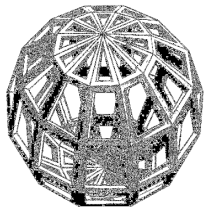
Mathematik für alle Sinne
Akademientag zur Mathematik 2008



Primzahlen schützen das Internet – aber wie lange noch?

Referenten: Johannes Buchmann, Nadja Kokic, Elias Most, Erik Tews

Das Internet hat Information und Kommunikation revolutioniert. Milliarden Menschen sind online. Deutsche Schüler chatten z.B. mit ICQ und machen Informationen über sich selbst verfügbar z.B. im Schüler VZ. Wo bleibt da die Privatsphäre?

Der Vortrag beginnt mit einer Demonstration, die zeigt, dass beim Chat jeder zuhören kann. Glücklicherweise haben Mathematiker und Informatiker Methoden erfunden, die es erlauben, Chats durch Verschlüsselung geheim zu halten. Wie zum Beispiel das berühmte Diffie-Hellman-Schlüsselaustauschverfahren. Es ermöglicht den Austausch geheimer Schlüssel über eine öffentlich zugängliche Leitung. Klingt unmöglich, ist es aber nicht. Primzahlen spielen dabei eine zentrale Rolle. Problem gelöst? Einstweilen ja! Aber Mathematiker, Informatiker und Physiker sind aktive Leute. Sie haben Pläne für Quantencomputer in der Schublade, die das Diffie-Hellman-Verfahren unsicher machen werden. Das dauert aber noch Jahre. Und was dann?

Was sicher bleibt, wenn es Quantencomputer gibt, zeigt der Vortrag an elektronischen Signaturen. Sie schützen Software-Updates. Ohne diesen Schutz könnte es zu großen Schäden kommen. Außerdem beschreiben die Referenten das Merkle-Signaturverfahren. Es beruht auch auf sehr schönen mathematischen Ideen und hat das Potenzial, sehr lange sicher zu bleiben.

Demos

Erik Tews und Nadja Kokic zeigen, wie man den Chat Client Trilian abhören kann, wie man ihn mit dem Diffie-Hellman-Verfahren absichert, und dass die Schlüssel bei Trilian leider zu klein gewählt wurden. (Entwicklung der Demo: Nadja Kokic)
In einer weiteren Demo zeigen Erik Tews und Elias Most, wie das zukunftssichere Merkle-Signaturverfahren in TLS, dem Internetprotokoll für sichere Verbindungen, funktioniert. (Jugend-forscht-Projekt von Elias Most)

Biographien

Prof. Johannes A. Buchmann, Jahrgang 1953, ist Mitglied der Akademie der Wissenschaften und der Literatur Mainz, der Berlin-Brandenburgischen Akademie der Wissenschaften und der Deutschen Akademie der Technikwissenschaften acatech. Er hat Mathematik, Physik, Philosophie, Pädagogik an der Universität zu Köln studiert, 1982 promovierte er dort im Fach Mathematik und legte 1984 das zweite Staatsexamen ab (Lehramt an Gymnasien). Die Habilitation folgte 1988 in Düsseldorf. Im selben Jahr trat er an der Universität des Saarlandes eine Professur für Informatik an. 1996 folgte er dem Ruf der Technischen Universität Darmstadt, wo er bis heute als Professor für Informatik und Mathematik tätig ist. Seine Spezialgebiete sind die Kryptographie und die Computersicherheit. Von 2001 bis 2007 war er Vizepräsident der TU Darmstadt. 1993 wurde Johannes A. Buchmann mit dem Leibnizpreis der Deutschen Forschungsgemeinschaft ausgezeichnet; 2006 erhielt er den Karl Heinz Beckurts-Preis.

Nadja Kokic, Jahrgang 1981, machte 2000 ihr Abitur in Heilbronn. Seit 2002 studiert sie Informatik mit den Nebenfächern Recht und Psychologie an der TU-Darmstadt. Zu ihren Schwerpunkten im Studium gehört neben Kryptographie auch die IT-Sicherheit.

Elias Most, Jahrgang 1990, besucht seit 2004 das Darmstädter Gymnasium Lichtenbergschule, an dem er in der Jugend-forscht-Arbeitsgruppe Weird Science Club beteiligt ist. Derzeit besucht er die 12. Klasse (Leistungskurse Physik und Mathematik). Er hat dort unter anderem ein Projekt über die Integration quantensicherer Signatur- und Verschlüsselungsverfahren in das TLS Protokoll in Kooperation mit Prof. Buchmann und seinen Mitarbeitern an der TU Darmstadt durchgeführt.

Erik Tews, Jahrgang 1983, legte 2002 sein Abitur ab und studierte bis 2007 Informatik an der TU Darmstadt. Seit 2004 arbeitete er als wissenschaftliche Hilfskraft im Fachgebiet Theoretische Informatik, wo er 2007 seine Diplomarbeit schrieb. Thema war die Entwicklung eines neuen Angriffs auf WEP gesicherte Funknetzwerke, der zurzeit

als der beste Angriff gegen solche Netzwerke gilt. Seit Herbst 2007 arbeitet er als wissenschaftlicher Mitarbeiter an der TU Darmstadt und beschäftigt sich mit angewandter Kryptoanalyse.

Zeit und Ort des Vortrages

Donnerstag, den 19. Juni 2008, von 14.15 Uhr,
im Leibnizsaal der Berlin-Brandenburgischen Akademie der Wissenschaften
(Jägerstraße 22-23, Berlin-Mitte)