Programm der Herbsttagung 1999

Mathematische Gesellschaft in Hamburg
zusammen mit dem
Fachbereich Mathematik der Universität Hamburg

Mathematik und Informatik

Freitag, 5. November 1999, Hörsaal H 1, Geomatikum

15.15 - 15.30 Uhr Begrüßung und Einführung

15.30 - 16.15 Uhr Manfred Kudlek (Hamburg)

Geschichte der Theoretischen Informatik

16.30 - 17.00 Uhr Kaffeepause

17.00 - 17.45 Uhr Sven Heinrich (Hannover)

Das Jahr-2000-Problem aus der Sicht eines Rückversicherers

18.00-18.45 Simone Fischer-Hübner (Hamburg)

Datenschutz durch Technik

ca. 19.30 Uhr Nachsitzung im Hotel Elysée, Rothenbaumchaussee 10,

Raum *Hamburg* (Anmeldung erforderlich).

Für das Essen wird ein Kostenbeitrag

von DM 40,- pro Person erhoben.

Sonnabend, 6. November 1999, Hörsaal H 1, Geomatikum

9.15 - 10.00 Uhr Wilfried Brauer (München)

Zum Gemeinsamen und Trennenden von Mathematik und Informatik

10.15 - 11.00 Uhr Michael Hortmann (Bremen)

Kryptografie, Fragen der Zertifizierung, Datensicherheit aus dem aktuellen Stand

11.15-11.30 Pause

11.30 - 12.15 Uhr Monika Seiffert (Hamburg)

Kryptologie in der Schule

14.30 Uhr Exkursion zum Fachbereich Informatik

``Vorführung aus verschiedenen Forschungsbereichen

(Künstliche Intelligenz; theoretische, technische Informatik)''

Zusammenfassung der Vorträge

Geschichte der Theoretischen Informatik Prof.Dr.Dr. M. Kudlek

Es werden Ursprünge der und Einflüsse auf die Theoretische Informatik vorgestellt. Diese kommen aus verschiedenen anderen Disziplinen.

1.

Rechnen: Entwicklung der Zahlschrift und des Rechnens.

2.

Logik: Entwicklung der Formalen und Algebraischen Logik (Aristoteles, Scholastik, Boole, Frege, ...).

3.

Zeichen: Untersuchung von Zeichenketten (Thue, Post), Entwicklung Formaler Systeme und von Kalkülen für Logik und Mathematik.

4.

Mathematik: Rekursive Funktionen, Berechenbarkeit, Algorithmus (Church, Turing).

5.

Linguistik: Formale Beschreibung Natürlicher Sprachen (Chomsky), Entwicklung von Programmiersprachen.

6.

Unentscheidbarkeit: Unvollständigkeit (Gödel).

7.

Biologie: Formale Beschreibung biologischer Systeme (Lindenmayer).

8.

Information: Komplexität (Hartmanis, Kolmogorov).

9.

Physik: Quantencomputer.

Das Jahr-2000-Problem aus der Sicht eines Rückversicherers Dr. Sven Heinrich

Allgemein besteht eine große Besorgnis und Unsicherheit über die Auswirkungen des sogenannten Jahr-2000-Problems. Wie die meisten Versicherungsunternehmen hat auch die Hannover Rück-Gruppe hierzu eine Vielzahl von Aktivitäten eingeleitet, die von einem eigenen Projekt koordiniert werden.

In erster Linie betreffen diese Aktivitäten die Überprüfung der vorhandenen technischen Systeme und die Behebung erkannter Probleme mit dem Wechsel von 1999 auf das Jahr 2000. Betroffen sind vor allem die Systeme der Informationsverarbeitung, aber auch alle anderen technischen Anlagen.

Bei einem Finanzdienstleister werden darüber hinaus in besonderer Weise Aktiva und Passiva der Bilanz berührt. So muß zum einen das versicherungstechnische Exposure durch die Jahr-2000-Thematik abgeschätzt und beim Underwriting berücksichtigt werden. Zum anderen sind mögliche Auswirkungen der Jahr-2000-Thematik auf die Kapitalanlagen zu analysieren und entsprechende Maßnahmen einzuleiten.

Weitere Aktivitäten betreffen die Information der Geschäftspartner einschließlich der Zusicherung der Jahr-2000-Festigkeit seitens wichtiger Lieferanten, die Beantwortung von Anfragen von Behörden und Geschäftspartnern, die Abklärung der juristischen Rahmenbedingungen sowie die Erarbeitung einer Notfallplanung.

Die Abschätzung des versicherungstechnischen Exposures durch das Jahr-2000-Problem wirft erhebliche Probleme auf und entzieht sich letztlich einer Quantifizierung. Gleichwohl gibt es Möglichkeiten der Exposurebegrenzung, wobei diese in den verschiedenen Märkten in unterschiedlichem Ausmaß genutzt werden.

Datenschutz durch Technik Dr. Simone Fischer-Hübner

In unserer vernetzten Gesellschaft ist Datenschutz zunehmend in Gefahr und wird verstärkt zum internationalen Problem. Eine internationale Harmonisierung der Datenschutzgesetzgebung ist jedoch aufgrund kultureller Unterschiede kaum erreichbar. Daher wird von Datenschutzbeauftragten und vom deutschen Gesetzesgeber verlangt werden, daß Datenschutz auch durch Technik durchgesetzt werden muß. Dieser Beitrag soll einen Überblick zu Datenschutztechnologien zum Schutze von Benutzern und Betroffenen geben. Zunächst werden Datenschutztechnologien zum Schutze der Benutzeridentitäten betrachtet, welche insbesondere Anonymität, Pseudonymität, Unbeobachtbarkeit für die Benutzer gewährleisten können. Danach wird ein aufgabenbasiertes Datenschutzmodell vorgestellt, welches in Form eines formalen Zustandsmaschinen-Modells definiert wurde und speziell das Ziel hat, juristische Datenschutzforderungen technisch durchzusetzen.

Zum Gemeinsamen und Trennenden von Mathematik und Informatik Prof.Dr.Dr.h.c. Wilfried Brauer

Es werden Denk- und Vorgehensweisen sowie generelle Zielsetzungen und Fragestellungen betrachtet, und zwar unter folgenden Gesichtspunkten:

Theorie (Konzepte, Formalismen, Methoden),

Praxis (Ingenieurskunst, Anwendungen),

Mechanisierung (Hilfsmittel, Werkzeuge, ihre Konstruktion und Verwendung).

Während in der Mathematik die Theorie im Zentrum steht, ist es in der Informatik die Mechanisierung/Automatisierung (mit Hilfe des Computers).

Unterschiedliche Vorgehensweisen in der Informatik beruhen auf verschiedenen Auffassungen vom Computer als

symbolverarbeitende Maschine zur Durchführung mathematischer und logischer Operationen,

physikalisch/technisches Gerät zur Steuerung von Geräten, Maschinen, Prozessen,

künstliches ``Gehirn'' zur Nachahmung intelligenten Verhaltens von Lebewesen.

Kryptographie, Fragen der Zertifizierung, Datensicherheit aus dem aktuellen Stand Dr. Michael Hortmann

Die Kryptologie ist eine der Basiswissenschaften für die Informationsgesellschaft im Zeitalter des Internet. Im Wortsinne beschäftigte sie sich zunächst mit der Verschlüsselung von Texten bzw. Daten, seit der Entdeckung der Public Key Kryptographie vor 30 Jahren aber auch mit komplexeren Anwendungen wie Digitalen Signaturen, Digitalem Geld oder geheimen und fälschungssicheren demokratischen Wahlen via Telekommunikation. Vor 30 Jhren wandelte sich damit die Kryptologie von einer arkanen Wissenschaft im Umfeld der Geheimdienste in eine Teildisziplin der Mathematik

mit engen Verflechtungen zur Informatik, aber neuerdings auch mit der (theoretischen) Entwicklung von DNA- und Quantencomputern der Molekularbiologie und Physik.

Der Vortrag geht ein auf die Mathematischen Grundlagen der Public Key Systeme, auf Infrastrukturen wie Trust Center, die zur Verwaltung solcher Systeme bei massenhfter Anwendung notwendig sind, sowie auf rechtliche und politische Probleme beim Aufbau dieser neuen Infrastrukturen.

Ausführliche Zusammenfassung im pdf-Format

Kryptologie in der Schule Monika Seiffert

Kryptologische Verfahren eignen sich für Lernsituationen sowohl im Mathematikunterricht als auch im Informatikunterricht. Da ihnen noch immer ein Geruch von Geheimdienst und Krimi anhaftet, sie andererseits wegen ihrer Bedeutung für die Sicherheit von Datenübertragungen in einem öffentlichen Netz hoch aktuell sind, geht von ihnen eine hohe Motivation aus. Je nach Fachperspektive werden im Unterricht die Schwerpunkte unterschiedlich gesetzt. Dabei stößt man im Mathematikunterricht ohne Computer genau so schnell an Grenzen wie im Informatikunterricht ohne Mathematik.

Im Vortrag sollen Ideen für solche Lernsituationen in der Sekundarstufe I und II vorgestellt werden. Jeweils wird betrachtet, welche Inhalte des betreffenden Faches dabei erarbeitet oder geübt und welche Ziele damit verfolgt werden können.