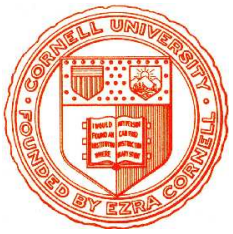
Seminar Kryptographie und Datensicherheit

Wintersemester 2006/07



Christoph Kreitz

kreitz@cs.uni-potsdam.de

http://www.cs.uni-potsdam.de/ti/lehre/06-Kryptographie

1. Ziele der Veranstaltung
2. Organisatorisches
3. Themenvergabe

Seminarthema

Die Verschlüsselung von Nachrichten ist seit über 2500 Jahren ein bewährtes Mittel zur sicheren Übermittelung 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.

Lernziele

- **Verständliche Präsentation von Wissenschaft**
  - Auswahl der wichtigsten Punkte aus einem wissenschaftlichen Text
  - Selbständige Ergänzung durch Sekundärquellen
  - Vortrag unter Verwendung geeigneter visueller Hilfsmittel
  - Leitung einer inhaltlichen Diskussion
  - Kompetente Beantwortung von Rückfragen
- **Inhaltlich: Kryptographie & Datensicherheit**
  - Verständnis der wichtigsten Verfahren
  - Gutes Verständnis der mathematischen Grundlagen
  - Verständnis von Stärken und Schwächen verschiedener Methoden

  ... aufgrund von Vorträgen und Literaturquellen

Konkrete Themen

• * Einfache kryptographische Systeme und ihre Analyse	(§1)	26.10.2006
• Datensicherheit und Shannon's Theorie	(§2)	02.11.2006
• Block Codes (incl. DES & AES)	(§3:1-6)	09.11.2006
• Kryptographische Hash Funktionen	(§4:1-3)	16.11.2006
• Message Authentication Codes	(§4:1,4,5)	23.11.2006
• Public-key Kryptographie mit dem RSA Schema	(§5:1-3,7-9)	30.11.2006
• Primzahltests und Faktorisierung	(§5:4-7)	07.12.2006
• ElGamal Systeme	(§6:1-2,6-7)	14.12.2006
• Public-key Kryptographie mit Diskreten Logarithmen	(§6:1-4)	11.01.2007
• Elliptische Kurven	(§6:4-5)	18.01.2007
• Digitale Unterschriften mit ElGamal	(§7:1-4)	25.01.2007
• Andere Protokolle für digitale Unterschriften	(§7:5-7)	01.02.2007

Kapitelnummern beziehen sich auf Douglas R. Stinson *Cryptography: Theory and Practice*

Rahmenbedingungen

- **Nur aktive Teilnahme möglich**
  - Aktiv $\equiv$ eigener Vortrag als selbständige Leistung
  - **Maximal 22 Teilnehmer** (2 pro Thema)

    Im Zweifel Entscheidung durch Losverfahren
- **Vorträge – 75 Minuten inkl. Zwischenfragen**
  - Zentrale Aspekte des Themas ausführlich vorstellen und illustrieren
  - Hintergrundmathematik muß gründlich erklärt werden
  - Buchkapitel dient als Leitline, reicht aber nicht aus
  - Zusätzliche Quellen selbständig aufsuchen, einbeziehen, und zitieren
  - Vortrag muß (auch bei Überlappungen) in sich abgeschlossen sein
  - Leitung einer inhaltlichen Diskussion
  - Vortragsfolien spätestens 2 Tage vorher elektronisch einreichen
- **Alle Teilnehmer: Anwesenheit in allen Sitzungen**
  - Aktive Teilnahme an der inhaltlicher Diskussion

  Unentschuldigte Abwesenheit ist eine Beleidigung für die Vortragenden

Leistungsbewertung

- **Qualität des Vortrags** 50%
  - Wurde das Thema verständlich und anschaulich dargestellt?
  - Hat der Vortrag hinreichende Tiefe?
  - Kann auf Rückfragen eingegangen werden?
- **Qualität der schriftlichen Ausarbeitung** 50%
  - Spätestens bis zum Mitte Februar 2007 elektronisch (PDF) einreichen
  - 8–10 Seiten
  - Korrekte und verständliche Darstellung des Themas
  - Quellennachweis
  - Textliche/sprachliche Qualität zählt auch !
- **Aktive Teilnahme an der Diskussion**
  - Aufmerksames zuhören (Laptops bitte geschlossen halten)
  - Fragen stellen / Feedback geben
  - Mehrmalige unentschuldigte Abwesenheit führt zur Abwertung