idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Clausthal
Jochen Brinkmann

06.09.2000
http://idw-online.de/de/news24091

Buntes aus der Wissenschaft
Mathematik, Physik / Astronomie
regional

Verschlüsselung und Codierung: Datensicherheit durch Mathematik

Am 29. September lädt das Institut für Mathematik der TU Clausthal zu einer Fortbildungsveranstaltung (9.30 Uhr - 16.30 Uhr) für Mathematiklehrerinnen- und lehrer ein. Diese Fortbildung gibt einen für die Schule geeigneten exemplarischen Einblick in die Kryptographie und in die Codierungstheorie.

In der Kryptographie geht es um Methoden, die gestatten, Nachrichten so zu übermitteln, daß ihr Inhalt geheim und unverfälscht den Empfänger erreicht.

Der Vortrag stellt insbesondere das 1977 entwickelte RSA Verschlüsselungsverfahren nach Rivest, Shamir und Adleman sowie dessen zahlentheoretische Grundlagen vor. Eine praktische Erprobung findet in Form von Laborübungen im Rechnerpool des Instituts statt.

Ziel der Codierungstheorie ist es, Fehler in der Übertragung von Daten zu erkennen, möglichst sogar zu korrigieren. Dazu werden die Daten so codiert, daß kleinere Fehler nicht zu Verwechslungen führen können. Mit algebraischen Methoden lassen sich gute Codes konstruieren. In diesem Vortrag wird ein System von Telefonnummern entworfen, das auch bei falscher Wahl von einer Ziffer noch zum richtigen Anschluß führt.

Beide Vorträge verwenden grundlegende Konzepte der Zahlentheorie (Kongruenzen) und Algebra (endliche Körper), die auch auf Schulniveau erarbeitet werden können. Zusätzlich wird ein Ausblick gegeben auf komplexere Analysen und Anwendungen, die als Motivation für die Beschäftigung mit diesem Stoff dienen können.

In den abschließenden Übungen erhalten die Teilnehmer Gelegenheit, sich mit den Problemen aktiv, zum Teil unter Einbeziehung des Computers, auseinander zu setzen und mit den Vortragenden zu diskutieren.

Die Referenten sind Professor Dr. Lutz Lucht und Professor Dr. Walter Klotz, beide Institut für Mathematik der TU Clausthal.

Diese Veranstaltung ist als Lehrerfortbildung von der Bezirksregierung Braunschweig anerkannt. Für die Teilnahme ist Sonderurlaub bei der Schulleitung zu beantragen.

Anmeldung/weitere Informationen:
Dr. H. Behnke
Institut für Mathematik
Erzstraße 1
38678 Clausthal-Zellerfeld
Telefon (05323) 72-3183
Telefax (05323) 72-2304
e-mail:behnke@math.tu-clausthal.de