notwendige Hilfswissenschaft für die Informatik.

Richtige Antwort!

Das Pilotygebäude …

… ist sehr schön, das schönste Gebäude der TU von denen die ich kenne.

Darmstadt ist …

… ganz nett. Nicht zu groß, nicht zu klein und hat eine schöne Innenstadt. Man kann hier wohnen.

Machen Sie aber nicht?

Das hat andere Gründe: Meine Freundin arbeitet woanders, deswegen müssen wir in die Mitte ziehen.

Die schönste Programmiersprache ist …

… für mich C oder C++, weil ich nicht viel anderes kann. Auf jeden Fall aber objektorientierte, imperative Programmiersprachen, keine funktionalen.

Und das als Theoretiker.

Ja, das ist dann praktische Theorie.

Haben Sie noch eine eigene Frage, die Sie gerne mal gefragt werden möchten?

Sie sollten vielleicht mehr nach der Person fragen.

Wenn das nicht zu persönlich ist. Spielen Sie ein Instrument fürs Fachbereichsorchester?

Klavier kann ich ein bisschen klimpern. Ich habe das furchtbar lange gelernt aber ich bin sehr untalentiert. Und ich kann ein bisschen Kontrabass oder Bassgitarre spielen. Das könnte ich im Fachbereichsensemble beisteuern.

Also im Moment gibt es noch kein Ensemble, aber das wäre schon mal ein Anfang.

Eigentlich ist mir Sport auch lieber als Musik. Ich spiele Volleyball und Tennis, wenn es da mal eine Fachbereichsmannschaft gäbe, würde ich da mitspielen.

Mit unseren Professoren? Können Sie sich das vorstellen? Aber am Sommerfest gibt es immer Fußball Dozenten gegen Studierende, da könnten Sie mitmachen.

Ja, das habe ich vor.

Das Gespräch führte Arne Pottharst

Mein geheimes KIF-Tagebuch

Liebes Tagebuch,

du wunderst dich nun sicher, warum du wieder aus dem Schrank gezerrt wirst, in dem du so lange geschlafen hast. Nun ja, ich bin von unserem Chefredakteur „gebeten" worden einen Artikel über die KIF zu schreiben. Ach, du weißt ja gar nicht was KIF bedeutet. Also dann erst mal eine kurze Erläuterung zum aktuellen Stand der Dinge. Die Zeit der Pickel und Schulhausaufgaben ist vorbei, wir schreiben bereits das Jahr 2005 und mittlerweile studiere ich Informatik an der TUD. Zweimal im Jahr treffen sich die Fachschaftler aus Deutschland, der Schweiz, Luxemburg und Österreich um Erfahrungen auszutauschen oder Beschlüsse über aktuelle Geschehnisse zu verfassen. Die 33,5te KIF fand dieses Mal in Lübeck statt. Eigentlich fand die KIF in Lübeck statt und es war die 33,5te. KIF bedeutet übrigens Konferenz der Informatikfachschaften.

Mittwoch, 09.11.2005: Die Hinfahrt

Heute habe ich mich mit fünf Verrückten mittags am Bahnhof getroffen. Zu allem Übel waren das meine Begleiter für die nächsten 4,5 Tage. Der erste Zug brachte uns bis nach Lüneburg. Hier bildeten sich Rauchschwaden im Zug: Die Bremsen hatten versagt. Glücklich, dass wir hier aussteigen mussten, nahmen wir die nächste Regionalbahn, die uns bis nach Lübeck an den Busbahnhof brachte. Dort wurden wir von den Organisatoren empfangen und in den richtigen Bus gesetzt, der uns dann endlich auf das Unigelände brachte. Eingedeckt mit ein wenig zu wenig Bier

hetzten wir dann in den Vorlesungssaal, in dem das Eröffnungsplenum stattfand. Hier wurden zahlreiche Arbeitskreise für die nächsten Tage vorgestellt. Gegen 0:30 Uhr waren wir dann im KIF-Café, um erst mal ein ordentliches Frühstück zu uns zu nehmen, denn Frühstück gibt es auf der KIF rund um die Uhr. Deswegen heißt es auch „ewiges Frühstück".

Donnerstag, 10.11.2005

Guten Morgen, liebes Tagebuch,

streichen wir das „guten". Es ist jetzt halb sieben und ich habe immer noch kein Auge zugemacht. Rechts und links von mir liegen zwei Personen, die sehr deutlich hören lassen, dass wenigstens sie gut schlafen. Naja, eine Stunde hab ich noch und der nächste Tag soll auch nicht sonderlich anstrengend werden. Bin mal gespannt, wie das gleich mit den Duschen klappt, nicht, dass ich da so lange warten muss. Gleich danach geht's dann ab zum Frühstück und danach zu meinem ersten Arbeitskreis Bachelor/Master. Bin ja mal gespannt, was man in einem Arbeitskreis alles so anstellt. Anschließend werd ich dann mit auf die Stadtführung in die Lübecker Innenstadt fahren. Aber jetzt nutze ich erst nochmal die Gelegenheit um ein wenig zu schlafen, im Moment ist es ein wenig stiller geworden.

Christoph, Trier

Bernhard, Graz

Jetzt ist es schon wieder 4 Uhr morgens, und eigentlich bin ich totmüde. Aber bevor ich alles wieder vergesse, möchte ich kurz noch erzählen, was heute (naja, eigentlich gestern) denn nun wirklich passiert ist. Zu allererst bin ich sehr froh, dass ich kein Mann bin, denn die haben heute Schlange stehen vor den Duschen gespielt. Da ist der geringe Frauenanteil in der Informatik doch mal was positives. Der erste Arbeitskreis hat sich mit dem kritischen Thema des Bachelor/Master-Systems befasst. Dazu bildeten wir einen Stuhlkreis, alle redeten durcheinander, aber trotzdem einigte man sich nachher auf die Themen für die kommenden drei Tage. Dazu gehörten neben dem Master als Regelabschluss auch noch die Auslandsaufenthalte und die Unterschiede zwischen Uni und FH. Zum Mittag hin gab es dann eine Pause, in der wir uns von der Qualität des Mensaessens überzeugen durften. Wenn man auf Bio und Vegetarierzeugs steht, dann kann man sich da den Bauch vollschlagen. In der Innenstadt habe ich den Unterschied zwischen Klassizismus, Barock, Renaissance und Gotik gelernt und dass alles in einer Straße. Vorgetragen wurde es von einer älteren Dame, die sehr nett war, aber dieselbe monotone Erzählweise besaß wie all die anderen Stadtführer auch. Nach zwei Stunden Lübeck City sind wir endlich am Zielort angekommen: Dem Lübecker Marzipanhaus Niederegger. Hier gibt es ganze Regale mit Marzipan in den unterschiedlichsten Formen und Farben. Davon werde ich jetzt noch ein wenig träumen.

Gute Nacht, liebes Tagebuch.

Freitag, 11.11.2005

Juchhu, Karneval würde man wohl in vielen Städten rufen, doch in Lübeck veranstaltet man lieber eine Party mit dem Namen „KIF statt Karneval". Dafür werd ich mich gleich noch umziehen. Aber ich wollte dir erst noch kurz mitteilen, was ich heute alles erlebt hab. Nach dem Aufstehen hab ich in aller Ruhe geduscht und bin dann frühstücken gegangen, bevor ich im Arbeitskreis „Wiki" war. Ich fand es sehr spannend zu erfahren, welche einfache

Möglichkeit ein Wiki bietet, gleichzeitig als Kommunikations- und Informationsplattform zu dienen. Die Idee, als Leser und Autor einen Artikel zu lesen und ihn um sein eigenes Wissen zu ergänzen, ist so simpel wie einleuchtend. Jetzt muss ich mich aber beeilen, die anderen wollen los.
Also bis morgen.

Abschlussplenum der KIF. Ich wurde von vielen Leuten gewarnt, dass es sehr lange dauern kann und wollte dir nur eben von dem Arbeitskreis rund um Fachschaftszeitungen erzählen. Geleitet wurde dieser Kreis von unserem eigenen Chefredakteur. Dort habe ich sehr viel über die verschiedenen Möglichkeiten erfahren, wie man eine solche Zeitung aufbaut und sie

Samstag, 12.11.2005

(Aufgrund überhöhtem Alkoholkonsum ist dieser Tagebucheintrag nicht mehr zu entziffern gewesen und kann von der Redaktion nicht abgedruckt werden. Wir entschuldigen uns bei all unseren treuen Lesern und probieren diese Seiten bei der nächsten Feier mit stärkerem Alkoholpegel zu entziffern)

Hallo mein Tagebuch,

jetzt ist es gleich halb 7 abends und in einer halben Stunde beginnt das unter die Studenten bringt. Ich schreib dir nach dem Plenum noch einmal, wie es war. Bis gleich.

… 9 Stunden später …

Puh, da bin ich wieder. Hat doch sehr lange gedauert. Also am Anfang ging es noch ziemlich schnell. Da wurden alle Arbeitskreise die es gab vorgestellt und es wurde kurz erklärt, was sie diskutiert haben und zu welchem Ergebnis diese Kleingruppen gekommen sind.

In drei dieser Kleingruppen wurde dann

auch noch eine so genannte Resolution beschlossen. Ich konnte mir darunter auch erst nichts vorstellen, aber habe dann unseren Weisen Alten befragt und er hat mir gesagt, dass es eine Resolution eine Bitte an die nächste KIF oder eine Forderung für die Öffentlichkeit im Name der KIFfels ist. Interessant war es mitzuerleben wie man eine Abstimmung über ein Meinungsbild machen kann, obwohl schon eine Abstimmung vorausgegangen ist?! Da geht die eigentliche Frage dann schon mal unter.

Aber wenigstens gab es genug Pausen, in denen man die Biervorräte wieder auffüllen konnte.

Jetzt lieg ich gerade auf meiner Luftmatratze und ärger mich darüber, dass ich nicht vor der KIF ihre Funktionalität überprüft habe. Naja, ich hätte ja heute eh nicht schlafen können, weil hier im Halb-Stunden-Takt Leute rein laufen, das Licht anmachen und ihre Sachen packen. Auf jeden Fall versuch ich jetzt noch eine Stunde zu schlafen, weil wir morgen Mittag ja schon zurückfahren.

Sonntag, 13.11.2005

Liebes Tagebuch,

jetzt sitze ich in der Bahn zurück nach Darmstadt und ich bin totmüde. Insgesamt zehn Stunden Schlaf in den letzten fünf Nächten waren dann doch etwas zu wenig. Deswegen nur noch kurz ein kleiner Bericht von heute morgen. Nach dem Aufstehen gab es noch ein ausgiebiges Frühstück und danach folgte eine große Verabschiedungsrunde und jetzt freu ich mich sehr auf mein Bett. Dich, liebes Tagebuch, werde ich wohl wieder im Schrank verstauen und zur nächsten KIF im Mai in Bremen wieder mitnehmen.

Alexander Juling & Jacqueline Vogel

Resolutionen der 33,5ten KIF

(ap) Dieses Mal waren wir wieder besonders fleißig auf der KIF und haben es geschafft, vier Resolutionen zu verabschieden. Im folgenden sind sie im Wortlaut abgedruckt. Alle wurden in Lübeck am 13. November 2005 nach jeweils endloser Diskussion verabschiedet.

Resolution Regelabschluss

Die 33,5te Konferenz der Informatik-Fachschaften fordert den Master als Regelstudienabschluss in Bachelor-/Masterstudiengängen.

Resolution CHE-Rankings

Die 33,5 Konferenz der Informatik-Fachschaften stellt fest:

Es gab und gibt an verschiedenen Hochschulen Aufforderungen, in den Fragebögen der CHE-Umfrage Kritik zu unterlassen und die Hochschule möglichst gut darzustellen.

Studierende, ProfessorInnen und Hochschulleitungen befürchten, dass von den Ergebnissen der Rankings Hochschulfinanzen und das Ansehen des Abschlusses an der Hochschule abhängen.

Wir befürchten daher, dass die Teilnehmenden systembedingt einen Anreiz haben, diese Umfrage zu manipulieren. Schon aus diesem strukturellen Grund sind Umfragen dieser Art nicht dazu geeignet, als Argumentationsgrundlage zu dienen.

Resolution Grundrechte

Die Beschränkung der Grundrechte in Deutschland wird seit Jahren unter zunehmend fadenscheinigeren Gründen („internationaler Terrorismus“) staatlicherseits vorangetrieben. Die derzeitigen Koalitionsverhandlungen zeigen auf, dass eine zukünftige Bundesregierung die Abschaffung wesentlicher Datenschutzrechte und den Ausbau ungerichteter Überwachungsmaß-

nahmen weiter voranzutreiben plant.

Die 33,5te Konferenz der Informatikfachschaften fordert die Politikerinnen und Politiker aller Parteien auf, sich auf ihre Verpflichtung zur Wiederherstellung und Bewahrung der Grundrechte zu besinnen und die inneren Feinde der Demokratie in den großen Parteien daran zu hindern, Deutschland noch weiter in einen Überwachungsstaat zu verwandeln.

Zielquoten

Die 33,5. Konferenz der Informatik-Fachschaften in Lübeck sieht das Niveau des Informatikbachelors gefährdet:

In Deutschland gibt es bildungspolitische Bestrebungen, dass 80% der StudienanfängerInnen den Bachelorabschluss erreichen sollen. Diese feste Vorgabe widerspricht jeglicher Erfahrung in den Informatikstudiengängen. In Diplominformatik-Studiengängen an deutschen Universitäten liegt die Zahl der AbbrecherInnen im Mittel bei 38% und bei 19% FachrichtungswechlerInnen. Mit 8% Zuwanderung aus anderen Studienrichtungen ergibt sich eine Schwundquote von insgesamt 49%.

Diese Größenordnung an StudienabbrecherInnen kann auch für das Vordiplom angenommen werden, da es an Universitäten kaum StudienabbrecherInnen nach erfolgreichem Vordiplom gibt. Mit der Einführung neuer Bachlorstudiengänge verschiebt sich zudem die Messmarke eines Teilziels im Studium vom 4. Semester (Vordiplom) auf das 6. Semester (Bachelor). Es ist nicht zu erwarten, dass sich dadurch die Anzahl der StudienabbrecherInnen verringern würde. Wir befürchten, dass die politisch gewollte Zielzahl für AbsolventInnen eines Bachelorstudiums in der Praxis vorrangig durch Niveauabsenkung des Bachelorstudiums gegenüber den bisherigen Studiengängen erkauft wird.

Diese Absenkung der Anforderung kommt für uns nicht in Frage.

Die 33,5te Konferenz der Informatik-Fachschaften fordert die Politik auf, die Forderung nach Zielquoten für Bachelorstudiengänge zurück zu nehmen.

Grundsätzlich befürwortet die 33,5te Konferenz der Informatik-Fachschaften selbstverständlich, dass diejenigen, die ein Informatikstudium aufnehmen, dieses auch erfolgreich abschließen können.

Dies kann beispielsweise durch bessere Information und Aufklärung der SchülerInnen über ein Hochschulstudium erfolgen, indem bereits im „Informatik“-unterricht die Unterschiede der Informatik und „Informationsverarbeitung“ dargestellt werden. Wichtig ist vor allem die Aufklärung über Inhalte und Anforderungen eines Informatikstudiums an den verschiedenen Hochschultypen.

„Wir sind doch gebildete Menschen!“

Über den Wandel von Begriffen im gesellschaftlichen Kontext, Kompetenz als Bildung, den Blick über den Tellerand und Fachidioten.

Wir nennen uns gerne gebildet. Und wir bilden uns immer weiter. Schließlich verbringen wir die Woche damit, Wissen in Form von Vorlesungen und Übungen aufzusaugen, Seminarvorträge zu halten oder komplizierte Probleme in allerlei Praktika zu lösen. Ist es das wirklich? Ist Wissen gleich Bildung? Schon bevor ich letztes Jahr mein Nebenfach (Pädagogik) begann und in der Onlinevorlesung "Einführung in die Informationspädagogik" eine Aufgabe zu diesem Thema bearbeiten musste, war mir klar: Einfaches Reproduzieren von Wissen kann es wohl nicht sein. Da muss schon mehr dazugehören. Ich erinnere mich an die Mathematikvorlesungen, die ich in grauer Vorzeit einmal gehört habe: An diese Vorlesungen kann ich mich inhaltlich kaum noch erinnern. Aber ich weiß genau, dass sie mir geholfen haben, mein mathematisches Denken zu schulen und die Probleme, vor denen ich heutzutage im Studium oder beim Arbeiten stehe, zu lösen. Ist es also dann Bildung, wenn der primäre Sinn nicht in der Wissensvermittlung, sondern in der Schulung des Denkens, im Erwerb einer Problemlösungskompetenz liegt?

stock.xchng

Zwei grundlegende Dinge habe ich im Verlauf meiner Pädagogik-Seminare gelernt:

1. Begriffe wie Bildung verändern im Laufe der Zeit ihre Bedeutung.

2. Wenn mehrere Leute von "Bildung" reden, gibt es immer mehr als eine Vorstellung davon, was mit diesem Wort eigentlich gemeint ist.

Was die hiesigen Pädagogen (und ich jetzt auch) unter Bildung verstehen, beinhaltet mehr als das reine Lösen von Problemen. Was wir in der Informatik nicht lernen ist, sich zu fragen, ob ein Problem überhaupt gelöst werden sollte, was wir damit bewirken, wenn wir ein Problem lösen, ein Programm schreiben oder eine Ausarbeitung zu einem bestimmten Thema veröffentlichen. Vor kurzem ist mir beispielsweise das Thema "anonyme Peer-to-Peer-Netze" untergekommen. Es gibt sicher eine Menge interessanter technischer Probleme die man in diesem Be-

reich lösen könnte, aber ich frage mich, ob man diese wissenschaftliche Neugier nicht besser hinten anstellen sollte, wenn man bedenkt, dass die Leute, die sich am meisten über so etwas freuen, vermutlich die Vertreiber von Videos sind auf denen kleine Kinder Sex haben.

Bildung hat damit zu tun, über Konsequenzen nachzudenken, die durch das eigene Handeln entstehen; dazu in der Lage zu sein, selbst über sein Leben zu bestimmen und dabei die Gesellschaft nicht aus dem Auge zu verlieren.

Leider ist der Bildungsbegriff gerade dabei, seine Bedeutung zu verändern, hin zu der reinen Problemlösungskompetenz. Das, was wir brauchen, um im Leben über die Runden zu kommen, eine Arbeit zu finden und erfolgreich zu sein, wird als Bildung bezeichnet. "Sollte ich das Problem lösen?" ist nicht mehr wichtig -- nur noch "Wie löse ich es?".

Das sieht man unter anderem daran, dass der Bachelor-Master-Studiengang kein Nebenfach mehr hat. Es wird nur noch ein Anwendungsfach geben, das aber, im Gegensatz zum Nebenfach, eine Beziehung zur Informatik haben muss. Das Nebenfach diente dem Blick über den Tellerrand. Es war explizit erwünscht, dass sich Studenten Nebenfächer wählten, die nichts mit der Informatik zu tun haben.

Der Blick in andere Fachbereiche ist in Zukunft mit einem erheblichen persönlichen Aufwand verbunden. Man kann zwar eine Geschichtsvorlesung besuchen, aber die Credits kann man nicht in das eigene Studium einbringen. Wenn man sein Studium dadurch nicht unnötig verlängern will, muss man zusätzlich zu den gut gefüllten 24 SWS, die man sowieso hat, noch mehr Zeit investieren. Ich kann mir kaum jemanden vorstellen, der dazu in der Lage wäre.

Also produzieren wir demnächst doch nur noch Fachidioten; und mit *wir* meine ich nicht uns hier am Fachbereich Informatik an der TU Darmstadt, sondern *un*s hier in Deutschland. Denn das Phänomen, dass das Studium effizient, und ökonomisch nützlich sein muss, und Studenten nicht mehr die Freiheit haben, etwas zu tun, dessen Nutzen nicht in irgendeiner Form messbar oder zumindest klar erkennbar ist, zieht weitere Kreise: Deutschlandweit, wenn nicht sogar europa- oder weltweit.

Nils Knappmeier

Was ist der Master wert?

(ap) Der Master ist so in etwa gleichzusetzen mit dem Diplom, sagt zumindest unser Präsident. Wenn man sich das Diplom der FH anschaut, so bekommt man dort einen Bachelor dafür, der mindestens ebenbürtig ist. Dieser FH-Bachelor ist mit Auflagen dem Uni-Bachelor äquivalent, der auch nicht viel mehr als das Vordiplom ist, was auch schon fast mit einem BA-Abschluss aufzuwiegen ist. Dieser BA-Abschluss, den man durchaus nach einem Fachabitur machen kann, beinhaltet eine berufsbegleitende Ausbildung, die wiederum aus einem Realschulabschluss ein Abitur macht. Durch die Verkürzung auf zwölf Jahre wird das Abitur dem Fachabitur stark angenähert. Und in manchen Bundesländern ist der Realschulabschluss nicht weit vom Hauptschulabschluss entfernt. Wenn man sich diese Implikationskette anschaut, ist es nicht weit her mit dem Master ...

Der Spieleabend der Fachschaft Informatik

Wir veranstalten offene Spieleabende mit Brett- und Kartenspielen aller Art für interessierte Informatiker und Nichtinformatiker.

Derzeit treffen wir uns in der Regel jeden Donnerstag ab 19 Uhr im Piloty in Raum E102. Die aktuellen Termine stehen auf der Website und im Forum der Fachschaft Informatik.

Neue Mitspieler sind jederzeit willkommen. *Schau' vorbei!*

D120.de/gnom/

Anonym surfen im Internetcafé?

Überwachung des Internets

Durch die schnelle Entwicklung des Internets zu einem Massenmedium bekommt plötzlich jede Person – zumindest in der entwickelten Welt – die Möglichkeit, beliebige Inhalte anonym zu verbreiten. Jedes andere Medium wird in gewissem Maße gesellschaftlich kontrolliert, nur das Internet hat sich bisher weitgehend einer Kontrolle entzogen. Dies wird kein Dauerzustand bleiben.

Unter dem Deckmantel der „Terrorismusbekämpfung" werden seit Jahren immer weitergehende Überwachungsmaßnahmen gefordert und umgesetzt. Doch wie wirkungsvoll sind diese Maßnahmen? Sind sie wirklich dazu geeignet, kriminelle Handlungen im Internet zu unterbinden, oder ist das alles nur wirkungsloser Aktionismus um (vermeintliche) Tatenkraft zu demonstrieren?

Im Dezember 2005 hat das EU-Parlament eine Richtlinie beschlossen, nach der zukünftig sämtliche Telekommunikationsanbieter zu einer verdachtsunabhängigen Vorratsdatenspeicherung verpflichtet werden. In Deutschland sollen diese Daten zukünftig sechs Monate lang gespeichert werden. Mit diesem Beschluss hat das EU-Parlament die Unschuldsvermutung praktisch abgeschafft, da künftig jede Person, unabhängig von einem konkreten Verdacht, in das ohnehin schon immer enger werdende Überwachungsnetz von staatlichen und in zunehmendem Maße auch privaten Organisationen gerät.

Verbindungsdaten sind unter anderem die Telefonnummer (worüber sich eine genaue Adresse ermitteln lässt), Benutzerkennung, IP-Adresse, Server- und Dateiname bei Nutzung des Hypertext-Transfer-Protokolls, Datum, Uhrzeit, die Dauer der Verbindung und bei Mobilfunkverbindungen zusätzlich die Funkzellen (um den Standort ermitteln zu können). Die für die Provider entstehenden Kosten und der mit der Richtlinie verbundene Aufwand ist nicht zu un-

terschätzen: Man schätzt, dass alleine am deutschen Internet-Knoten DeCIX Verbindungsdaten von ungefähr 415 Terabyte gespeichert werden müssen – pro Tag! In sechs Monate sind das circa 750 Exabyte alleine am DeCIX. Die Massenspeicherindustrie wird den Überwachungsplänen wahrscheinlich nicht sonderlich abgeneigt sein …

Durch die immer stärkere Überwachung des Internets soll es für die Behörden einfacher werden, kriminelle Netz-Aktivitäten zu verfolgen. An sich ist das ja in Ordnung. Allerdings scheinen die meisten Politiker sich nicht im klaren darüber zu sein, wie wirkungslos diese Maßnahmen gerade gegenüber denjenigen Gesellschaftsfeinden (Terroristen) sind, wegen denen sie eingeführt werden sollen. Wer sie umgehen will, kann dies relativ einfach tun. Und erfahrungsgemäß wecken vorhandene Daten oft das Interesse anderer Interessensgruppen, die sie auch gerne nutzen würden.

Vielleicht haben einige Politiker auch schon Gedanken für eine weitere Verwendung der Daten im Hinterkopf. In einem Entwurf zur Umsetzung der EU-Richtlinie findet sich in der Bundesdrucksache 16/545 vom 07.02.06 in Abschnitt II, Punkt 2a folgender Satz: „… die Beschränkung der Datenabfrage zu Zwecken der Strafverfolgung auf die Ermittlung, Aufdeckung und Verfolgung erheblicher oder mittels Telekommunikation begangener Straftaten;“. Der letzte Teil dieses Satzes lässt anklingen, dass außer den Strafverfolgungsbehörden künftig auch andere „Institutionen“ (etwa **die** Musik- und Filmindustrie) auf die gespeicherten Daten Zugriff bekommen sollen. Die Einschränkung „mittels Telekommunikation begangener Straftaten“ lässt sich sehr weit interpretieren.

Betrachten wir uns nun grob, welche Möglichkeiten es gibt, um das Internet auch in Zukunft anonym nutzen zu können.

Technische Grundlagen der anonymen Kommunikation

Wie bei der Benutzung anderer elektronischer Medien hinterlässt auch ein „normaler“ Internetnutzer „Datenspuren“, über die man einen Kommunikationsvorgang eindeutig einem Anschluss und meist auch einer Person zuordnen kann. Im Gegensatz zu geschlossenen Systemen wie dem Telekommunikationsnetz, in dessen Infrastruktur die Benutzer nicht eingreifen können, ist das Internet ein offenes Medium, das es versierten Benutzern erlaubt, Datenspuren zu verwischen oder gar nicht erst entstehen zu lassen.

stock.xchng

stock.xchng

Bei der Vorratsdatenspeicherung fallen gigantische Datenmengen an

Bei der Ermittlung von Urhebern über Server-Logs ist die IP-Adresse das zentrale Datum. Ohne sie ist eine Internet-Verbindung nicht möglich. Doch wie kann man das Internet benutzen, ohne über die IP-Adresse ermittelbar zu sein? Man kann sich bei einem Provider einwählen, der keine Verbindungsdaten speichert. Solche findet man vor allem im Ausland, die man über das Telefonnetz aber auch hierzulande nutzen kann. Oder man verwendet anonymisierende „Proxy-Server“. Ein Proxy-Server führt die Kommunikation stellvertretend für einen anderen

Rechner aus. Ein Rechner kann eine Anfrage über einen Proxy laufen lassen, der dann die Anfrage an den eigentlichen Zielrechner weiterleitet. Als IP-Adresse kann der Zielrechner nur die des Proxys speichern. Wenn dieser aber die Adresse des abfragenden Rechners nicht speichert, ist eine Rückverfolgung zu dem Ursprungsrechner nicht mehr möglich. Vor allem im Ausland gibt es etliche offene Proxy-Server, die von jedem genutzt werden können. Auch in Deutschland gibt es anonymisierende Proxy-Netze, die man legal nutzen kann (zum Beispiel JAP http://anon.inf.tu-dresden.de/ oder TOR http://tor.eff.org/).

Eine Sonderform von „unfreiwilligen Proxys" sind offene WLAN-Netze. An vielen Orten findet man heute ungeschützte Funknetze, die man anonym nutzen kann. Wer eine Kommunikation über ein offenes WLAN-Netz oder ein Anonymisierungsnetzwerk führt, ist praktisch nicht zu ermitteln. Jedenfalls, sofern der Inhalt des Datenverkehrs keine Rückschlüsse auf ihn zulässt. Um dies sicherzustellen, kann man sich mit Mitteln der Kryptographie und Steganographie schützen.

Vom Verschlüsseln ...

Mit kryptographischen Methoden können Nachrichten verschlüsselt werden, so dass sie nur von Personen mit dem richtigen „Schlüssel" gelesen werden können. Der Begriff Verschlüsselung ist übrigens nicht mit Kodierung zu verwechseln. Bei einer Kodierung wird jedes Zeichen auf ein anderes Zeichen abgebildet. Es genügt also, das Verfahren zu kennen, mit welchem die Nachricht kodiert wurde. Eine bekannte Kodierungsvorschrift ist beispielsweise ROT13, die auf Caesar zurückgeht. Bei ihr wird jeder Buchstabe um 13 Stellen in eine bestimmte Richtung verschoben. Ein „a" würde so zu einem „n". Der Nachteil ist offensichtlich: Hat man einmal den Code geknackt (was mit statistischen Methoden nicht schwierig ist), kann man sämtliche damit kodierten Texte knacken.

Bei der heute üblichen schlüsselbasierten Kryptographie reicht das Wissen um die Verschlüsselung *nicht* aus. Es wird zusätzlich ein „digitaler Schlüssel" benötigt. Die Public-Key-Kryptographie basiert auf der Verwendung von zwei verschiedenen *asymmetrischen Schlüsseln*, einem *privaten* und *öffentlichen* Schlüssel. Der private Schlüssel wird zur Entschlüsselung von Nachrichten verwendet, die mit dem öffentlichen Schlüssel verschlüsselt wurden. Während der öffentliche Schlüssel für jeden frei verfügbar sein kann, darf der private Schlüssel nie in falsche Hände geraten, da mit ihm Dritte mitlesen können. Das Verfahren gilt heute als eines der sichersten und praktikabelsten und ist in Form von Software wie GnuPG (http://www.gnupg.org/) weit verbreitet.

Es gibt sogar eine Verschlüsselungsmethode, die nachweislich sicher ist und außer durch dem Durchprobieren aller möglichen Schlüssel nicht geknackt werden kann: das *One-Time-Pad*. Hierbei wird eine Nachricht mit einem Schlüssel *der gleichen* Länge verschlüsselt. Jedes Zeichen der Nachricht wird auf genau ein Zeichen des Schlüssels abgebildet. Wenn der Schlüsseltext *wirklich* zufällig gewählt wurde, gibt es kein Muster, nachdem man den Text entschlüsseln könnte.

... und Verstecken

Ein mit dem korrekt angewandten Public-Key-Verfahren verschlüsselter Text kann zwar über alle unsicheren Kanäle gesendet werden, aber eines kann auch der verschlüsselte Text nicht verbergen: dass eine Kommunikation stattgefunden hat. Selbst wenn Behörden mit einem verschlüsselten Text nichts anfangen können, kann es eine sehr interessante Information sein, dass eine bestimmte Person mit einer anderen kommuniziert hat. Und genau diese Verbindungsdaten werden in Zukunft für längere Zeit gespeichert. Mit Hilfe der *Steganographie* (übersetzt etwa „verstecktes Schreiben") kann man verbergen, dass überhaupt eine Kommunikation stattgefunden hat.

Mit steganographischen Methoden kann

man Nachrichten in unverdächtige Trägernachrichten einbetten. Es findet zwar eine Kommunikation statt, aber diese muss nicht direkt zwischen zwei Personen stattfinden und man kann ihr nicht ansehen, dass außer den „offensichtlichen Daten“ noch weitere übertragen worden sind.

Das Prinzip von modernen Steganographieverfahren ist einfach: Das menschliche Auge merkt es nicht, wenn sich in einem digitalen Bild ein Farbwert minimal verändert. Ändert man den Wert eines Bildpunktes in der blauen Farbebene von 154 auf 155, nimmt das Auge einen Farbunterschied von 1/256 nicht wahr. Ein Computerprogramm aber kann jeden Bildpunkt nach einem bekannten Einbettungsmuster durchsuchen und so eine eingebettete Nachricht extrahieren. Abhängig von der Größe des Bildes lassen sich so auch größeren Datenmengen unentdeckt übermitteln.

Zum Beispiel wie folgt: Über ein Anonymisierungsnetzwerk lädt eine Person unter einem Pseudonym unverdächtige (Urlaubs-) Bilder hoch. Eine andere Person schaut immer mal wieder dort vorbei und untersucht neue Bilder auf ein vereinbartes Einbettungsmuster. Beide könnten sogar komplett überwacht werden – nichts deutet auf eine Kommunikation hin. Die eingebetteten Nachrichten sind natürlich auch noch verschlüsselt.

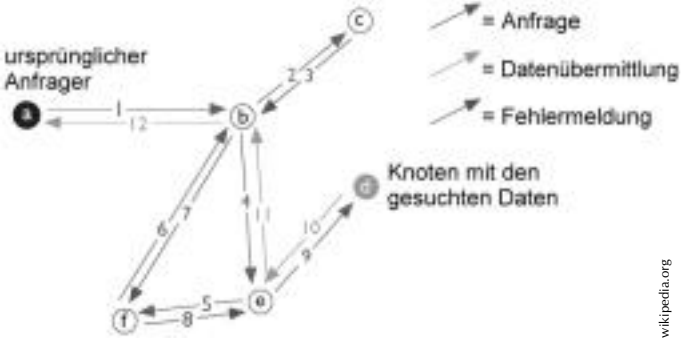
Dieses Prinzip kann man auf viele andere Medientypen übertragen. Bei einer Audiodatei kann man minimale Veränderungen in der Tonhöhe vornehmen, die für das menschliche Gehör nicht wahrnehmbar sind. Freie Steganographieprogramme sind unter anderem steghide und outguess.

Zensurresistente Netze

Noch weiter gehen Netze wie Freenet (http://www.freenetproject.org/). Dies ist ein seit 1999 im Entwicklungsstadium befindliches Netz, das eine anonyme und zensurresistente Kommunikation über das Internet ermöglicht. Es basiert auf Dezentralität, Verschlüsselung, Redundanz und dynamischem Routing

Im Freenet werden Inhalte über ihren *Hash-Wert* identifiziert. Dies ist eine Art „elektronischer Fingerabdruck“. Für jede Datei kann ein eindeutiger Hash-Wert berechnet werden. Wirklich eindeutig ist kein Verfahren, aber die so genannte „Kollisionswahrscheinlichkeit“, dass zwei verschiedene Dateien den gleichen Hash-Wert haben, ist extrem gering und wird vernachlässigt. Um an eine bestimmte Datei zu kommen, muss ihr Hash-Wert bekannt sein. Die Freenet-Software verfügt im Speicher über eine Liste mit anderen Freenet-Rechnern und eine ungefähre Angabe, für welche Hash-Werte dort die dazugehörigen Dateien vorhanden sind.

Sobald ein Nutzer eine bestimmte Datei anfordert, schickt die Freenet-Software eine Anfrage an einen Rechner, der diese Datei



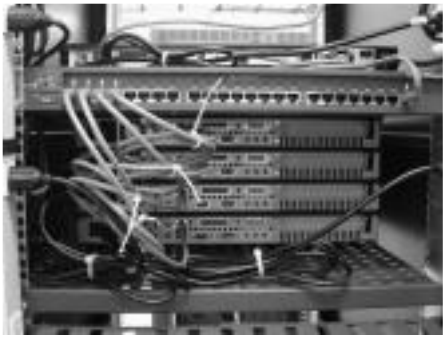
wikipedia.org

Typischer Ablauf einer Anfrage in Freenet

am wahrscheinlichsten hat oder am wahrscheinlichsten weiß, wo es sie gibt. Wenn dieser die Datei nicht hat, fragt er wiederum den nächsten Rechner. Und so weiter. Wenn der Inhalt sich irgendwo im Netz befindet, kommt die Anfrage irgendwann an einen Rechner, welcher über die Datei verfügt. Dieser verschickt nun die Datei. Allerdings sendet er die Daten nicht direkt an den Ur-

sprungsrechner — den kennt er nicht —, sondern auf „dem gleichen“ Weg zurück, über den die Anfrage gekommen ist. Dadurch weiß bis auf den anfragenden Rechner kein System in der Kette, ob es die Daten an den Ursprungsrechner schickt oder die Daten nur weitergeleitet werden.

Jeder an der Kommunikationskette beteiligte Rechner speichert Teile der übertragenen Datei, um sie selbst wieder verteilen zu können. Häufig abgefragte Dateien verbreiten sich dadurch sehr schnell. Dabei läuft die gesamte Kommunikation natürlich verschlüsselt ab. Auch die Inhalte, die ein Rechner bereitstellt, sind verschlüsselt. Selbst der Besitzer eines am Freenet angeschlossenen Rechners weiß zu keinem Zeitpunkt, welche Daten auf seinem System gespeichert und verteilt werden. Dies soll



stock.xchng

Die Rechtsgrundlage hängt oft vom Standort des Internetservers ab

verhindern, dass der Besitzer für die Verbreitung von illegalen Inhalten belangt werden kann.

Der größte Nachteil von Freenet ist die bislang fehlende Suchmöglichkeit. Man kann noch nicht direkt nach bestimmten Dateien suchen, sondern braucht erst ihren Hash-Wert. Doch bis zur ersten fertigen Version soll es eine Suchfunktion geben.

Wozu dann Vorratsdatenspeicherung?

Die meisten Überwachungs- und Zensurmaßnahmen scheitern an der Offenheit und Grenzenlosigkeit des Internets. Doch auch, wenn man „das Recht“ global durchsetzen könnte — welches wäre es dann? Schon heute kommt es oft zu Streit bei der Kollision völlig unterschiedlicher Rechtssysteme und -auffassungen. Ein Beispiel ist das Leugnen des Holocausts, das in Deutschland verboten, aber etwa in den Vereinigten Staaten erlaubt ist. Dort gibt es etliche Server, die solche Inhalte legal verbreiten – und natürlich auch hierzulande abgerufen werden können. Dadurch kommt es zu einer Abwärtsspirale, bei der sich Personen einen Standort für ihre Inhalte aussuchen können, deren Rechtssystem ihnen am besten passt. Das Recht wird verhandelbar. Zumindest für die entwickelten Teile der Welt. In den unterentwickelten Teilen gibt es erst gar kein Recht. Und damit auch weltweit nicht.

Trotzdem ist es kein hoffnungsloser Kampf. Auch wenn sich die „großen Fische“ nicht mehr oder nur noch durch eigene Pannen werden fangen lassen, kann dennoch einiges gegen die illegale Nutzung getan werden.

- Am wichtigsten ist die Zusammenarbeit vieler vor allem entwickelter Länder bei der Strafverfolgung. Nur wenn sich diese auf ein gemeinsames Vorgehen gegen Straftaten einigen, wird es gelingen, große Teile des Internets halbwegs unter Kontrolle zu bringen. Dabei werden sie sich aber zunächst darüber einigen müssen, welche Inhalte überall als verboten gelten sollen.
- Die freiwillige Selbstkontrolle, überhaupt eine Ur-Idee offener Netze, sollte gestärkt werden. Jedem Internetnutzer sollten zentrale Meldestellen bekannt sein, über die er - auch anonym - Seiten mit illegalem Inhalt melden kann. Vereinzelt gibt es solche Meldestellen auch schon, wenn auch meist nur für bestimmte Inhalte (beispielsweise das „Netz gegen Kinderporno“ von Heise).
- Es sollten mehr Personen in staatlichen Stellen mit Sachkenntnis und der entsprechenden Ausstattung als Internet-Fahnder

eingesetzt werden. Sie sollten auch mehr Rechte haben und zum Beispiel lügen dürfen. Derzeit muss ein Beamter etwa im Chat auf Nachfrage wahrheitsgemäß antworten, dass er BKA-Beamter sei.

- Trotz aller Einschränkungen ist eine Vorratsdatenspeicherung von Verbindungsdaten nicht von vornherein zu verteufeln. Zwar lässt sich diese verhältnismäßig leicht umgehen, doch gerade „Gelegenheitsgauner“ konnte man bisher oft über die Verbindungsdaten ermitteln.

Nicht, um missverstanden zu werden: Die Vorratsdatenspeicherung gedankenlos als Mittel zur Terrorismusbekämpfung durchsetzen zu wollen, wie es derzeit geschieht, ist irrsinnig. Denn wie gezeigt nützen sie nichts gegen Personen, die sie wirklich umgehen wollen. Aber die Verbindungsdaten sind bereits heute für die Ermittlungsbehörden von enormer Bedeutung. Ohne diese Daten kommt man an Urheber von illegalen Inhalten oder auch Betrüger auf Auktionsplattformen meist nicht ran.

Das Recht wird verhandelbar

Auch wenn es libertären (nicht liberalen!) Menschen missfällt: Nur weil das Internet ein noch immer vergleichsweise junges Medium ist, ist es kein rechtsfreier Raum. Es hat schon immer Mittel und Wege gegeben, Gesetze zu umgehen. Doch nur, weil dies möglich ist, darf man sie nicht gleich komplett für nutzlos erklären. Wenn sichergestellt werden könnte, dass die gespeicherten Daten nicht für andere Zwecke missbraucht würden und jede weitergehende Verwendung ausgeschlossen werden könnte, wäre es bei kürzerer Speicherdauer eine Maßnahme, über die sich diskutieren ließe.

Eine einfache Lösung gibt es nicht. Es ist wie so oft im Leben auch hier eine Frage des Maßes. Gerade der Datenschutz gerät in Zeiten der Informationsgesellschaft unter immer höheren (Rechtfertigungs-) Druck. Über das Verschwinden des Privaten in einer immer gläserner werdenden Gesellschaft wird es im nächsten Inforz gehen.

Andreas Marc Klingler

Ein Tag in der Uni

Was ist eigentlich Informatik? Was bedeutet, es Informatik zu studieren? Ist Informatik etwas für mich?

Diese Fragen sollte man sich stellen, bevor man ein Informatikstudium beginnt. Aber eine vernünftige Antwort wird man wohl selten erhalten. Zumindest nicht, wenn man noch nie eine Uni gesehen hat und noch nie in einer Informatik-Vorlesung gesessen hat. Um gegen dieses Unwissen etwas zu unternehmen, haben wir ganz kurzfristig das Programm „Universitäts-Erfahrung“ (UE oder Ü) ins Leben gerufen.

Die Idee ist relativ einfach: Interessierte Schüler werden mit willigen Studenten paarweise zusammengebracht und begleiten diese durch den ganz normalen Uni-Alltag. Das ganze fand in der ersten Januarwoche statt, in der die Schüler noch Ferien hatten. Wie das ganze bei den Schülern angekommen ist, könnt ihr im folgenden Interview nachlesen.

Wenn ihr selber Lust habt, einen Schüler in dieser Art und Weise zu betreuen meldet euch einfach unter ue@d120.de. Ihr seid dann qualifiziert, wenn ihr einen interessanten Stundenplan habt. Es ist sicher nicht sehr spannend für Schüler, dabeizusitzen, während ihr Seminarausarbeitungen schreibt. Auch wenn das zum Uni-Alltag natürlich dazugehört. Wir werden diese Aktion bestimmt noch einmal wiederholen.

An dieser Stelle möchte ich noch einmal allen Beteiligten danken. Das Engagement war wirklich überwältigend. Immerhin kam die Idee erst Mitte Dezember auf. Ich finde es toll, dass man solche Aktionen mit Euch auch noch so kurzfristig planen kann.

Nils Knappmeier

Wer bist Du und wo kommst Du her?

Ich heiße Christopher und gehe in die 12. Klasse in Kronberg/Taunus.

Interessierst Du Dich für Informatik oder für Uni allgemein?

Beides. Ich war noch nie an einer Uni und wollte das mal kennenlernen an so einem Tag. Ich interessiere mich auch für Informatik. Ich mache Informatik-Unterricht bei uns an der Schule, fakultativ, und ich überlege mir, ob ich Informatik studieren will.

Hat dieser Tag heute Deine Überlegungen positiv beeinflusst oder hat es Dich eher abgeschreckt?

Abgeschreckt ganz sicher nicht, aber ich bin mir immer noch nicht ganz sicher, ob ich Informatik studieren werde.
Ich werde mir noch anderes anschauen, das war ja der erste Tag, den ich an der Uni war.

Christopher

Welche Fächer überlegst Du Dir noch? Eventuell verwandte Fächer?

Ja, Physik beispielsweise oder Elektrotechnik, also schon was technisches. Was mich auch interessiert ist Nachrichtentechnik, sowas in der Richtung. Aber im Moment ist es noch nicht ganz klar, was ich später machen werde.

Welche Veranstaltungen hast Du besucht?

Ich war … ich weiß nicht mehr genau, wie das hieß, es ging um verschiedene Verfahren wie Nearest Neighbour und Naive Bayes.

Ah, das war dann wohl „Maschinelles Lernen: Symbolische Ansätze“.

Ich war auch noch in einer Übung, aber da habe ich nicht so viel verstanden.

Naja, das tun die Studenten auch nicht ...

Was fandest Du gut oder schlecht heute?

Allgemein den ganzen Tag fand ich super. Ich weiß jetzt, was Studenten so machen, wo ich mich anschließen kann. Ich finde es ziemlich gut, dass sowas angeboten wird, würde ich auch anderen empfehlen, mal hinzugehen.
Schlecht fand ich eigentlich nichts, kann ich nicht so sagen.
Schade finde ich nur, dass allgemein keinen Draht zwischen Schule und Uni aufgebaut wird. Nur der Informatiklehrer hat uns mal angesprochen und gesagt, dass es diesen Universitäts-Tag gibt.

Wer bist Du?

Julen aus Kronberg, ich bin am Altkönigschule-Gymnasium.
Welche Veranstaltungen hast Du heute besucht?
Ich habe eine Vorlesung in HCS besucht und eine GdI3-Übung mitgemacht.

Kennst Du Dich mit den Abkürzungen schon aus?

Naja, so ungefähr, aber wenn es ins Detail geht, das weiß ich natürlich noch nicht.

War es interessant oder eher langweilig, so in den Vorlesungen rumzusitzen?

Julen

Es ist schon interessant gewesen, aber es ist schwer, wenn man so ein paar Details schon kennt, diese in den Kontext einzuordnen.
Aber ein paar Dinge habe ich schon mal gehört, das war dann ganz gut.

Ist die Uni so wie Du sie Dir vorgestellt hast?

Es ist auf jeden Fall anders als in der Schule. Die Arbeitsatmosphäre ist ganz anders. Ich bin mit der Erwartung gekommen: ja, vielleicht sind die Leute ganz nett, vielleicht findet man jemanden, mit dem man zusammenarbeitet. Jetzt ist mir aufgefallen, dass alle in Teams arbeiten, das hat mich positiv erstaunt.

Warst Du in der Mensa?

Ja.

Wie war's?

Ziemlich groß, so zweistöckig.

Und wie war das Essen?

Ähm, ja, das ist jetzt eine Fangfrage, oder? (lacht) Aber es hat geschmeckt, man durfte sich zum Glück aussuchen, was man möchte.

Gab es Dinge, die Dir nicht so gefallen haben?

Nein, gab es eigentlich nicht.

Also nach einem Tag noch keine negativen Eindrücke. Hast Du Dich jetzt für ein Informatikstudium entschieden oder eher was ganz anderes?

Ich werde mir das natürlich noch mal überlegen, aber ich denke, dass ich hier an der TU Informatik studieren möchte, allerdings würde ich das gerne noch mit einem Fach kombinieren, ich weiß aber noch nicht genau, mit welchem. Ich war heute ja nur bei der Informatik.

Als Kombination gibt es beispielsweise Maschinenbau, das ist das CE, Computational Engineering oder mit Elektrotechnik nennt sich das IST, Informations-System-Technik. Hast Du sonst noch eine Anmerkung zum Schluss?

Ich fand es nett organisiert, dass man sich mit Studenten treffen kann, es hat mir Spaß gemacht.

Die Gespräche führte Arne Pottharst

Du bist Informatik!

Nach dem Einsteinjahr 2005 findet dieses Jahr nicht nur das Mozartjahr, sondern auch das Jahr der Informatik statt. „dank Informatik!“ ist das Motto des Jahres.

Vielleicht hat der Ein oder Andere von euch das große Plakat im Hauptbahnhof gesehen. Darauf zu sehen sind eine halber Hund und eine drittel Katze, die „dank Informatik!“ wie 400.000 andere Streuner mittels eines Chips unter der Haut wieder ihr Zuhause gefunden haben. Das ist eines von mehreren Plakaten, die auf das „Jahr der Informatik“ aufmerksam machen sollen.

Seit 2000 läuft eine Initiative des Bundesministeriums für Bildung und Forschung (BMBF). Jedes Jahr wird ein Wissenschaftsjahr gefeiert. Nachdem letztes Jahr die Physiker mit Albert Einstein an der Reihe waren, sind nun die Informatiker dran. Die Gesellschaft für Informatik (GI) und die Initiative Wissenschaft im Dialog (WiD) sowie viele Partner aus Kultur und Bildung sind ebenso daran beteiligt.

Sinn und Zweck des Jahres ist es, die Präsenz der Informatik im Alltag zu zeigen und Interesse an der Informatik zu wecken. Dazu sollen bestimmte Themen Laien verständlich dargestellt werden. Schwerpunkte sind die Themen Mobilität, Sicherheit, Kommunikation, Gesundheit, Sport, Wohnen und Kultur sowie Entertainment.

Dazu werden bundesweit Veranstaltungen verschiedenster Art angeboten. Es gibt Ausstellungen, Wettbewerbe, Vorträge, Workshops und vieles mehr. Am 17. Januar war beispielsweise Eröffnung in Berlin, mit „Invent a Chip 2006“ im Februar wurde ein Schülerwettbewerb vom Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) veranstaltet. Eine ganze Ausstellung widmet sich allein dem „pong.mythos“. Sie ist bis zum 30. April 2006 in Stuttgart zu sehen. Vorträge wie beispielsweise „Wieviel Platz braucht ein Bild? Von der Steintafel zur DVD und weiter …“ beschäftigen sich mit den unterschiedlichsten Themen. Für die Kreativen unter euch ist vielleicht der interaktive Videoclip- und Flashfilm-Contest „clip ab“ von Interesse.

Nach einem Vortrag über „embedded systems“ Mitte Februar ist für Darmstadt bis zum Redaktionsschluss nur noch eine Veranstaltung gemeldet, die „Game Days 2006“. Diese werden vom 1. bis 3. Juni vom Zentrum für graphische Datenverarbeitung (ZGDV) ausgerichtet. Allerdings wird hier eine Teilnahmegebühr von 60 Euro fällig.

Teilnehmen an den Veranstaltungen kann generell jeder. Teilweise ist eine Anmeldung nötig. Veranstaltungen organisieren kann generell auch jeder. Bedingung ist allerdings, dass die Veranstaltung für „unwissende“ Laien verständlich und zugänglich sein sollte.

Es gibt einen Kalender im Internet unter www.informatikjahr.de, in dem man sich über die angemeldeten Veranstaltungen informieren kann. Man kann die Suche nach verschiedenen Kriterien wie beispielsweise Ort, Datum, Zielgruppe oder Art der Veranstaltung filtern.

Das Jahr der Informatik beinhaltet aber nicht nur jede Menge Veranstaltungen im ganzen Bundesgebiet, sondern auch jede Woche einen „Algorithmus der Woche“. Diese Idee stammt vom Fakultätentag Informatik. Wöchentlich wird eine neuer Algorithmus erklärt. Dieser wird bunt illustriert und verständlich dargestellt. Wer also schon immer mal wissen wollte, wie Quicksort wirklich funktioniert ist hier an der richtigen Stelle.

Und warum der Fachbereich sich bisher nicht beteiligt um für ein Informatikstudium zu werben und Öffentlichkeitsarbeit zu betreiben, wissen wir leider auch nicht.

Brigitte Haaß

BMBF-Plakat:
http://www.bmbf.de/pub/menschen_verbinden.pdf

Bundesministerium für Gesundheit

IT-Systeme im Alltag

Neues Jahr, neue Technik, die „elektronische Gesundheitskarte“ (eGK) steht vor der Tür. Dieses Jahr steht ganz im Zeichen der Informatik. Das Einsteinjahr ist zu Ende und das neue Wissenschaftsjahr soll der Informatik gewidmet werden. Das beginnt gleich mit einer umfangreichen Diskussion über die neue Gesundheitskarte, die den Austausch zwischen verschiedenen Ärzten sowie das Rezept digitalisieren und die "alte" Krankenkassenkarte ablösen soll. Aber was bringt uns eine Karte mehr? Was kann diese Karte und wie sicher ist sie?

Österreich hat sie schon und die Schweiz hat eine Einführung verabschiedet und Deutschland soll ungefähr bis 2008 ebenfalls eine solche Gesundheitskarte bekommen. Eigentlich sollte das Prestigeobjekt der Bundesgesundheitsministerin bereits Anfang 2006 eingeführt werden, was aber nicht mehr realisiert werden konnte. Es handelt sich mit über 80 Millionen Teilnehmern um das weltweit größte Telematikprojekt.

Im Laufe des Jahres soll nun in Deutschland eine solche eGK, spätestens bis 2007, flächendeckend für alle Bürger eingeführt werden. Zu diesem System gehört das passende Gegenstück für Ärzte und Apotheker, der sogenannte Heilberufeausweis (HBA). Diese Einführung betrifft neben den Bürgern 180.000 Arztpraxen, 21.000 Apotheken, 2200 Krankenhäuser und etwa 260 Krankenkassen.

Die eGK soll in mehreren Schritten erweitert werden. Zunächst wird sie die bis heute

noch eingesetzte Krankenkassenkarte ablösen, dann in den weiteren Phasen das verpflichtende elektronische Rezept realisieren und es auf freiwilliger Basis ermöglichen die Patientenakte, Ärztebriefe, andere Behandlungsergebnisse und Diagnosen digital zu übermitteln.

Auf der Rückseite der eGK befindet sich, wie heute schon auf manchen neueren Krankenkassenkarten, die Europäische Krankenversichertenkarte. Hier sind alle wichtigen Daten zur Person mit Unterschrift vermerkt. Die EKVK macht den Auslandskrankenschein in Zukunft überflüssig.

Umfang & Möglichkeiten

Die eGK wird die noch aktuelle Krankenkassenkarte vollständig ersetzen und somit auch alle ihre Funktionen übernehmen. Sie ist aufgeteilt in einen Pflicht- und einen Freiwilligen-Teil, die in mehreren Stufen eingeführt werden. Der Bundesbeauftragte für den Datenschutz Peter Schaar geht davon aus, dass es noch gut 5 Jahre dauern wird, bis alle Ideen und Möglichkeiten der Karte voll umgesetzt und ausgeschöpft sind. Das heißt also, dass die meisten der hier erläuterten Funktionen wohl frühestens ab 2010 zu erwarten sind. Der Grundstein ist gelegt, jedoch kann man wohl davon ausgehen, dass es bis 2010 eine neue Version der Gesundheitskarte gibt, die sich dann ihrer „Kinderkrankheiten" entledigt hat. Hoffen wir nur, dass sie nicht in starke „Pubertätsprobleme" verfällt, sondern schnellstmöglich „erwachsen" wird. Also wird die digitale Patientenakte oder die Arzneimitteldokumentation zunächst Zukunft bleiben.

Die eGK unterscheidet sich äußerlich von der bisherigen Karte. Sie wird ebenfalls einen Chip sichtbar in der Karte tragen, darüber hinaus enthält sie auf der rechten Seite ein Bild des Besitzers.

Die Karte wird, wie bisher üblich, zur Vorlage in der Praxis gebraucht. Auf ihr gespeichert sind von Anfang an folgende „Pflichtdaten": Name, Adresse, Geburtsdatum, Kasse, Versichertennummer, -status, Ge-

Bundesministerium für Gesundheit

Schematische Übersicht über die verwalteten und gespeicherten Daten

schlecht, Gültigkeit, Status (in Nutzung, gesperrt, zu sperren, abgelaufen) sowie den Zuzahlungsstatus (nur bei gesetzlich Krankenversicherten). Wechselte man seinen Wohnsitz, musste bisher über die Krankenkasse eine neue Karte beantragt werden. Das wird nicht mehr nötig sein, da die Karte so gestaltet ist, dass die Daten auf ihr angepasst werden können. Verpflichtend ist außerdem von Anfang an die Nutzung des neuen „digitalen Rezepts", genannt eRezept.

Kosten wird den Patienten diese Karte nichts. Aber man wird wohl davon ausgehen können, dass entsprechende Kosten auf die Versicherten durch den Beitragssatz abgewälzt werden. Die Kostenträger sind nicht nur Krankenkassen, aber wer was genau bezahlt, scheint bis heute nicht richtig geklärt, genauso wenig wie die Gesamtkosten des Projekts

Bundesministerium für Gesundheit

Die Gesundheitskarte

Als „weitere freiwillige Funktionen" sollen dann nach und nach die Arzneimitteldokumentation, elektronische Patientenakte, Notfallinformationen (wie beispielsweise Blutgruppe und Arzneimittelunverträglichkeiten), Diagnosen, Röntgenbilder und Ärztebriefe mit aufgenommen werden. Dabei ist im Einzelnen noch nicht genau geklärt, ob die Daten auf die Karte selbst gespeichert werden oder ob sie auf einem zentralen Server signiert und verschlüsselt abgelegt werden. Dies wird sich erst in Zukunft durch die Testphase ergeben. In jedem Fall behält der Patient die Kontrolle darüber, was für Daten abgelegt, wem sie zugänglich gemacht und ob sie gelöscht werden. Dazu später mehr.

Durch die so gespeicherten Daten hat der behandelnde Arzt die Möglichkeit etwaige Komplikationen durch sich gegenseitig beeinflussende Medikamente und andere Diagnosen auszuschließen. „Denn jährlich sterben mehr Menschen an Arzneimittelunverträglichkeiten als im Straßenverkehr", sagte die Bundesgesundheitsministerin Ulla Schmidt (SPD). Dazu sollen ebenfalls unnötige Doppeluntersuchungen vermieden werden.

Sicherheit & Technik

Um entsprechende Sicherheit gewährleisten zu können, müssen Funktion und Architektur ihre Alltagstauglichkeit unter Beweis stellen.

Am 15. Dezember 2005 wurde ein Testlabor in Berlin in Betrieb genommen, um die schrittweise Einführung der elektronischen Gesundheitskarte im zweiten Quartal 2006 vorzubereiten. Für diesen Labortest wurden fiktive Patientendaten herangezogen. Aktuell läuft eine Testphase mit realen Patientendaten für das Projekt in acht Bundesländern. Dadurch sollen Fehler und Probleme entdeckt und vermieden werden. Aber natürlich muss die Infrastruktur und die Sicherheit schon weitgehend realisiert sein, so dass die freiwillig am Projekt teilnehmenden Patienten nicht in ihren Datenschutzrechten verletzt werden.

Ein Problem stellte sich bereits beim rheinland-pfälzischen Modellprojekt dar: „Ein Problem war, die Arztpraxen alle online-fähig zu kriegen", erläutert Jürgen Riebling Geschäftsführer der CompuGroup Health Services GmbH Koblenz, die am Modellversuch beteiligt ist.

Die Chipkarte selbst besteht aus einem ungefähr 64KB fassenden Chip. Die meisten Daten, die auf der Chipkarte gespeichert werden müssen (Pflichtdaten), fassen gut 34KB. Die Karte und ihr Inhalt ist mit einer PIN, die nur der Besitzer kennt, geschützt. Nur er selbst kann im Umfang der freiwilligen Daten bestimmen, was auf die Karte soll oder nicht und was gelöscht wird. Außerdem werden die letzten fünfzig Kartenzugriffe auslesbar für den Patienten gespeichert.

Die verschlüsselten und signierten Daten auf der Karte können nur in Verbindung mit der eGK, der auf ihr gespeicherten Signatur und der geheimen PIN sowie dem HBA des Doktors oder Apothekers gelesen werden. Hier kommt eine Art der Public-Key-Struktur zum Tragen, die sich auf zwei Karten abbildet. Wie beim RSA Verfahren wird mit zwei Schlüsseln (wie beim Verschlüsseln mit PGP) gearbeitet. Der Patient kann an Terminals selbst den Inhalt seiner Karte einsehen. Doch er kann an den Terminals nicht die Inhalte begutachten, die zusätzlich auch noch den HBA benötigen. Somit soll die informationelle Selbstbestimmung zum Teil, aber auch die Sicherheit gewährleistet bleiben.

Wie eben schon angesprochen, werden einige Daten (auch ob eine Karte noch gültig ist oder vielleicht gesperrt wurde) auf einem zentralen Server gespeichert. Diese Server sind über das Internet zugänglich.

Das bedeutet, dass alle Praxen, Krankenhäuser und Apotheken mit entsprechender Technik ausgestattet werden müssen, die es ermöglicht, abgesichert sowie ausfallsicher und schnell auf entsprechende Telematik-Dienste zuzugreifen.

Dafür ist jede Arztpraxis neben den Kartenterminals mit einem sogenannten „Konnektor“ ausgestattet. Der Konnektor verbindet das Primärsystem in der Arztpraxis mit der Telematik. Hier wurde eine extra Infrastruktur für den Einsatz der eGK entwickelt, die über die bloße Bereitstellung der Daten auf Servern hinausgeht. Der Konnektor baut eine verschlüsselte Verbindung der Gesundheitsnetzbetreiber über das Internet zu den Telematikdiensten auf. Für das Gesundheitsnetz soll ein extra reservierter IP-Bereich benutzt werden.

Arztpraxen, Apotheken und Krankenhäuser

Für Arztpraxen sowie für Apotheken und die komplexe Struktur in Krankenhäusern muss entsprechende Hardware zur Verfügung gestellt werden. Dazu gehört neben den Kartenterminals die schon angesprochenen Konnektoren sowie die zum Primärsystem in der Praxis gehörenden Server und eventuell Terminals zur Patienteninformation und zur Einhaltung des Grundsatzes der informationellen Selbstbestimmung.

Notfallinformationen

Geplant sind ebenfalls Notfallinformationen auf der Karte zu speichern. Somit wären wichtige Daten für Rettungsdienste und Notärzte verfügbar.

Hier stellt sich jedoch die Frage, wie die Rettungsdienste vor Ort verfahren. Thomas Maus merkte in seinem Vortrag auf dem 22. Choas Communication Congress (22C3) genau diese Problematik an. Schließlich kann ein Ersthelfer vor Ort nicht erst nach einer Karte mit hilfreichen Notfalldaten suchen. Diese Daten wären also höchstens nach der wichtigen Erst-Versorgung des Patienten in der weiteren Behandlung von Bedeutung. Allerdings stellt sich auch hier die Frage, inwieweit der Patient Löschfunktionen auf Notfalldaten nutzen kann und wie sinnvoll dann nicht mehr vollständige Notfalldaten sind.

Kartenterminal

Zum Terminal steht in einer über 160 Seiten umfassenden Spezifikation zur eGK: „Keiner der vorhandenen Kartenterminal-Standards erfüllt alle Anforderungen. Vertreter der Industrie bevorzugen in Abhängigkeit von ihrem Produktportfolio entweder MKT (Multifunktionales Kartenterminal nach Teletrust e.V.; Anm. d. Verf.) oder FINREAD Kartenterminals. Daher wird eine

eigene Kartenterminal-Schnittstelle definiert, die auf den vorhandenen Kartenterminals aufgesetzt werden kann und eine Interoperabilität der Kartenterminals zueinander ermöglicht."

Für den Hausbesuch des Arztes soll es ein kleines mobiles Terminal geben. Der Arzt soll einen offline-Konnektor mit sich führen. Daten können dann auch mit einem mobilen Drucker ausgedruckt werden.

Patiententerminals

Es sollen so genannte Patiententerminals (Kiosksysteme) aufgestellt werden, die den Trägern der eGK dazu dienen sollen, sich über die Daten auf der eGK zu informieren. Hiermit wird der Grundsatz zur informationellen Selbstbestimmung realisiert. Trotzdem ist es nicht möglich ohne weiteres an die Patientendaten einer entwendeten Karte zu gelangen, da hierfür immer der „Zweitschlüssel" in Form des HBA nötig ist.

eRezept

Das elektronische Rezept ist eine der ersten und verpflichtenden Neuerungen der eGK. Hier kann der Patient nicht wählen, ob er das elektronische Rezept nutzen möchte oder nicht.

Durch die eGK wird vermieden, dass für den Apotheker bspw. Medikamentennamen und Hinweise zur Einnahme nicht richtig lesbar sind und es werden erhebliche Papierkosten gespart. Die auf ca. 40-50 Cent geschätzten Bearbeitungskosten pro Rezept bei ca. 700 Millionen Rezepten pro Jahr sollen drastisch gesenkt werden.

Arzneimitteldokumentation & Patientenakte

In einer der weiteren Phasen ist es dem Patient auf Wunsch möglich, neben dem eRezept auch eine Arzneimitteldokumentation und eine Patientenakte zu speichern. Die Arzneimitteldokumentation ist sinnvoll, um etwaige Wechselwirkungen im Voraus auszuschließen.

Die Patientenakte ist sinnvoll für größere Untersuchungen, bei denen der Gang zum Spezialisten nicht ausbleibt. Der Patient ist dann in der Lage, über seine eGK Befunde und Diagnosen, Röntgenbilder und weiteres zum nächsten Arzt mitzunehmen.

Bundesministerium für Gesundheit

Manche Daten der elektronischen Gesundheitskarte lassen sich nur in Verbindng mit dem Heilberufeausweis lesen

Auf der Karte wird jedoch bei maximal 64KB nicht genug Platz sein, um Röntgen- oder Computertomografiebilder abzuspeichern. Vor allem, wenn sich mit der Zeit die Daten bei chronisch erkrankten Patienten

häufen, wird der Speicherplatz kaum ausreichen. Wird der Patient dann vom Terminal mit einer Meldung dazu aufgefordert, Teile seiner Patientenakte oder seiner Notfalldaten zu löschen, damit das Röntgenbild der Zahnzwischenräume beim Zahnarzt gespeichert werden kann? Die Entscheidung ob die Daten auf der Karte oder auf einem Server gespeichert werden sollen, dürfte also nicht schwer fallen.

Kosten, Mängel und andere Probleme

Der Sprecher der Techniker Krankenkasse, Hermann Bärenfänger, bezweifelte die Verlässlichkeit bisheriger Schätzungen: „Kein Mensch weiß, was das kosten wird, bis heute nicht." Ausgaben, die der Kasse aufgebürdet würden, müssten „letztlich auch von den Beitragszahlern bezahlt werden".

Wie Focus berichtete geht Klaus Dietz vom Bundesverband der privaten Krankenversicherung davon aus, dass die Einführung der eGK eher 4 Milliarden. Euro, statt der vom Bundesgesundheitsministerium veranschlagten 1,4 Milliarden Euro Gesamtkosten verursachen wird. Wie viel das ganze letztendlich genau kostet wird sich wohl erst im Laufe der Zeit zeigen.

Ein anderes Problem ist die Herstellung der abgesicherten und verschlüsselten Verbindung zwischen Praxen und Krankenhäusern via VPN über die Gesundheitsnetz-Betreiber zur Telematik. Nichts ist hundertprozentig sicher. Das Ausspionieren von Daten wird sich in Zukunft erhöhtem Interesse erfreuen. Die zur Verfügung gestellten Server sind eventuell angreifbar über sogenannte Denial of Service Attacken. Bei DoS Angriffen wird versucht, die Server durch Überlastung arbeitsunfähig zu machen.

Bei der Übermittlung von Patientendaten werden gleiche Datenstrukturen und Begriffe immer wieder auftauchen. Hier bietet das System für einen Mitlauscher die Möglichkeit für eine Known-Plain-Text-Attacke.

Inwieweit das System es erlaubt, es zu überlisten, gefälschte Signaturen zu benutzen, abgelaufene Karten oder gar manipulierte Kartenterminals, wird sich erst in der Zukunft zeigen. Hacker haben für solcherlei Arbeiten immer wieder eine akribische und konsequente Beharrlichkeit bewiesen. Wie wir wissen ist kein System wirklich sicher, zumindest nicht auf lange Zeit.

Fragen

Wie immer haben sich beim Durcharbeiten der Informationen einige Fragen ergeben, die sich aus selbigen nicht beantworten ließen.

Wird der Inhalt auf einer Karte gelöscht (vernichtet) wenn die Karte abgelaufen/gesperrt ist?

Muss der Patient die Karte vernichten oder zurückgeben? Wird die Karte beim Doktor eingezogen?

Was passiert, wenn der Doktor seinen HBA verliert? Ist dann der Betrieb in der Praxis überhaupt noch möglich?

Falls sich einige der Fragen bis zur nächsten Ausgabe klären, werde ich die Antworten hier natürlich mitteilen.

Ich hoffe dieser Artikel hat Euch einen guten und hinreichenden Einblick in die neue Gesundheitskarte und ihre Zukunft geben können. Durch die GI, den Bundesdatenschutzbeauftragten Peter Schaar und andere Datenschutzexperten und Vereine wurden schon Kritikpunkte angebracht und das System mit Spezialisten nach und nach verbessert.

Trotzdem sollten wir als Patienten (oder "Kunden") immer unsere Daten und Sicherheit im Blickfeld haben. Nicht nur bei der Gesundheitskarte, auch beim täglichen Einkauf, wo wir an jeder Ecke Mitgliedskarten angeboten bekommen, wo uns Geschäfte mit Prozenten ködern, um möglichst leicht Zugriff auf Kundendaten und Kaufverhalten zu bekommen.

Ulf Karrock

Begegnung der dritten Art

Um vor Augen geführt zu bekommen, was Informatiker für einen Ruf haben, genügt es, auf einer Feier oder bei einer anderen geeigneten Gelegenheit einfach einmal den Satz „Ich studiere Informatik …“ auszusprechen und die darauf folgenden Reaktionen abzuwarten. Und doch: Im Vergleich zu dem, was man teilweise außerhalb der Informatik erlebt, verblassen all die typischen Informatiker-Klischees. Hier nur ein Beispiel.

Samstagnachmittag, irgendwann im Spätsommer. Die aufgrund der Jahreszeit schon deutlich schwächer werdenden Strahlen der Sonne mischen sich mit den ersten Tropfen einer aufziehenden Regenwolke. Schwer beladen komme ich von meinem wöchentlichen Großeinkauf zurück, als ich sehe, dass im Eingangsbereich des Nachbarhauses ein junger Mann zusammengekauert auf dem Bauch liegt. Er ist mit einem Anzug bekleidet und scheint zu schlafen. Unsicher, was zu tun ist, verstaue ich erstmal meine Lebensmittel im Kühlschrank und denke darüber nach, ob ich ihn ansprechen soll oder nicht. Vielleicht hat er seinen Haustürschlüssel vergessen und wartet darauf, dass seine Mitbewohner heimkommen und ihm die Tür öffnen? Seine Freundin hat ihn vor die Tür gesetzt? Vielleicht schläft er seinen Rausch aus? Auf der anderen Seite könnte ihm durchaus auch Ernsteres zugestoßen sein, Gesundheitliches etwa, und das Viertel in dem ich wohne ist auch nicht gerade das Beste in Darmstadt. Ich muss noch einen Brief einwerfen, also nehme ich diesen und verlasse das Haus. Der Mann liegt nach wie vor an Ort und Stelle, regungslos, während der Regen nach und nach seinen Anzug durchnässt. Keine Atembewegungen sichtbar.

Zum Glück bewegt er sich, als ich ihn an-

Svenja Kahn

stupse und anspreche. Er dreht sich um und sieht mich verschlafen an. Meine Frage, ob alles okay sei, beantwortet er mit ja. Als ich ihn frage, was er dort mache, entgegnet er, dies könne er nicht sagen, weil es ihm peinlich sei. Während ich ihn fragend ansehe, richtet er eine Bitte an mich. Er sagt, er werde noch länger an dieser Stelle bleiben müssen und mache sich Sorgen, dass jemand seine Wertsachen entwenden könne. Ob ich aus diesem Grund eventuell solange auf seine Uhr und sein Geld aufpassen könne.

Für eine Sekunde bin ich fest davon überzeugt, dass es sich um einen Versuch von Psychologie-Studenten handeln muss. Doch schon im nächsten Augenblick wird mir klar, dass dies nicht sein kann. Studenten würden für einen Versuch wohl einiges tun, aber sicher nicht bei Regen durchnässt an einem Hauseingang liegen bleiben. Es handelt sich also um keine gestellte, sondern um eine echte Situation, die durch die Tatsache, dass der Mann weder betrunken noch verwirrt erscheint, nicht gerade weniger bizarr wird. Ich bin der Ansicht, nicht einfach die Wertsachen des Mannes mitnehmen zu können und sage ihm dies auch. Nachdem ich mich abermals erkundigt habe, ob wirklich alles okay ist, bringe ich schließlich meinen Brief zur Post. Als ich zurückkomme, ist der Mann verschwunden. Dafür begegne ich einer ganzen Gruppe von ähnlich gekleideten Personen an einer Kirche, die eine halbe Straße entfernt liegt. Ob er zu dieser Gruppe gehörte? Diese Frage wird wohl für immer ungeklärt bleiben..

Svenja Kahn

Termine & Mitteilungen

Fachschaftssitzung	jeden Mittwoch um 18 Uhr in D120
Schlossgrabenfest	25.-28. Mai 2006
Konferenz der Informatikfachschaften	24.-28. Mai 2006
Hochschulwahlen	19.-22. Juni 2006
Ende der Lehrveranstaltungen	21. Juli 2006
Heinerfest	29. Juni - 3. Juli 2006

Ab sofort ist die gesamte TUD rauchfrei, es herrscht Rauchverbot in allen Gebäuden und Einrichtungen.

Die FHD (Fachhochschule Darmstadt) heißt jetzt HDA (Hochschule Darmstadt, h-da.de) und hat ein ganz tolles neues schickes Logo.

Die Bauarbeiten der Universität sollen im 2. Quartal 2006 beginnen und abschnittsweise bis voraussichtlich Mitte 2008 abgeschlossen sein. Insbesondere betrifft dies das Audimax, das in dieser Zeit geschlossen ist. Der Kaffeeautomat ist ja schon weg.

Seit dem 15. April könnt Ihr Eure gesamte Post — also Briefe, Päckchen und Pakete — auch im AStA-Büro Stadtmitte aufgeben. Innerhalb des Maximail-Zustellgebiets und bei Paketen gelten deutlich bessere Konditionen als mit der Deutschen Post AG, sonst die gewohnten Preise der gelben Post. Mehr Informationen gibt es unter www.asta.tu-darmstadt.de/cms/maximail/ und das ist KEIN Aprilscherz.

Prof. Hofmann verlässt uns wieder in Richtung Zürich. Er war seit Dezember 2004 Professor für das Fachgebiet Intelligente Systeme und seit Februar 2005 Leiter des Fraunhofer IPSI.

Die Marmelade vom vorletzten Jahr, die wir im Kühlschrank gefunden haben, haben wir übrigens den Biologen verkauft. Bevor jetzt jemand sucht ...

Was ist eigentlich ein Student?

Studieren tut man nicht, man lebt das Studium. Dennoch, habt Ihr Euch schon mal gefragt, was eigentlich einen Student oder eine Studentin ausmacht? Dabei ist es ganz offensichtlich. Aber dazu später. Zunächst mal ein kleiner Abriss aus der allgeliebten Enzyklopädie Wikipedia:

Als Studenten (v. lat.: studens = „strebend (nach), sich interessierend (für)“) bezeichnet man alle an einer Hochschule oder Fachhochschule immatrikulierten Personen.

Ein Studentenwohnheim ist eine Unterkunft für Studenten, meist in kleinen Einzelzimmern („Studentenbuden“) oder in Wohngemeinschaften.

Umgangssprachlich bezeichnet man eine eher kleine Wohnung oder ein Zimmer – oft in einem Studentenwohnheim -, das von einem Studenten außerhalb seines Elternhauses bewohnt wird, mit Studentenbude.

Ein Studentenwerk ist an einem Hochschulstandort zuständig für die sozialen, wirtschaftlichen und kulturellen Belange der Studenten.

Der Studentenprotest ist eine grundsätzlich gewaltlose Form von Protestaktionen. Häufig soll auf schlechte Studienbedingungen hingewiesen werden.

Eine Studentengemeinde (auch Hochschulgemeinde) ist eine spezielle Form einer Kirchengemeinde, bei der die Mehrheit der Gemeindemitglieder Studenten sind.

Als Studenteninitiative bezeichnen sich viele studentische Gruppen, die Kontakte zwischen Studenten und Unternehmen oder Institutionen fördern sowie inner- und außeruniversitäre Ziele anstreben.

Eine Studentenverbindung oder auch Studentenkorporation ist ein Verband, der Brauchtum und gewachsene Traditionen pflegt.

Aber beschreiben diese trockenen Definitionen wirklich die Realität? Wer im November 2005 eine der beliebten „Erstie“-Tüten (Unicum Wundertüte) ergattern konnte, dem ist sicher klar, was es heißt zu studieren.

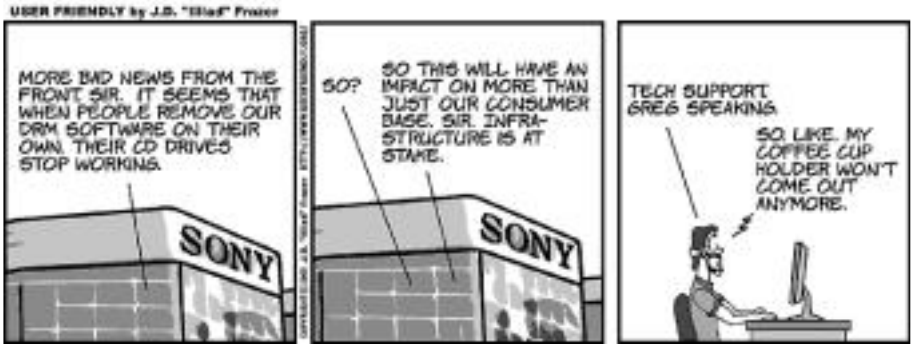
Hier der Inhalt (und jeder möge sich bitte seinen Teil dazu denken ;-))

- Nescafe Xpress, Nescafe Latte Macchiato
- Veltins energy+
- durex Kondom "Emotions", durex Gleitgel "Play Warming"
- Deutsche Bank Schlüsselhalsband
- O2 Post-It-Streifen
- Studenten-Presse

Wem das jetzt nicht klar ist, dann weiß ich auch nicht …

Also immer weiter so,

Fabian Marx



Freiraum

Im „freien“ Studentenleben sind studentische Arbeitsräume zentrale Orte. Hier soll man frei von irgendwelchen – vor allem zeitlichen – Zwängen nach Lust und Laune lernen können. Praktisch sieht es an unserer TU aber leider nicht so gut damit aus. Dennoch gibt es auch hier etliche Orte an denen man in Ruhe lernen kann.

Ständige Freiräume

- Das Allgemeine Lernzentrum (S1|04) (zwischen dem Alten Hauptgebäude und der Mensa Stadtmitte) verfügt über zwei größere Arbeitsräume, die Montags bis Freitags von 9 bis 19 Uhr geöffnet sind.
- Die Otto-B.-Mensa (S1|11) ist auch nach der Mittagszeit noch geöffnet. Nach der Mittagszeit hat man dort bis ungefähr 17:30 Uhr auf zwei Etagen viel Platz und meist auch Ruhe.
- Im Mathe-Bau (S2|15) gibt es etliche studentische Arbeitsräume, zum Beispiel die Räume 217, 336 (falls dort keine Sitzung stattfindet), 415, 417, 444 und natürlich das allseits beliebte (und daher meist recht volle) Lernzentrum Mathematik 244.
- Wenn man in Ruhe alleine lernen will, lohnt es sich oft, die verschiedenen (Fachbereichs-) Bibliotheken zu besuchen. Ruhig ist es dort auf jeden Fall, und manche „Teilbibliotheken“ sind ziemlich unbekannt und folglich auch nur schwach besucht.
- Die Universitäts- und Landesbibliothek (S3|12) verfügt über dem (chronisch überfüllten) Lesesaal über einen Gruppenarbeitsraum für 4-6 Personen mit Strom- und WLAN-Versorgung. Der Raum kann an der Information im Lesesaal für maximal vier Stunden (auch

im voraus) gegen Vorlage eines ULB-Benutzerausweises zu den Öffnungszeiten des Lesesaals (Mo-Fr. von 9 bis 22 Uhr) gebucht werden.
- Findet sich in Darmstadt nichts passendes, kann man auch an andere Orte ausweichen. Will man mit einer Gruppe beispielsweise einen ganzen Tag lang lernen, kann es sich lohnen, in andere Bibliotheken in der näheren Umgebung (wie die Uni- oder Nationalbibliothek in Frankfurt, oder direkt die Stadtbibliothek in Darmstadt) auszuweichen.

Freiräume am Abend

Gegen 19 Uhr werden fast alle Gebäude der Uni abgeschlossen (einige Fachbereiche schließen ihre Gebäude sogar schon um 18 Uhr). Doch ist eine Universität der natürliche Lebensraum eines Studenten, und das Leben endet nun mal nicht um 19 Uhr. Die folgende Auflistung enthält eine Übersicht über abendliche Freiräume.

- Der Lesesaal sowie die Lehrbuchausleihe der Universitäts- und Landesbibliothek (S3|12) ist von Montag bis Freitag bis 22 Uhr geöffnet. Abends findet man dort normalerweise auch immer einen Platz.
- Im Robert-Piloty-Gebäude (S2|02) ist der E-Poolraum der RBG rund um die Uhr verfügbar. Nach 19 Uhr kann man mit einem Transponder durch den Seiteneingang in den Poolraum gelangen.
- Das Alte Hauptgebäude (S1|03) ist unter der Woche bis 24 Uhr geöffnet. Ab 19 Uhr kommt man aber nur noch durch den Haupteingang in das Gebäude. Offene Räume werden in der Regel ab 18 Uhr von den Hausmeistern abgeschlossen. Allerdings müssen sie die Räume 9 bis 13 auf Nachfrage von Studenten Montags bis Freitags von 18 bis 22 Uhr und am Wochenende von 10 bis 18 Uhr aufschließen.
- Ebenfalls im Alten Hauptgebäude gibt es den offenen AStA-Raum (S1|03/056). Dieser Raum befindet sich im ersten Zwischengeschoss. Er ist normalerweise immer geöffnet und steht allen Studierenden rund um die Uhr zur Verfügung.
- Das HRZ betreibt im Alten Hauptgebäude zwei Poolräume, S1|03/016 und S1|02/030, die von Montag bis Freitag bis 24 Uhr geöffnet sind. Dort gibt es auch einige Tische für Notebooks. Und wenn man die Tastatur zur Seite schiebt, kann man dort auch mit Papier und Büchern arbeiten. Auf den PCs selbst läuft allerdings nur ein Klicki-Bunti-OS (Linux läuft dort entgegen den Informationen auf den Webseiten des HRZs *nicht*).

Freiräume am Wochenende

Auch Samstags und Sonntags gibt es Freiräume, wie die folgende Übersicht zeigt.

- Der Lesesaal sowie die Lehrbuchausleihe der Universitäts- und Landesbibliothek (S3|12) ist Samstags und Sonntags von 9 bis 18 Uhr geöffnet.
- Der HRZ-Poolraum S1|03/016 im Alten Hauptgebäude ist Samstags von 10 bis 18 Uhr geöffnet.
- Im Alten Hauptgebäude stehen die Räume 9 bis 13 im Prinzip ganztägig zur Verfügung. In dem Zeitraum von 10 bis 18 Uhr müssen die Hausmeister am Wochenende auf Nachfrage von Studierenden diese Räume öffnen (siehe oben).
- Im Alten Hauptgebäude ist der offene AStA-Raum immer verfügbar (siehe oben).

Eine aktuelle Version davon findet Ihr auf D120.de/freiraum/. Dort könnt Ihr auch nach Räumen suchen, die zwischen Veranstaltungen liegen und in dieser Zeit frei sind. Wenn Ihr weitere Freiräume kennt, freuen wir uns auf Eure E-Mail an andreas@D120.de.

stock.xchng

Professorensprüche

Prof. J. Buchmann: „Abends sind Menschen über 50 dumm!“

Prof. J. Buchmann: „Wenn Leute zu mir in die Prüfung kommen … ich bin immer so glücklich, dass ich nicht der Prüfling bin.“

Prof. J. Buchmann: „Ja, der junge Mann da vorne mit dem schwarzen T-Shirt, das … bevor es zusammen mit dem blauen T-Shirt gewaschen wurde mal … rot war?“ – Wenig später: „Es tut mir leid, ich wollte Ihr T-Shirt jetzt nicht diskriminieren.“

Prof. J. Buchmann, nachdem er hingebungsvoll etwa zwei Minuten damit zugebracht hat, eine falsche Formel mit allen ihm zur Verfügung stehenden Stiften zu überkritzeln: „Also Sie haben gesehen, auch Informatik kann Kunst sein.“

Prof. J. Buchmann: „Text ist auch schön. Zieht die Sache in die Länge, muss ich nicht so viel arbeiten.“

Prof. J. Buchmann: „‚Ah, Scheiße!‘ hat der Fermat gesagt … also, der war ja Franzose ... ‚Merde! ‘“

Prof. J. Buchmann: „Wie man das einschaltet weiß ich nicht … ah, hier, an der Wand, sehr cool.“

Prof. J. Buchmann: „Der Fermat dachte, dass die alle Primzahlen wären, weil er an dem Tag noch was vorhatte …“

Prof. J. Buchmann: „Was ist 140 mod 37? 34? Also ich kann das nicht überprüfen … zu alt.“

Prof. Sorin A. Huss: „Jetzt hat man das Problem, dass man manchmal einen neuen Wert reinschreiben will. Soll vorkommen bei nem RAM-Speicher.“

Ein Handy klingelt, es dauert etwas, bis es ausgemacht wird. Prof. Fürnkranz: „War das Ihr Handy oder Ihr Wecker?“

Prof. Huss bekommt endlich einen von zwei Beamern zum Laufen: „Jetzt werden wir gierig, den zweiten kriege ich auch noch an.“

Ein Student verlässt den Raum, nachdem Prof. Huss den Titel der Vorlesung bekannt gegeben hat. Student: „Ich bin hier in der falschen Vorlesung.“ Prof. Huss: „Bei mir sind Sie immer richtig!“

Prof. Huss: „VLSI heißt Very Large Scale … ääh … Baustein.“

8 Uhr, Rekonfig. Shoufan: „Wenn ich mich umschaue, sehe ich mindestens acht Leute gähnen. Das ist eine Art Parallelismus, das passt zu dieser Vorlesung.“

Prof. Eveking (ETiT): „Bestimmte Dinge können nie gleichzeitig auftreten, zum Beispiel Ostern und Dienstag.“

Prof. Weihe zum Thema biologische Evolution: „Wir sind alle Nachkommen von Pfadfindern. Die, die das Flachland erreicht haben. Und nicht von denen, die sich auf dem Mont Blanc verirrt haben.“

Prof. Weihe, kurz vor Vorlesungsende: „Klatschen ist immer eine gute Möglichkeit, dem Sprecher das Wort abzunehmen.“

Prof. Weihe kurz vor der Pause: „Ich rate mindestens 30% der Anwesenden, sich einen Kaffee zu ziehen. Muss kein Kaffee sein, kann auch was härteres sein.“

Prof. Huss an unruhige Studenten: „Ich kann auch die Folien ohne Ton kommentieren, wenn sie möchten.“

Prof. Huss: „Sie haben dann die Fähigkeit, bestimmte Dinge nicht zu können.“

Prof. Huss vor einer Teilklausur: „Wenn sie in den Übungen nicht nur die Luft verdrängt haben, dürften sie gut vorbereitet sein.“

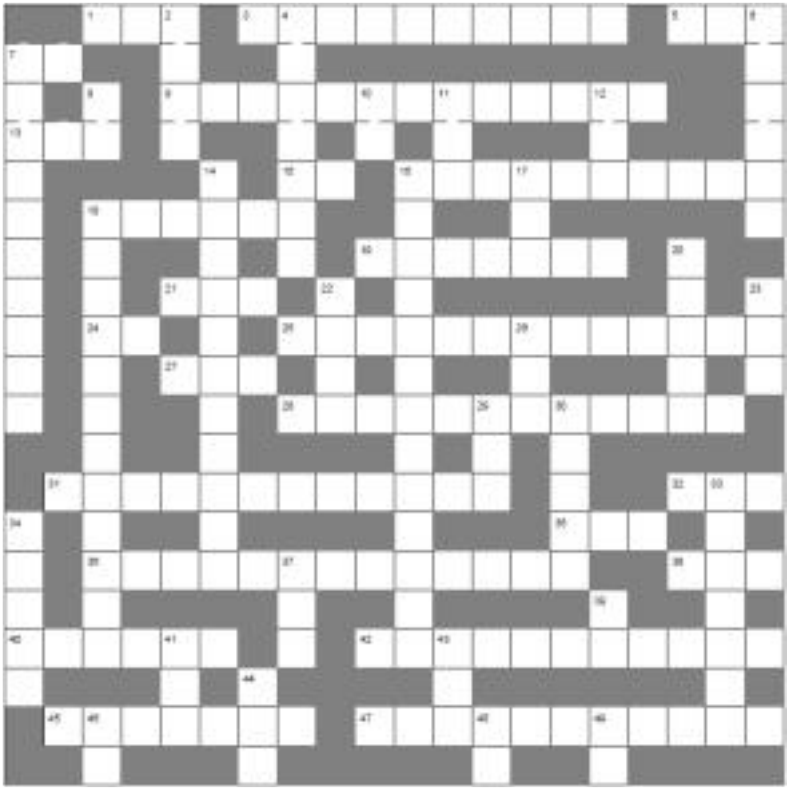
Dr. Fraikin: „Ich bin inhärent schreibfaul.“

Unbekannter Physik-Professor bei der Evaluation: „Sie können die Blätter oben in die Boxen links und rechts legen, von Ihnen aus gesehen wäre das rechts und links.“

Prof. Fürnkranz: „Der linke und rechte Teil der Gleichung ist richtig, das habe ich abgeschrieben, aber die mittlere Umformung ist sicher falsch, die habe ich selber gemacht.“

Vielen Dank an alle fleißigen Sammler, sammelt weiter!

Kreuzworträtsel



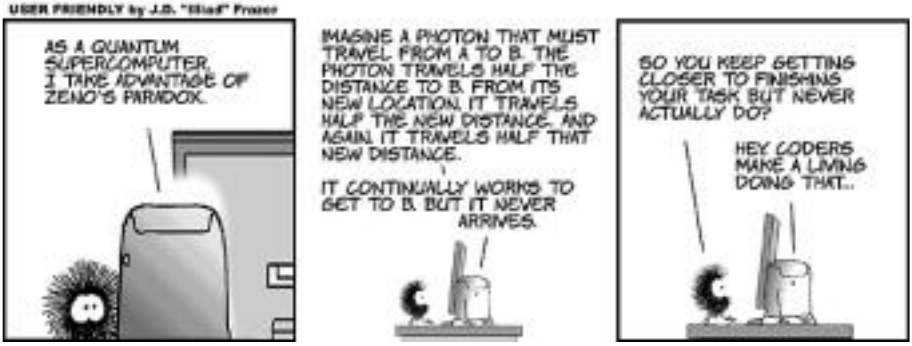
Waagerecht :

01 Vereinigung intern. Standardisierungsgremien (Abk.)
03 Drucker, Maus, Modem, Monitor sind Geräte der ...
05 Lebensbund
07 Abk. für Computer, Rechner
09 (geheime) Nachrichten verborgen übermitteln
13 griechischer Buchstabe
15 Künstliche Intelligenz (en; Abk.)
16 Menschenfeind
18 Eine europäische Hauptstadt
19 Grundstoff
21 Das höchstwertigste (linkeste) Bit (Abk.)
24 Schlüsselwort für Abfragen (Java)
25 Restgraph eines Flußgraphen (Graphenth.)
27 Erbinformationsträger
28 Erfinder der Programmiersprache Pascal (schweizer)
31 Drucker mit Trommel zum Auftragen der Farbe
32 von A nach B
35 Abk. für Telekommunikations-Anschlusseinheit
36 Egoshooter
38 Ugs. Geschlechtsverkehr
40 körperliche oder seelische Qualen
42 Hochschullehrer (Mehrz.)
45 Blasinstrument
47 Schutz von digitalen Informationen

Senkrecht :

02 Nahrungskategorie
04 Ein europäisches Land
06 Ein Kontinent
07 Kommunik. unter Gleichgestellten (Inf. ausgeschr.)
08 Auswärtiges Amt (Abk.)
10 festgelegte Höhe, Meeresspiegel
11 Graphische Benutzeroberfläche (Abk.)
12 Kurz: Variablentyp für Ganze Zahlen (Inf.)
14 beseitigen, ausschalten, entfernen
16 Name für Anzahl Additionen derselben Zahl (Math.)
17 Abschiedsgruß
18 franz. Phil., Physiker & Mathem. des 17 Jh.
20 Teil eines Baumes
22 Vorsilbe für zehnten Anteil (lat.)
23 Hörorgan
26 Kadaver
29 Zeitmesser
30 ärmelloses Kleidungsstück
33 Arzneimittelschein auf der eGesundheitskarte
34 Kampfgerät
37 elektronische Gesundheitskarte (Abk.)
39 Informatik (en; Abk.)
41 Zahlwort
43 häufig
44 Modell zur Datenbankmodellierung (Abk.)
46 chem. Zeichen für Silber
48 Hühnerprodukt
49 Nachfolger der Kassette und LP (Abk.)

Lösung von November 2005



Griechische Buchstaben

Wir gehen in die sechte Folge der fachübergreifend beliebten Sammelserie der griechischen Buchstaben. Schnell ausschneiden und ins Sammelalbum einkleben oder mit Freunden tauschen!

Wir verlassen die seichten Gebilde der Anfängerbuchstaben und nähern uns den etwas unbekannteren Buchstaben, die nicht so häufig verwendet werden. Aber trotzdem sollte in der vollständigen Sammlung der Griechischen Buchstaben das ζ nicht fehlen, schon alleine, um etwas humanistische Bildung zu demonstrieren.

Verwendung

Es gab mal einen berühmten Mathematiker namens Riemann, der hat eine Funktion erfunden und diese ζ -Funktion genannt. Sie stellt die Verteilung der Primzahlen als Formel dar.

Und es gab auch mal ein paar Informatiker, die haben ein Betriebssystem mit diesem Namen versehen, das früher auch mal als BeOS bekannt war.

Der Autobauer Lancia hat ein Auto namens ζ herausgebracht.

Viel mehr Beispiele der Verwendung gibt es eigentlich nicht, da dieser Buchstabe so unbekannt ist, verwenden ihn wohl nur wenige.

Zubereitung

Man nehme einen Stift, zum Beispiel den Lieblingsfüller mit gefederter und ergonomisch geformter Griffmulde. Mit diesem nun das Papier berühren und dabei die Bewegungen ausführen, die zum Erscheinen des ζ auf selbigen führen. Diese wären: eine kleine Schleife gegen den Uhrzeigersinn, dann eine große hintenangehängt. Wenn eine halbe Umdrehung vollbracht ist, die Richtung ändern und einen kleinen Schlenker unten anhängen. Fertig ist das ζ und kann fortan bewundert werden.

Empfehlung

Da der ungeübte Laie bei der Zubereitung des ζ leicht eine Sehnenscheidentzündung bekommen kann, empfehlen wir, eine ausgewogene Mischung aus ζ und anderen Buchstaben zu verwenden. Sieht dann auch nicht so eintönig aus.

Und wenn Ihr ganz brav seid, bekommt Ihr nächstes mal ein η.

Arne Pottharst

Impressum

Auflage: 1000
ISSN 1614–4295

Inforz — Zeitung der Studierenden des Fachbereiches Informatik der Technischen Universität Darmstadt.

Die Redaktion tagt unregelmäßig. Erreichbar ist sie im Fachschaftsraum, per E-Mail an inforz@D120.de oder im Internet unter D120.de/inforz/ und inforz.D120.de.

Redaktionsschluss dieser Ausgabe: 5. April 2006
Redaktion dieser Ausgabe: Arne Pottharst
ViSdP: AStA der TU Darmstadt
Satz: Arne Pottharst
Titelbild: stock.xchng
Druck: Druckwerkstatt Arheilgen

Vielen Dank an alle Helfer (w/m) (in willkürlicher alphabetischer Reihenfolge): Alexander Juling, Andreas Höfer, Andreas Marc Klingler, Brigitte Haaß, Gina Häußge, Jacqueline Vogel, Nils Knappmeier, Prof. Alexander May, Svenja Kahn, Ulf Karrock.

Angebote der Fachschaft

Die Fachschaft tagt jeden Mittwoch um 18.00 Uhr in Raum S2|02-D120. Gäste und Besucher, Neugierige und Interessierte sind jederzeit herzlichst willkommen.

Aktuelle Informationen auf unserer Website
www.fachschaft.informatik.tu-darmstadt.de oder kurz: www.D120.de

Eure Mitstudierenden erreicht Ihr im Forum unter
www.D120.de/forum/

Anregungen und Fragen sendet Ihr bitte an:
fs@D120.de
Schnelle Antwort garantiert!

Wenn's noch schneller gehen muss: Telefon 06151 16-5437

Unsere Tür steht jederzeit für Euch offen! Schaut einfach mal rein!

Fachschafts - Sitzung 26. Mai '97

PROTOKOLL

Anwesende:

Post: Einladung zur TiHF

Protokollant: Oli

Mitteilungen: Lust-Kommission sucht jemanden für Multi-Media-Unterkommission.

FBR: Tronje berichtet. Bis 16:30 Uhr gedauert.

- Kommissionen: EDV ex. weiterhin
  LUST: Mike Fischer hinzu
  Auslandsst: Julia Stoll
- Forschungssemester: R. Hofmann SS 98
  Neuhold "
- Stellungsnahme bis zum 30. Mai wegen Wirt-Studienordnung (Neu!)