Christian Nelius

Kryptographie (SS 2011)

Veranstaltungskommentar

XVYXNGTVLXBARMDBYAAITVNMEIDAUFGIFVXSRYDAY
JFXYCYLMPTKBWJMDAYFFGSIZL

Schon vor mehr als 2000 Jahren wurden im militärischen und im diplomatischen Bereich geheimzuhaltende Nachrichten in verschlüsselter Form gesandt und mußten dann vom Empfänger wieder entschlüsselt werden. Eines der ältesten Verfahren geht auf Gaius Julius Caesar zurück. In der heutigen Zeit ist die Verschlüsselung von Daten zum Zwecke ihrer sicheren Übertragung sehr wichtig geworden, man denke nur an den elektronischen Bankverkehr, den Telephonverkeht, an die digitale Unterschrift oder das Passwort für den Zugang zu einem Computer.

In dieser Vorlesung werden neben einigen historischen Verfahren insbesondere moderne Ver- und Entschlüsselungsverfahren behandelt (wie etwa das asymmetrische RSA-Verfahren, der Diffie-Hellman-Schlüsseltausch, die El Gamal-Verschlüsselung oder Shamir's No–Key–Algorithmus), sowie die dafür notwendigen mathematischen Grundlagen. Dabei handelt es sich in erster Linie um zahlentheoretische Ergebnisse, wie z.B. den Satz von Euler und Fermat. Ein wichtiger Punkt ist weiterhin die Frage nach der Sicherheit eines Verschlüsselungsverfahrens. Natürlich werden wir uns auch mit Methoden der unerlaubten Entschlüsselung von Geheimtexten beschäftigen.

Am Ende des Semesters können wir dann den obigen Geheimtext entschlüsseln.

Literaturangabe: Albrecht Beutelspacher: "Kryptologie", Vieweg-Verlag

Hörerkreis: G,H,R,Ges

Prüfungsgebiet: Hauptstudium

Scheinerwerb: Aktive Teilnahme an den Übungen, Berabeitung von Übungsaufgaben, Klausur

vorausgesetzte Kenntnisse: Grundlagen der Zahlentheorie

Vorbesprechung: 1. Vorlesungstermin