Sommersemester 2003

Doz. Dr. D. Burde

Vorlesung: Kryptologie

Dienstag 15:15–16:45, Mittwoch 17:15–18:45, Hörsaal 6

In der Kryptographie geht es um die Techniken mit denen man Daten geheimhalten, Nachrichten elektronisch signieren, den Zugang zu Rechnernetzen kontrollieren, elektronische Geldgeschäfte absichern und einiges mehr kann. In dieser Vorlesung sollen die gängigen kryptographischen Verfahren vorgestellt und ihre mathematischen Grundlagen erläutert werden.

Als Vorkenntnisse werden erwartet: Lineare Algebra (Matrizen, endliche Körper) sowie einige wenige Begriffe der elementaren Zahlentheorie (Kongruenzen, Primzahlen, Teilbarkeitslehre). Wir behandeln folgende Themen:

- **Verschlüsselungsverfahren**

Symmetrische und asymmetrische Verschlüsselung, Public-Key-Kryptographie, RSA, Rabin, Diskreter Logarithmus, Diffie-Hellman, ElGamal

$$n = pq,\ \varphi(n) = (p-1)(q-1), \quad y^t \equiv x^{k\varphi(n)+1} \equiv x \mod n$$

- **Grundlagen aus der elementaren Zahlentheorie**

Teilbarkeit in $\mathbb{Z}$, Fundamentalsatz der Arithmetik, eindeutige Faktorisierung in Hauptidealringen, zahlentheoretische Funktionen, Kongruenzen, Primitivwurzeln

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

- **Primzahltests**

Lucas, Pollard, Solovay-Strassen, Rabin-Miller, Pepin u.a.

$$F(7) = 2^{2^7} + 1 = 34.279.974.696.877.740.253.374.607.431.768.211.457$$

- **Elliptische Kurven**

Affine und projektive Kurven, elliptische Kurven über endlichen Körpern, Schoof-Algorithmus, supersinguläre elliptische Kurven, das Probelm des diskreten Logarithmus für elliptische Kurven.

$$\begin{aligned} p_1 &= (0,0), \\ p_2 &= (1,0), \\ p_{10} &= (161/16, -2065/64) \\ p_{22} &= (51678803961/12925188721, 10663732503571536/1469451780501769) \end{aligned}$$