Mathematics Department University of Fribourg

Vortragsdienst Mathematik

Kryptographie

Mathematik ist die Grundlage aller moderner Verschlüsselungssysteme.

Electronic-Banking soll kinderleicht und absolut sicher sein. Kryptographische Methoden ermöglichen die sichere Übermittlung von Daten beim elektronischen Zahlungsverkehr.

Grundlagen der modernen Methoden liefert die Zahlentheorie, die Theorie kommutativer Gruppen und die algebraische Geometrie.

Auch Codes von **Bank-Karten**, vertrauliche **e-Mails**, der **Schriftverkehr zwischen Regierungen** oder persönliche **medizinische Daten** müssen durch Verschlüsselung vor Dritten geschützt werden.

Die Protokolle von Diffie und Hellman und das RSA-Public Key Verfahren gehören derzeit zu den sichersten Methoden. Doch Quantencomputer könnten bald auch diese Codes knacken. Daher wird schon jetzt nach beweisbar sicheren Verschlüsselungen geforscht.

In der Schweiz werden **elektronische Abstimmungsverfahren** erprobt. Erst kryptographische Verfahren ermöglichen es, die Demokratie aus ihrer elektonischen Wiege zu heben.

Der Vortrag zeigt die Entwicklung der Verschlüsselung von ihren Anfängen bei Spartanern und Römern bis hin zu neusten Techniken.

www.unifr.ch/math

Kontaktadresse
norbert.hungerbuehler@unifr.ch

UNIVERSITAS FRIBURGENSIS

FACULTY OF SCIENCE