



Universität Karlsruhe (TH)

Fakultät für Informatik
*Institut für Algorithmen und
Kognitive Systeme*

Prof. Dr. Th. Beth
Dr. Jörn Müller-Quade
Dipl.-Inform. S. Röhrich
Dipl.-Inform. D. Unruh

Am Fasanengarten 5
Postfach 69 80
D-76128 Karlsruhe

Telefax: +49 721 608 55022

Seminar im Sommersemester 2005

Kryptographische Protokolle in Theorie und Anwendung

Kryptographische Protokolle erlangen durch die immer weitreichendere Nutzung offener Netzwerke eine wachsende Bedeutung. In diesem Seminar sollen einige gebräuchliche Protokolle näher vorgestellt und daraufhin untersucht werden, ob sie aus Sicht der theoretischen Kryptographie sicher sind und inwieweit theoretische Sicherheitslücken Praxisrelevanz haben können.

Es ist geplant, daß in jedem Vortrag zuerst ein Seminarteilnehmer ein gängiges Protokoll vorstellt und danach dessen Eigenschaften in obigem Sinne diskutiert werden.

Mögliche Vortragsthemen sind u. a.:

- SSL/TLS
- SSH
- IPSec, insbesondere IKE
- DNSSec
- SET
- Bluetooth
- S/MIME, OpenPGP
- Formate: PKCS (am Beispiel Elster), X.509 und ähnliche

Das Seminar richtet sich an Studenten der Informatik, Mathematik, Physik und verwandter Fächer im Hauptstudium. Grundlegende kryptographische Kenntnisse, z. B. aus den Vorlesungen Public-Key-Kryptographie und Signale, Codes, Chiffren II werden empfohlen.

Anmeldung: per E-Mail oder persönlich

Vorbesprechung: Mittwoch, 13. April 2005, um 13¹⁵ Uhr im Seminarraum 252.

Fragen bitte richten an:

Jörn Müller-Quade (Zi. 238, 608-4327), Stefan Röhrich (Zi. 230, 608-4025), Dominique Unruh (Zi. 238, 608-6287) im Informatik-Neubau.

E-Mail: {muellerq, sr, unruh}@ira.uka.de

WWW: <http://iaks-www.ira.uka.de/home/roehrich/lehre/ss2005/seminar-krypta/>