Informationen zum Seminar „IT-Sicherheit“ des Lehrstuhls für Kommunikationssicherheit

Wichtige Termine

Mo. 05.11.2007, 17h: Vorbesprechung in Raum IC 4/161
Mo. 18.02.2008: Endgültige Abgabe der schriftlichen Ausarbeitung
Mo. 10.03.2008, 10-15h: Präsentationen aller Seminarteilnehmer in IC 4/39

Allgemeine Hinweise
Im Rahmen des Seminars wird es dieses Jahr ensprechend zwei Überthemen geben:

1. **„Cryptography and Security in Banking“** (s. Seite 2),
2. **„Alternative Cryptology“** (s. Seite 3)

Außerdem ist zusätzlich zur schriftlichen Ausarbeitung und der Präsentation ein Wikipedia-Eintrag in englischer Sprache fester Bestandteil der Seminarleistung.

Templates für die schriftliche Ausarbeitung und die Vortrags-Folien sind unter www.crypto.rub.de verfügbar. Dort findet ihr auch einige von uns zusammengestellte Tipps, u.a. zum Schreiben in englischer Sprache und dem Halten von Vorträgen.

Vorbesprechung
Während der Vorbesprechung stellen die Betreuer ihre Themen kurz vor. Anschließend werden die Themen (und damit auch die Betreuer) Interessenten zugeordnet. Wenn sich mehrere Interessenten für ein Thema finden, entscheidet das Los.

Schriftliche Ausarbeitung
Die Ausarbeitung soll in Latex angefertigt werden, einen Umfang von ca. 15 Seiten haben und in englischer Sprache geschrieben sein (deutsch nur in Ausnahmefällen). Alle Ausarbeitungen werden auf unserer Webseite veröffentlicht. Wer sich noch nie mit Latex befasst hat findet unter de.wikipedia.org/wiki/LaTeX viele nützliche Hinweise.
Achtung: wer seine Ausarbeitung nicht bis zum 18. Februar seinem Betreuer per eMail geschickt hat bekommt keinen Seminarschein!

Wikipedia-Eintrag
Eine Kurzfassung (ca. eine DIN-A4 Seite, auf jeden Fall in englisch) der schriftlichen Ausarbeitung soll ins englische Wikipedia eingepflegt werden. Dazu bitte einen Benutzernamen anlegen und alle Änderungen mit diesem Benutzernamen vornehmen. Als weiterführende Literatur bitte stets eure Seminarausarbeitung angeben, die auf unserer Webseite unter http://www.crypto.rub.de/its_seminar_ws0708.html verfügbar ist. In die Revision-History bitte stets das folgende Kommentar eingeben: „This contribution is a result of the seminar 'Cryptography and Security in Banking'/'Alternative Cryptology' which was held at the chair for communication security at the Ruhr-University Bochum, Germany“.

Präsentation der Ergebnisse
Die Abschluß-Präsentation setzt sich aus 20 Minuten Vortrag und anschließenden 5 Minuten für Fragen zusammen. Bitte mit eurem Betreuer einen Termin für den Probevortrag absprechen. Auf den Folien bitte unbedingt den Weblink für den Wikipedia-Eintrag angeben.

Sollten noch Fragen bestehen, einfach eine eMail mit Betreff „Seminar-0708“ an abogdanov@crypto.rub.de schreiben.

Themenliste zum Thema „Cryptography and Security in Banking“ (Seminar „IT-Sicherheit“)

Thema	Betreuer	Interessent
Kommunikation und Kryptographie von Geldautomaten	Andrey Bogdanov	Renuli
Wie funktioniert die Geldkarte? Wie sicher ist die Geldkarte?	Thomas Eisenbarth	Klose
Ebanking Vulnerabilities	Tim Güneysu	Borrmann
Smart Card als Zahlungswerkzeug	Timo Kasper	Welz

Themenliste zum Thema „Alternative Cryptology“ (Seminar „IT-Sicherheit“)

Thema	Betreuer	Interessent
Cryptography on Trace-Zero Varieties	Andrey Bogdanov	Wienecke
Multivariate Polynomial Based Cryptography	Thomas Eisenbarth	Kluge
Quantum Cryptography	Timo Kasper	Silbermann
Identity-Based Cryptography	Axel Poschmann	Oswald