

Proseminar Kryptographie und Datensicherheit

Wintersemester 2004



Christoph Kreitz / Eva Richter

{kreitz,erichter}@cs.uni-potsdam.de

<http://www.cs.uni-potsdam.de/ti/lehre/04-Kryptographie>



1. Ziele der Veranstaltung
2. Organisatorisches
3. Themenvergabe

LERNZIEL: PRÄSENTATION

- **Verständlicher Vortrag zu einem Thema**
 - Auswahl der **wichtigsten Punkte** aus einem Text
 - Verwendung geeigneter **visueller Hilfsmittel**
 - Wenn nötig Ergänzung durch Sekundärquellen
- **Inhaltliche Kompetenz**
 - **Kenntnis von Details**, die nicht präsentiert werden
 - Beantwortung von Rückfragen
 - Leitung einer inhaltlichen Diskussion
- **Schriftliche Abhandlung eines Themas**
 - Prägnante Darstellung in **lesbarer Form**
 - Kurzfassung (Abstract) + Themenausarbeitung + Quellenangaben

Die Verschlüsselung von Nachrichten ist seit über 2500 Jahren ein bewährtes Mittel zur sicheren Übermittlung von Informationen. Kryptographische Verfahren sollen sicherstellen, daß geheime Informationen nicht decodiert werden koennen und daß die Authentizität von Nachrichten überprüfbar wird.

Im Seminar sollen **die wichtigsten Verfahren** der Vergangenheit und Gegenwart sowie **ihre mathematischen Grundlagen** ausführlich betrachtet werden.

● Kreditpunkte: 3

- Verbindliche Anmeldung bis 5.11.

● Termin

- Wöchentlich **Dienstags 15.15-16.45**
- Einführung in die Thematik im Anschluß
- **Teilnehmervorträge ab 19. Oktober**

● Hauptquelle

- **Douglas R. Stinson *Cryptography: Theory and Practice***
- Zusätzliche Quellen sollten mit einbezogen werden

● Sprechstunden

- C. Kreitz: **Do 15:30–16:30** ..., und immer wenn die Türe offen ist
- E. Richter: **Di 13:00–15:00** ..., und immer wenn die Türe offen ist

ERFOLGSKRITERIEN

“Sie können bei uns über alles reden,
nur nicht über eine Stunde”

- **Vortrag – 60 Minuten inkl. Zwischenfragen**
 - Vortrag spätestens 1 Woche vorher kurz mit Frau Dr. Richter besprechen
 - Vortragsfolien spätestens 2 Tage vorher elektronisch einreichen
 - **Inhaltliche Diskussionsleitung**
 - **Schriftliche Ausarbeitung**
 - 8–10 Seiten, spätestens bis zum 3. Februar 2005 einzureichen
 - **Anwesenheit in allen Sitzungen**
 - Aktive Teilnahme an der inhaltlicher Diskussion
 - Inhaltliche und didaktische Manoeuverkritik
- Unentschuldigte Abwesenheit ist eine Beleidigung für die Vortragenden

THEMENVERGABE

- **Vorrang für Teilnehmer ohne Proseminar**
 - Ziel des Proseminars ist Vortragen und Ausarbeiten zu lernen
 - Der Inhalt ist nachrangig
- **Danach: Auswahl nach Listenplatz**
 - Wir haben nur 14 Themen
 - Erstes Thema ist das leichteste, aber nur 1 Woche Vorbereitung
- **Für alle anderen**
 - **Vorlesung mit gleichem Thema im nächsten Semester**

EINZELTHEMEN

- Einfache kryptographische Systeme (§1.1) 19.10.
- Kryptoanalyse (§1.2) 26.10.
- Datensicherheit und Shannon's Theorie (§2) 2.11.
- Block Codes (§3.1-4) 09.11.
- Die Verschlüsselungsstandards DES & AES (§3.5/6) 16.11.
- Kryptographische Hash Funktionen (§4.1-3) 23.11.
- Message Authentication Codes (§4.4/5) 30.11.
- Public-key Kryptographie mit dem RSA Schema (§5.1-3) 07.12.
- Primzahltests und Faktorisierung (§5.4-6) 14.12.
- Attacken auf RSA, Rabin's Kryptosystem (§5.7-9) 04.01.
- Public-key Kryptographie mit diskreten Logarithmen (§6.1-3) 11.01.
- Sicherheit von ElGamal Systemen (§6.5-7) 18.01.
- Digitale Unterschriften (§7.1-4) 25.01.
- Nachweislich sichere Signatursysteme (§7.5-7) 01.02.