

Aktuelles Lexikon

RSA-System

Das wichtigste Verschlüsselungssystem (Kryptosystem) von Daten zum Schutz vor unbefugten Zugriffen ist zur Zeit das RSA-System. Es wurde 1978 von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt. Dieses System beruht auf der Tatsache, daß es praktisch nahezu unmöglich ist, zwei große Primzahlen p und q aus der alleinigen Kenntnis des Produkts $n = pq$ zurückzugewinnen (Problem der Primfaktorzerlegung). Zur Verschlüsselung genügt im wesentlichen die Bekanntgabe von n , zur Entschlüsselung müssen beide Primzahlen p und q bekannt sein. Das RSA-System verläuft folgendermaßen: Seien p und q zwei beliebige große Primzahlen; in der Praxis haben p und q ungefähr 100 Dezimalstellen; die Frage, ob eine Zahl Primzahl ist oder nicht, läßt sich „ziemlich sicher“ mit einem speziellen stochastischen Algorithmus feststellen. Es sei $n = pq$, und $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ sei definiert durch $\varphi(n) = (p-1)(q-1)$, die sogenannte Eulersche φ -Funktion. Man wählt eine beliebige Zahl c zwischen 1 und n für die $\text{ggT}(c, \varphi(n)) = 1$ gilt. Mit Hilfe des euklidischen Algorithmus kann dies auf einfache Weise maschinell erfolgen. Anschließend bestimmt man eine Zahl $d \in \mathbb{N}$, so daß $cd = 1 \bmod \varphi(n)$ erfüllt ist. Die Zahlen n und c legen dann die Verschlüsselungsfunktion V fest. Ein (vorher in Zahlen umzuwandelnder) Klartext w wird verschlüsselt durch die Abbildung

$$V(w) = w^c \bmod n.$$

Die Entschlüsselungsfunktion wird durch die Zahlen n und d festgelegt und bestimmt sich für einen Schlüsseltext w durch

$$E(w) = w^d \bmod n.$$

Beispiel: Seien $p = 47$, $q = 59$, $n = pq = 2773$ und $\varphi(n) = (p-1)(q-1) = 2668$.

Für c wählt man z. B. die Zahl 17 (wegen $\text{ggT}(17, 2668) = 1$) und für d die Zahl 157, denn es gilt:

$$cd = 2669 = 1 \bmod 2668.$$

Die Verschlüsselungsfunktion V wird durch das Zahlenpaar (n, c) , die Entschlüsselungsfunktion E durch das Zahlenpaar (n, d) festgelegt:

$$V(w) = w^c \bmod n = w^{17} \bmod 2773, \\ E(w) = w^d \bmod n = w^{157} \bmod 2773.$$

Um einen Text zu verschlüsseln, müssen zunächst die Buchstaben in Zahlen umgewandelt werden. Man setzt $A = 01$, $B = 02$, $C = 03$, ...

Das Leerzeichen habe die Codierung 00. Das als Zahl dargestellte Wort wird anschließend in Blöcke gleicher Größe zerlegt, die getrennt verschlüsselt werden. Für die Blockgröße empfiehlt sich die Zahl i , für die $10^{i-1} < n < 10^i$ gilt. Die Zahldarstellung des Wortes STALL lautet z. B. 1920011212.

Nach Zerlegung in Blöcke der Länge 4 ($10^3 < 2773 < 10^4$) und Auffüllen mit Leerzeichen erhält man 1920 0112 1200.

Durch Anwendung der Verschlüsselungsfunktion folgt der Schlüsseltext:

$$2109\ 1084\ 1444,$$

denn es gilt z. B.

$$2109 = 1920^{17} \bmod 2773.$$

Mit Hilfe der Entschlüsselungsfunktion erhält man den Klartext zurück:

$$1920 = 2109^{157} \bmod 2773.$$

Die bei der Ver- und Entschlüsselung auftretenden hohen Potenzen brauchen nicht effektiv ausgerechnet zu werden (Gefahr des Überlaufs), denn man kann die Zwischenergebnisse klein halten, indem man nach jeder Multiplikation *modulo* rechnet.

Die Sicherheit des RSA-Systems hängt wesentlich davon ab, ob in der Zukunft schnelle Algorithmen gefunden werden, um Zahlen in Primfaktoren zu zerlegen, was gleichbedeutend mit einem Knacken des Systems ist. Zur Zeit besteht noch keine Gefahr, denn die schnellsten Programme benötigen zum Zerlegen von 200stelligen Zahlen in Primfaktoren mehrere tausend Jahre Rechenzeit.

Andreas Schwill

Dieser Artikel wurde mit geringfügigen Änderungen dem Duden „Informatik“, 21993, des Dudenverlages, Mannheim/Leipzig/Wien/Zürich, entnommen.

Online

Unterrichtsmaterial über WWW

Internet-Verfügbarkeit – eine weitere multimediale Dimension

World Wide Web (WWW) ist ein einfach zu handhabendes Informationssystem auf dem Internet. Es wird heute weltweit zur Suche, Sichtung und zum Austausch von Informationen verwendet. Im Schulbereich mangelt es oft gerade am Austausch von Unterrichtsmaterialien. Bestehende Materialien wie traditionelle Aufgabensammlungen können nur mit großem Aufwand aktualisiert oder auf die eigenen Bedürfnisse angepaßt werden. WWW stellt eine erstklassige Plattform für den einfachen, kostengünstigen und schnellen Austausch von Unterrichtsmaterialien dar. Diese können als Multimediale Dokumente nach dem Hypertextprinzip auf dem Server gesichtet oder mittels eines integrierten Datenbanksystems gezielt gesucht werden. Ausgewählte Dokumente werden vom Benutzer auf den eigenen Computer heruntergeladen und können so in den vorhandenen Originalformaten weiterbearbeitet werden. Die Benutzer können auch zu einzelnen Unterrichtsmaterialien Kommentare und Ergänzungen anbringen oder selbst Unterrichtsmaterialien auf den Server hinaufladen.

Elektronische Informationen im Ausbildungsbereich

In den USA ist die Anwendung von Internet und World Wide Web an den Schulen schon sehr verbreitet. Gemäß einem Bericht des Office of Technology Assessment des U.S. Congress (1995) hatten 1995 bereits 35 % aller amerikanischen Schulen Zugang zum Internet. Die amerikanische Regierung hat sich zum Ziel gesetzt, bis im Jahr 2000 sämtliche Schulen ans Internet an-

zuschließen. Das Internet zusammen mit WWW und den nach dem "Click and go" bedienbaren Hypertext-Browsern wie *Netscape* erschließen den Schulen völlig neue Informationsquellen. Der ganze Schulbereich muß sich aber auch einer großen Herausforderung stellen.

Im folgenden wird speziell die Frage untersucht, welche Auswirkungen die neuen Medien im Lehrmittel-Bereich haben dürften. Wird es auch in Zukunft noch Lehrmittel im traditionellen Sinne geben? Oder stellen die Lehrkräfte die Lehrmittel individuell entsprechend ihren spezifischen Wünschen zusammen? Am Beispiel von *EducETH* – Prototyp eines Education Servers – werden die Möglichkeiten des elektronischen Publizierens im Unterrichtsbereich skizziert.

Das Internet zusammen mit dem WWW stellt eine Riesenfülle von Informationen zur Verfügung. Dabei kann zwischen verschiedenen Ebenen der Informationsnutzung unterschieden werden:

Shopping Center

Das Internet präsentiert sich in seiner ungeordneten Gesamtheit wie ein großes Einkaufszentrum. In einem Einkaufszentrum beispielsweise kann der Kunde mehr oder weniger ziellos umherschlendern. Er kann die Angebote der verschiedenen Geschäfte bestaunen, vergleichen, sich aber auch in der Vielfalt des Angebots verlieren. Hat der Kunde einen ganz spezifischen Wunsch, ist es oft nicht einfach das entsprechende Geschäft oder Regal zu finden. Einen speziellen Kundenservice (individuelle Anpassungen, Reparaturen etc.) kann man in einem großen Einkaufszentrum nicht unbedingt erwarten.

Genauso präsentiert sich das Internet in seiner ungeordneten Gesamtheit. Neben einer Unzahl von wertlosen Informationen finden sich auch aktuelle, für Schulen hochinteressante Angebote. Für die Lehrerinnen und Lehrer besteht die Schwierigkeit darin, diese Angebote zu finden. Die verschiedenen Suchhilfen (z. B. *Yahoo* oder Suchmaschinen wie *Lycos*) bieten zwar in vielen Fällen eine gewisse

Hilfe an, vergleichbar einem Informationsschalter in einem Einkaufszentrum. Für eine zielstrebige und effiziente Informationssuche muß aber der Suchraum vom Benutzer im voraus klarer abgegrenzt werden können. In der Analogie des Einkaufens wird der Kunde deshalb in vielen Fällen ein Fachgeschäft bevorzugen.

Fachgeschäft

Hat ein Kunde ein genau spezifiziertes Bedürfnis (beispielsweise ein Surfbrett) ist das Fachgeschäft (in diesem Fall ein Sportgeschäft) eine gute Wahl. Das Angebot umfaßt hier im wesentlichen nur Sportartikel, das Personal ist meistens speziell geschult und das Geschäft bürgt für eine gewisse Qualität. Selbstverständlich treffen diese Merkmale auch auf Sportgeschäfte in einem Einkaufszentrum zu! Im Fachgeschäft unter kundiger Beratung gelangt der Kunde im allgemeinen schnell zu seinem Ziel.

Entsprechend präsentiert sich die Situation auf dem Internet, sobald man auf spezifische Fachserver zugreift. Beim *Geometry Center* der Universität von Minnesota (<http://www.geom.umn.edu>) wird man kaum Hinweise zu frühmittelalterlichen Gedichten finden, hingegen viel und qualitativ hochwertiges Material aus dem Umfeld der Geometrie. Für die Lehrkraft stellt sich das Problem, wie gute Fachgeschäfte, sprich Fachserver, gefunden werden können.

Strickwarenladen

Das Angebot eines Strickwarenladen geht noch einen Schritt weiter als dasjenige von Fachgeschäften. In einem Strickwarenladen kann man nicht nur Wolle und Stricknadeln kaufen. Man kann sich auch beraten lassen: Auf Wunsch werden individuelle Strickmuster angefertigt, Anpassungen oder Überarbeitungen bestehender Strickmuster vorgenommen. Der Kontakt Kunde/Geschäft ist viel enger, und es kann durchaus sein, daß eine Kundin ihre Strickwaren im Geschäft zum Verkauf anbietet.

Genauso kann man sich speziell auf Schulen ausgerichtete Fachserver vorstellen. Die Funktion sol-

cher Schulserver (Education Server) ist nicht mehr nur die Bereitstellung gewisser Informationen, sondern die interaktive Verwaltung von Informationen und Unterrichtsmaterialien. Der Benutzer erhält die Möglichkeit aktiv das Informationsangebot zu beeinflussen.

Elektronisches Publizieren

In den nächsten Jahren kann davon ausgegangen werden, daß im Bereich von Unterrichtsmaterialien tiefgreifende Änderungen stattfinden werden. Das elektronische Publizieren nimmt ganz allgemein, speziell aber auch im Unterrichtsbereich einen immer größeren Stellenwert ein. Andrew M. Odlyzko (1995) und andere sagen für viele Publikationen aus dem Unterrichtsbereich einen baldigen Wechsel vom „auf Papier“ gedruckten Medium zum elektronischen Medium voraus. Eine Übersicht zum Themenkreis „Elektronisches Publizieren im Ausbildungsbereich“ findet man bei Andrew Treloar, Electronic Scholary Publishing and the World Wide Web, <http://www.deakin.edu.au/people/aet/>. Speziell für Fächer mit eher geringen Auflagen im Lehrmittelbereich bieten sich mit Internet und WWW völlig neue Möglichkeiten an. Im Ausbildungsbereich mit seinen dezentralen, föderalistischen Strukturen existieren oft keine einheitlichen, allgemein verwendeten Lehrmittel. Der Markt für Lehrmittel ist demzufolge relativ klein, und der kostengünstigen Herstellung und Verbreitung von Lehrmitteln kommt daher eine große Bedeutung zu.

Verbreitung von Unterrichtsmaterialien

Immer wieder hört man, die Zusammenarbeit und der Teamgeist unter den Lehrkräften sei mangelhaft. Insbesondere auf der Sekundarstufe II, auf der ein ausgeprägtes Fachlehrersystem gepflegt wird, sind es oft weniger zwischenmenschliche als organisatorische Gründe, die den Erfahrungsaustausch behindern. Welche Lehrerin, welcher Lehrer kennt nicht eine der folgenden Situationen:

- ▷ Eine ehemalige Studienkollegin ruft an. Ob man ihr nicht die Unterlagen zum Thema „Regenwürmer“ schicken könne. Jene Unterrichtseinheit, die man vor einem Jahr anlässlich einer Biologielehrer-Weiterbildung vorgestellt hat.
- ▷ Im Fachausschuß Mathematik wird ein „Freiwilliger“ gesucht, der die Aufgaben der letzten Abschlußprüfungen zusammenstellt, einheitlich redigiert und anschließend an die 483 Mitglieder verschickt.
- ▷ Für einen Einführungskurs in ein Standard-Textsystem hat die Beratungsstelle für Informatik einen attraktiven Lehrgang zusammengestellt, der von vielen Schulen verwendet wird. Leider ist kurz nach dem Druck des Lehrganges eine neue Version der Software auf den Markt gekommen. Die Änderungen gegenüber der alten Version sind nicht grundlegender Natur. Trotzdem sollten aus didaktischen Gründen einige Anpassungen vorgenommen werden.
- ▷ Die Vereinigung der Englischlehrerinnen und -lehrer gibt periodisch eine Leseliste heraus. Die Liste umfaßt eine ganze Sammlung von Büchern, die sich für den Einsatz im Englischunterricht eignen, aufgeteilt nach Schulstufe, Schwierigkeitsgrad und weiteren Kriterien. Leider sind gerade Neuerscheinungen, die aus aktuellem Anlaß für den Einsatz im Unterricht speziell interessant wären, nicht auf dieser Liste enthalten.
- ▷ Der Physiklehrer möchte zum Thema Thermodynamik eine Serie von Übungsaufgaben zusammenstellen. Gerne würde er einige Aufgaben aus einer weitverbreiteten Aufgabensammlung verwenden. Die ganze Aufgabensammlung umfaßt aber rund zehnmal mehr Aufgaben, als im normalen Unterricht behandelt werden können. Zudem sind viele Aufgaben im Schwierigkeitsgrad und in der Notation nicht mit dem laufenden Unterricht kompatibel. Der Physiklehrer möchte auch noch eigene, mehr anwendungsorientierte Aufgaben hinzunehmen. Er überlegt sich, ob er seine Übungsreihe durch

Kopieren, Schneiden und Kleben herstellen oder gleich die Aufgaben abschreiben und neu redigieren soll.

Die angeführten Beispiele haben alle ein gemeinsames Grundproblem: Unterrichtsmaterialien, die an und für sich bereits in elektronischer Form vorliegen, sollen *ergänzt, korrigiert, neu zusammengestellt* und anschließend *verteilt* werden. Bei den Materialien handelt es sich typischerweise nicht um Lehrbücher, sondern um Dokumente, die eine relativ kurze Halbwertszeit haben oder nur als Archiv für die Herstellung von Dokumenten dienen. Mit Dokumenten sind dabei nicht nur Textdokumente gemeint, sondern auch Multimediadokumente. Anstelle einer Physikaufgabensammlung kann ebenso eine Sammlung von Bildern für den Geografieunterricht oder Unterrichtssoftware treten.

In allen Beispielen ist die Suche, Sichtung, Überarbeitung und Verteilung der Unterrichtsmaterialien mit viel Aufwand und Kosten verbunden. Oft werden gerade dieser Aufwand oder die entstehenden Kosten gescheut, mit der bekannten Konsequenz: Unterrichtsmaterialien werden unter den Lehrkräften nur zaghaft ausgetauscht, und gedruckte Lehrmittel sind oft nicht aktuell genug.

Noch drastischer zeigen sich diese Schwierigkeiten an einer Lehrerfortbildungsstätte. An der ETH Zürich (ETHZ), einer der beiden Technischen Hochschulen in der Schweiz, werden Gymnasiallehrerinnen und -lehrer für naturwissenschaftliche Fächer und Mathematik ausgebildet. Seit einigen Jahren wird auch in den Ingenieurfächern eine Lehrerausbildung angeboten. Dieses Angebot ist mehr auf den Bereich der Fachhochschulen und die innerbetriebliche Ausbildung ausgerichtet. Ein wichtiger Teil der Lehrerausbildung an der ETHZ ist die Umsetzung von Unterrichtsmethoden aus der Allgemeinen Didaktik: Die Studentinnen und Studenten werden in der allgemeindidaktischen Ausbildung nicht nur theoretisch über eine Vielzahl von Unterrichtsmethoden informiert. Sie erarbeiten in ihrem Unterrichtsfach konkrete Unterrichtseinheiten, die

einzelne Unterrichtsmethoden illustrieren und von anderen Lehrkräften als Unterrichtsgrundlage eingesetzt werden können. Im Laufe der letzten Jahre ist auf diese Weise in allen Fächern eine Fülle von Leitprogrammen, Puzzleeinheiten, Fallstudien, Werkstätten und anderen Unterrichtsmaterialien entstanden. Die Qualitätsanforderung an diese Materialien orientiert sich dabei nicht am hohen Standard traditioneller Lehrmittel. Im Vordergrund steht vielmehr das Bestreben, den Schulen aktuelle Informationen schnell und einfach zugänglich zu machen. Die Dokumente werden deshalb auch meistens gleich als Kopiervorlage abgegeben. Aufgrund eingehender Rückmeldungen können die vorliegenden Materialien laufend überarbeitet und verbessert werden.

Mit der wachsenden Nachfrage nach solchen Unterrichtsvorbereitungen hat der administrative Aufwand rasch die Schmerzgrenze erreicht. Hier könnte *Elektronisches Publizieren und Kommunizieren* einen Ausweg anbieten. Nachdem nun mit World Wide Web eine einheitliche, hardwareunabhängige und einfach zu bedienende, grafische Benutzeroberfläche auf dem Internet zur Verfügung steht, ist es nur noch eine Frage von wenigen Jahren, bis der Großteil der Schulen die neuen Möglichkeiten des „Information Super Highways“ nutzen wird.

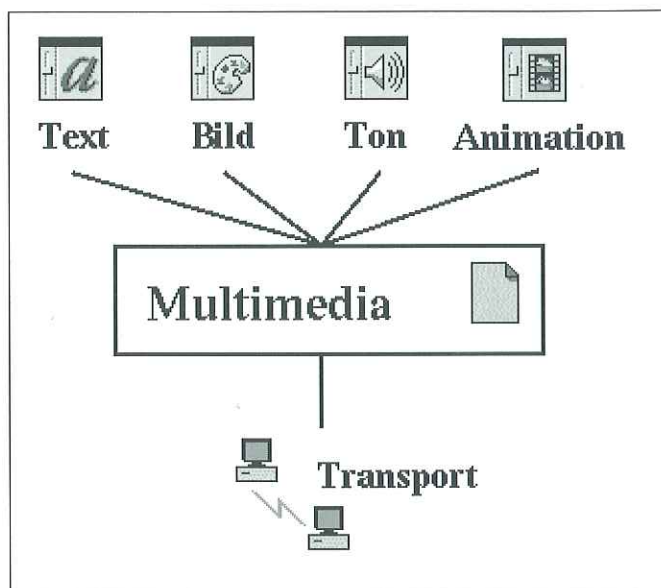
Elektronisches Publizieren und Kommunizieren

If you can call up any paper on your screen and, after deciding that it looks interesting, print it out on the laser printer on your desktop, will you need your university's library?

Andrew Odlyzko (AT&T Bell Laboratories)

Publishing umfaßt im wesentlichen die Herausgabe und Qualitätssicherung von Druckerzeugnissen wie Bücher, Zeitungen, Zeitschriften, wissenschaftliche Artikel und vieles mehr. An gutes *publishing* werden verschiedene Erwartungen gestellt. Das *publishing* muß effizient sein, seine Erzeugnisse sollen eine große Verfügbarkeit aufweisen und das Ergebnis muß benutzerfreundlich sein. Mit *Effizienz* wird die Schnelligkeit von der Er-

Bild 1:
Transportier-
barkeit als
neue Kompo-
nente eines
Multimedia-
dokuments.



stellung einer Arbeit bis zu deren Erscheinen auf dem Markt bezeichnet. *Verfügbarkeit* besitzt einen örtlichen und zeitlichen Aspekt. Ein Dokument aus einer Bibliothek beispielsweise ist sowohl örtlich als auch zeitlich begrenzt verfügbar. Das gleiche Dokument auf dem Internet ist im Gegensatz zum Bibliotheksdokument örtlich und zeitlich unbegrenzt verfügbar. In diesem Fall bildet einzig die Sprache und die Internetverfügbarkeit eine Beschränkung. Dokumente, die von einem größeren Kreis gelesen werden, weisen gewisse gemeinsame Merkmale auf: Inhaltlich liefern sie brauchbare neue Erkenntnisse zu einem bestimmten Fachgebiet. Außerdem sind sie meistens nach anerkannten Regeln der Typographie gedruckt. Deshalb erstaunt es nicht, daß auch für Internet-Dokumente bereits verschiedene *style guides* existieren.

Es ist schwierig vorauszusagen, wie die elektronische Zukunft das Verlagswesen verändern wird. Sicher ergeben sich jedoch grundlegende Änderungen im Bereich der Publikation wissenschaftlicher Literatur. Bereits heute stellen viele Fachgesellschaften ihre wissenschaftlichen Publikationen (wie z.B. *Electronic Journal for Combi-*

natorics) auf dem Internet zur Verfügung. Der Zugang zu den Publikationen ist gratis, und es sind über 500 Personen bei dem Journal „eingeschrieben“. Diese erhalten als besonderen Service neue Artikel per E-Mail zugesandt. Diese Publikation von wissenschaftlichen Arbeiten ist bei weitem nicht die einzige auf dem Internet. Allein im *Directory of Electronic Journals* (der Association of Research Libraries) fanden sich im April 1995 bereits 440 Einträge. Fachgesellschaften wie AMS (American Mathematical Society) und ACM (Association for Computing Machinery) sind längst „online“. Die Artikel auf dem Internet werden wohl jedoch nur dann gelesen, wenn sie als Multimediadokumente im Hypertextformat (mit anklickbaren Verweisen) zur Verfügung stehen. Für bestehende Arbeiten bedeutet dies eine zeitraubende Konvertierung in das *HTML*-Format. Der Trend zum elektronischen Publizieren wird zusätzlich durch den finanziellen Druck vorangetrie-

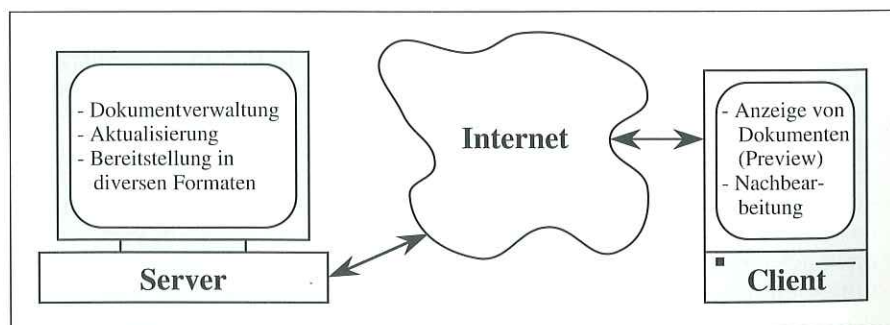
ben, der auf den Universitäten lastet. Die Form des elektronischen Publizierens ist wesentlich preisgünstiger als die herkömmliche Form der Druck-Erzeugnisse. Zudem kann die Flut von Veröffentlichungen nur noch auf elektronischem Weg verarbeitet werden.

Mit der Verbreitung von Textverarbeitungsprogrammen, wie *TEX* und *LATEX*, wurde Autoren ein Werkzeug zur Erstellung von Publikationen mit standardmäßig gutem Layout in die Hand gegeben. Durch WWW und die Hypertextstrukturen wird nun auch das Wegrationalisieren der Verleger mehr und mehr zu einer Tatsache. Die Vorteile der Qualitätssicherung durch das Lektorat eines Verlags sind nur scheinbarer Natur, denn auch im Bereich des elektronischen Publizierens ist ein Lektorats- und Referee-Prozeß möglich. Verlage und Fachgesellschaften müssen sich der neuen Herausforderung stellen und sich im *electronic publishing* engagieren. Eine Möglichkeit, die sich hier anbietet, ist das *proofreading* als ihre Stärke weiterzuführen, und auf dem Internet Verzeichnisse „guter“ Arbeiten zu verwalten.

Multimedia mit neuer Dimension

Der Begriff *Multimedia* ist ein Synonym für die Integration von „Text, Bild, Ton und Animation“ in einem Dokument. Mit der Entwicklung des WWW und der Internet-Technologie ergibt sich eine wesentliche Begriffserweiterung. Die *Transportierbarkeit und benutzergerechte Zusammenstellung (Customization) von Information* ist eine neue, zentrale Eigenschaft derselben. Multimedia wird also um eine dynamische Komponente erweitert. Dank Internet und geeigneten Pro-

Bild 2: Aufgabenverteilung
Server-Seite und Client-Seite.



grammen können heute beliebige Multimediadaten, aus der ganzen Welt auf fast jeden Computer geholt und weiter bearbeitet oder konfiguriert werden. Die weltweite Vernetzung erlaubt dabei im Gegensatz zu lokalen Netzwerken den ortsunabhängigen Zugriff auf die gewünschten Daten (Bild 1, S. 64).

Unterrichtsmaterialien sind typischerweise Multimediaprodukte. Gerade deshalb ist für Unterrichtsmaterialien *electronic publishing* von großer Bedeutung. Durch den Einsatz von *electronic publishing* können laufend auf einfache Weise neue und überarbeitete Multimedia-Dokumente schnell und kostengünstig zur Verfügung gestellt werden. Dadurch entsteht ein größerer und aktuellerer Bestand von verwendbaren Dokumenten als beim herkömmlichen Lehrbuch. Die Lehrkräfte treffen daraus eine ihren Bedürfnissen angepaßte, maßgeschneiderte Auswahl. *Customized retrievability* wird in Zukunft auch im übrigen Verlagswesen eine wichtige Rolle spielen.

Verschiedene Medien im Vergleich

Unterrichtsmaterialien können grundsätzlich auf viele verschiedene Arten zur Verfügung gestellt, beziehungsweise publiziert werden. Die folgenden Überlegungen beziehen sich auf das Fallbeispiel einer Physikaufgabensammlung. Die Aussagen gelten jedoch sinngemäß für beliebige Unterrichtsmaterialien.

Lehrbuch

Die Buchform stellt nach wie vor die verbreitetste Form der Verteilung von Unterrichtsmaterialien dar. Die Vorteile der Buchform sind:

- ▷ Lehrkräfte sind es gewohnt, mit Lehrbüchern umzugehen.
- ▷ Bücher sind kompakt und handlich.
- ▷ Auf ein Buch kann jederzeit zugegriffen werden.
- ▷ Ein Buch erlaubt es, Notizen anzubringen.
- ▷ Oft überdauert ein Buch mehrere Jahrzehnte und erhält somit

auch eine historische Komponente.

Wesentliche Nachteile der Buchform sind:

- ▷ Neue Aufgaben sowie Verbesserungen und Korrekturen können nur in Neuauflagen berücksichtigt werden.
- ▷ Die Information geht nur vom Buch zur Lehrperson, sie ist also unidirektional.
- ▷ Die Aufgaben liegen nicht in digitaler Form zur Nachbearbeitung vor, es sei denn eine Diskette ist beigelegt.

CD-ROM

Die Lösung auf CD-ROM ist mit der Form des Lehrbuches vergleichbar, erlaubt aber zusätzlich Multimedia. Positiv fällt ins Gewicht, daß die Dokumente in digitaler Form vorliegen und deshalb einfach weiterverarbeitet werden können. Zudem ist eine *rechnerunterstützte* Suche auf der Aufgabensammlung möglich. Die CD-ROM erfordert jedoch einen Computer und ein CD-Lesegerät.

ftp-Archiv

Als weitere Variante besteht die Möglichkeit eines ftp-Archivs (*file transfer protocol* – Protokoll zum Übertragen von Dateien zwischen zwei Rechnern) zur Bereitstellung von Aufgabensammlungen. Als Vorteil gegenüber den bisherigen Varianten können die Aufgaben immer auf dem neuesten Stand gehalten werden. Die Nachteile überwiegen jedoch stark:

- ▷ Es ist kein *preview* (Voransicht der Dokumente) möglich. Ein Zeitverlust durch das Herunterladen von Dokumenten vor deren Sichtung muß in Kauf genommen werden.
- ▷ Ein ftp-Archiv ist nicht jederzeit verfügbar, sondern abhängig vom Netzzugang.
- ▷ Ein ftp-Archiv setzt gewisse „informatiktechnische“ Fertigkeiten voraus.
- ▷ Die Suchmöglichkeiten sind beschränkt.
- ▷ Es stellt eine Einweglösung dar, Feedback ist nur beschränkt möglich.

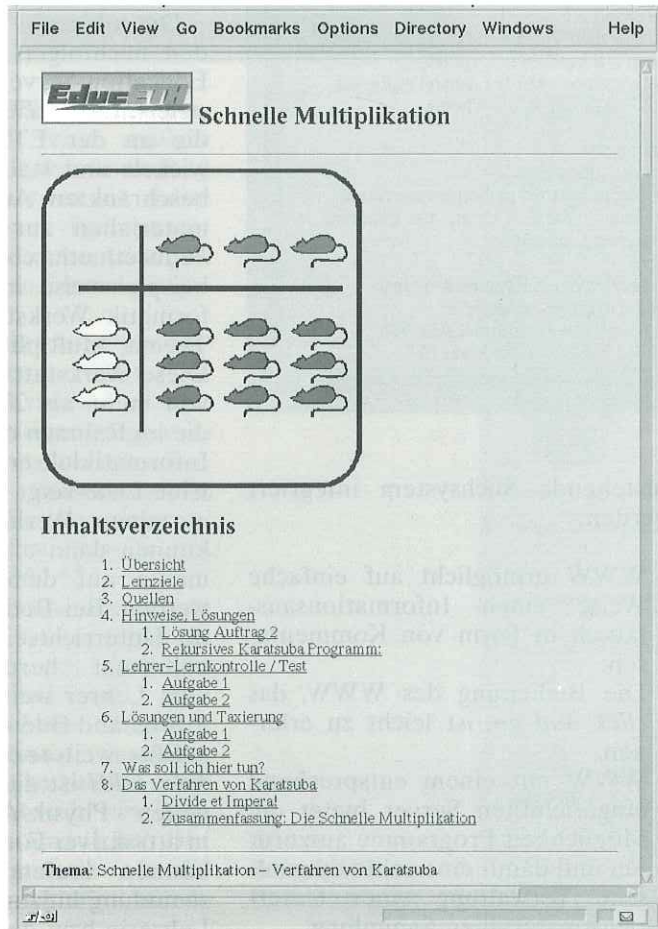


Bild 3:
Titelblatt eines Werkstattpostens zum Thema „Schnelle Multiplikation“.

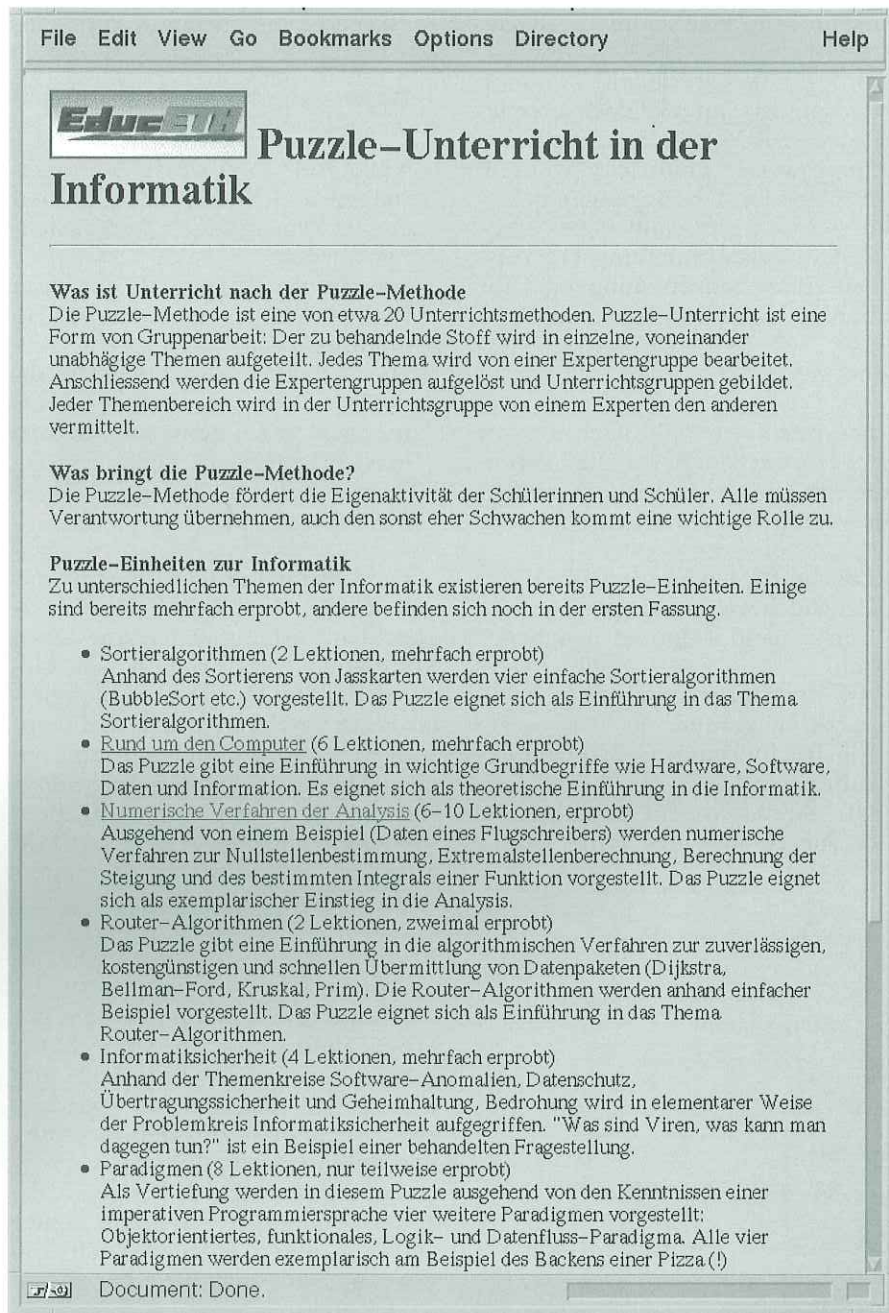


Bild 4:
Übersicht auf *EducETH*
zu Puzzle-Unterricht.

- ▷ Alle Dokumente werden in einem Standardformat gesichtet.
- ▷ Eine Nachbearbeitung von Aufgaben ist in gespeicherten Originalformaten des Dokumentes möglich.
- ▷ Eine PostScript-Version ist immer (durch einen WWW user agent) verfügbar.

Der Nachteil einer WWW-Lösung: WWW ist nicht jederzeit verfügbar, sondern abhängig vom Netzzugang (Bild 2, S. 64).

Aufgrund dieser Überlegungen zeigt sich, daß die Verteilung und Verwaltung von Unterrichtsmaterialien auf dem WWW zur Zeit die am meisten in die Zukunft gerichtete Variante ist.

Beispiel eines Education Servers

Die obigen Ausführungen werden nachfolgend am Beispiel des Education-Servers *EducETH* illustriert. *EducETH* wurde als Fallstudie an der ETH in Zürich entwickelt und stellt bereits heute in beschränktem Ausmaß Unterrichtsmaterialien zur Verfügung (<http://educeth.ethz.ch:8084/>). So werden beispielsweise im Fachbereich Informatik Werkstatt-Einheiten zum Thema Multiplikation angeboten. Diese Werkstatt ist eine Sammlung von mehr als 20 Werkstattposten, die im Rahmen der Ausbildung von Informatiklehrern entstanden sind. Eine Liste zeigt eine Übersicht der einzelnen Werkstattposten. Diese können dann als Hypertext-Dokumente auf dem Server gesichtet werden. Bei Bedarf werden einzelne Unterrichtseinheiten im Originalformat heruntergeladen und vom Lehrer weiterbearbeitet (Bild 3, S. 65 und Bild 4).

Ein weiterer Bestandteil von *EducETH* ist die Publikation einer neuen Physik-Aufgabensammlung in attraktiver Form. Neue Aufgaben können laufend zur Aufgabensammlung hinzugefügt werden. Die Lehrerin bzw. der Lehrer trifft eine

- ▷ Ein ftp-Archiv unterstützt Multimedia nicht direkt.

World Wide Web

WWW bietet zusätzlich zu den bereits erwähnten Varianten die wesentliche Komponente der Kommunikation. Unterrichtsmaterialien können nicht nur gesichtet und auf den eigenen Computer geholt werden; eine aktive Mitarbeit und Erweiterung einer solchen Sammlung ist möglich. Neue Dokumente können zum Server geschickt, und ins

bestehende Suchsystem integriert werden.

- ▷ WWW ermöglicht auf einfache Weise einen Informationsaustausch in Form von Kommentaren.
- ▷ Die Bedienung des WWW, das *click and go*, ist leicht zu erlernen.
- ▷ WWW mit einem entsprechend eingerichteten Server bietet die Möglichkeit Programme aufzurufen und damit eine echte dynamische Verwaltung einer Unterrichtsmaterialien-Sammlung.

EducETH Suchformular

Ich suche Aufgaben zu ..

Bitte pro Feld maximal einen Begriff angeben. Der Rest wird ignoriert.

Taxonomie minimal , maximal . (1 - 6)

Bearbeitungsdauer zwischen und Minuten.

oder

[EducETH](#) [Hauptseite](#)

Für Ihre Fragen und Kommentare
 Letzte Änderung: 29. Mai 1995 / sja

Bild 5:
Beispiel eines
Suchauftrages
in der Physik-
aufgaben-
sammlung.

Nach dem Einsatz einer Aufgabe im Unterricht, können die Erfahrungen mit der Aufgabe den Fachkolleginnen weitergegeben werden. Die angebrachten Kommentare können von der Aufgabenseite und von der Lösungsseite her gesichtet werden (Bild 7, nächste Seite).

Das Fallbeispiel der Physikaufgabensammlung zeigt sehr schön, wie die neuen Multimedia-Möglichkeiten sinnvoll genutzt werden können. In anderen Fachbereichen sind vergleichbare Bedürfnisse abzudecken. Selbstverständlich können auf *EducETH* auch Informationen im üblichen Rahmen zur Verfügung gestellt werden (z. B. Hinweise auf Lehrerfortbildungen, Listen von schulrelevanten WWW-Servern).

Dokumente auf *EducETH* werden in den folgenden Formaten auf dem World-Wide-Web-Server angeboten:

- ▷ in *HTML* (zur Sichtung)
- ▷ im Originalformat (für Download)
- ▷ in *PostScript* (für Download und Druck)

Um die Dokumente auf dem World Wide Web in Hypertextfor-

Auswahl von Aufgaben für den Unterricht und stellt eine maßgeschneiderte Aufgabensammlung her. Unterstützt werden sie dabei von einem Datenbank-Suchsystem. Sie können auch Kommentare und Ergänzungen zu einzelnen Aufgaben anbringen.

Das Suchformular dient zur Suche nach vorgegebenen Kriterien. Für die einzelnen Kriterien ist eine fachspezifische Unterstützung vorgesehen. Durch Anklicken beispielsweise von **Themenkreis** wird eine Hilfeseite mit den zur Verfügung stehenden Themen des Faches angezeigt (Bild 5).

Aus den Aufgabenseiten zeigen Verweise auf die Lösungen und zusätzliche Informationen. Auf die Funktionen **Kommentar anschauen**, **Kommentar hinzufügen**, **Aufgaben suchen**, **Aufgabe herunterladen** und **Statistik** zeigt sowohl ein Text als auch ein Piktogramm-Link. Der Statistikaufbau zeigt, wie oft die Aufgabe heruntergeladen wurde (Bild 6).

Bild 6:
Beispiel einer
Physikaufgabe.

File Edit View Go Bookmarks Options Directory Help

NEPRS Rahmen Lösung

Heisse Schokolade

Hatten Sie auch schon den Eindruck, dass eine heisse Schokolade etwas wässrig sei? Eine mögliche Ursache könnte das Verfahren sein, mit dem die kalte Milch in Gaststätten erhitzt wird. Man leitet heissen Wasserdampf in die kalte Milch und lässt ihn kondensieren.

Welche prozentuale Verdünnung entsteht, wenn Milch aus dem Kühlschrank (6 Grad C) auf diese Weise auf 60 Grad C erhitzt wird?

Hinweis: Die Milch darf, wenigstens was die thermischen Daten betrifft, als Wasser betrachtet werden. Kalorimetrie, Kondensationswärme

[EducETH](#) [Hauptseite](#)

Für Ihre Fragen und Kommentare
 Letzte Änderung: 30. Juni 1995 / sja

mat anzubieten, müssen die einzelnen Dokumente für die Sichtung ins HTML-Format konvertiert werden. Dazu gibt es für die verschiedenen Betriebssysteme und Textverarbeitungen entsprechende Konvertierungsprogramme. Der Aufwand für diese Konvertierung kann insbesondere bei älteren Dokumenten recht groß sein. Bei geschickter Planung läßt sich der Konvertierungsaufwand aber bei neu herzustellenden Multimedia-Dokumenten in engen Grenzen halten. Der heute noch aufwendige Satz mathematischer und technischer Dokumente (Formeln, Diagramme) dürfte mit kommenden HTML-Versionen sowieso hinfällig werden.

Wichtig bei der Entwicklung von *EducETH* war es, möglichst wenige Fremdsoftwareprodukte in das System zu integrieren, um späteren Versionenkonflikten (Kompatibilitätsproblemen) und Schnittstellenproblemen innerhalb des Education Servers vorzubeugen. Die Entwicklung eines Prototypen auf dem Internet bedingt bereits den Einsatz einer Vielzahl von Softwareprodukten, die miteinander kommunizieren müssen. Aus diesem Grund wurde die Datenorganisation beispielsweise direkt auf *UNIX* und nicht auf einer fremden Datenbank (*Oracle*, *Wais*, ...) implementiert.

Zusammenfassung und Ausblick

Durch die Spezifikation und Implementation eines interaktiven WWW-Servers wird die Grundidee des Informationsangebotes erweitert. *EducETH* vereinigt dynamische Aspekte in Form von *Subject-specific Search*, *Downloading*, *Dynamic Comments* und *Uploading* von Dokumenten. Weil der Prototyp auf dem Internet als WWW-Server realisiert wurde, ist die Bedienung mittels WWW *user agents* (wie *Netscape*) einfach. Die Implementation von *EducETH* basiert ausschließlich auf Standard-*UNIX*-Befehlen und *PERL*-Skripten und ist deshalb bezüglich neuen Anforderungen besonders flexibel. Dank dem Einsatz der hardware-unabhängigen Programmiersprache *PERL* kann der Prototyp ohne größere

Bild 7:
Kommentar zu
einer Aufgabe
hinzufügen.

The screenshot shows a web browser window with the title bar 'File Edit View Go Bookmarks Options Directory Help'. The main content area has the *EducETH* logo and the heading 'Kommentar hinzufügen'. Below this is a paragraph of text: 'Um optimal von den Aufgaben in dieser Sammlung profitieren zu können, sollten Sie alle wichtigen Erfahrungen mit einer Aufgabe ihren Fachkolleginnen und -kollegen weitergeben.' There are two input fields: 'Ihren Namen' (containing 'Hans Muster') and 'Einsatzbereich der Aufgabe' (containing 'Gymnasium'). Below these is a large text area with the text: 'Bitte tragen Sie hier Ihre Erfahrungen ein. Meine Schuelerinnen hatten Probleme mit dem Begriff "prozentuale Verduennung". Ich habe ihnen den Ausdruck anhand eines einfachen, einsichtigen Beispiels erlaeutert.' At the bottom of the form are two buttons: 'Kommentar aufnehmen' and 'Kommentar ungültig'. Below the form is a link 'Hauptseite' and a footer: 'Für Ihre Fragen und Kommentare Letzte Änderung: 28. Juni 1995 / sja'. The status bar at the bottom of the browser window shows 'Document: Done.'

Anpassungen auf ein anderes *UNIX*-System portiert werden.

Als nächster Schritt erfolgt ein längerer Praxistest, um Erfahrungen mit dem bestehenden Prototyp zu sammeln. Von entscheidender Bedeutung wird aber in erster Linie der Umfang und die Qualität der auf *EducETH* angebotenen Unterrichtsmaterialien sein. Lehrerinnen und Lehrer muß die Gelegenheit gegeben werden, sich mit den neuen Möglichkeiten des *Information Super Highways* bekannt zu machen. Konkret heißt das: Jede Schule sollte mindestens einen Zugang zum Internet besitzen. In der allgemeinen Lehreraus- und -fortbildung müssen Kurse zur Nutzung von Internet und World Wide Web angeboten werden. Zudem brauchen Informatiklehrkräfte eine solide Ausbildung. Sie müssen in der Lage sein, an Schulen selber Informations-Server aufzubauen und zu betreiben. Gerade die Datenautobahn und ihr Umfeld haben einmal mehr gezeigt, daß in der Informatik kein Ende der rasanten Entwicklung absehbar ist. Allein mit dem Ansatz einer integrierten Informatik wird man auf die Dauer in den Schulen nicht allen Entwicklungen Rechnung tragen können. Auch die

Schule benötigt über kurz oder lang für den Informatikunterricht Spezialisten mit der notwendigen Sach- und Methodenkompetenz.

Silvia J. Ackermann
Werner Hartmann
Informatik-Didaktik
Theoretische Informatik
ETH Zürich
CH-8092 Zürich
E-Mail: ackermann@inf.ethz.ch
oder: hartmann@inf.ethz.ch

Michael Stumm
Department of Electrical and
Computer Science
University of Toronto
Toronto, Ontario M5S 1A4
Canada
E-Mail: stumm@eecg.utoronto.ca

Literatur

Odlyzko Andrew M.: Tragic loss or good riddance? The impending demise of traditional scholarly journals. Cambridge: The MIT Press/ASIS monograph, 1995.

Office of Technology Assessment of U.S. Congress: Teachers and Technology: Making the Connection. 1995.