

Proseminar „Kryptographie“ im Sommersemester 2006

Wann und wo?

Das Proseminar findet jeweils montags von 12.15 Uhr bis 13.45 Uhr statt, und zwar in der Otto-Hahn-Str. 14, Raum 304.

Wann geht's los?

Das neue Semester (genauer: die Vorlesungszeit) beginnt am 3. April. Die Vorlesungszeit hat nur 12 Montage, wir haben 10 Vorträge, also beginnen wir am 24. April mit den Vorträgen.

Du möchtest gerne an dem Proseminar mit einem eigenen Vortrag teilnehmen? Dann die folgenden Informationen bitte per email (s.u.) an mich:

Vorname: _____ Familienname: _____

Matrikelnummer: _____

email-Adresse: _____

Schließlich die Information, für welche Proseminarthemen Du Dich interessierst. (Themen siehe Rückseite). Bitte mindestens drei Themen auswählen und mit einer Priorität von 1 bis 3 versehen:

1 = sehr gerne, 2= gerne, 3=auch nicht schlecht

(Es dürfen also auch z.B. mehrere mit Priorität 1 versehen werden.)

Hinweis: Die Dauer jedes Vortrags soll zwischen 1 Stunde 15 und 1 Stunde 30 liegen. Es wird erwartet, dass die Vortragenden zuhause ihren Vortrag probekalten, damit dieses Zeitlimit eingehalten wird.

Infos zum Proseminar (wie z.B. die Verteilung der Teilnehmer/innen auf die Vorträge):
<http://Ls2-www.cs.uni-dortmund.de/lehre/sommer2006/pro-krypto/>

Für die Themenliste das Blatt bitte wenden!

Bitte die Informationen bis zum Freitagabend, 17. Februar, elektronisch übermitteln an: th01 AT Ls2.cs.uni-dortmund.de

In der Vorbesprechung habe ich Kopien der Inhaltsverzeichnisse aus drei Kryptographiebüchern verteilt sowie zu jedem Thema die ersten beiden Seiten aus dem „Wätjen-Buch“. (Für genaue Referenzen siehe die Webseite zum Proseminar). Das soll Euch dabei helfen, herauszufinden, welche der Themen für Euch von Interesse sein könnten. (Googeln hilft auch !)

Da Thema Nummer 10 in einem Extrabuch (von Wayner) behandelt wird, dort die einleitenden Seiten aus diesem Buch stattdessen.

Thema	Kap. im Stinson-Buch	Kap. im Wätjen-Buch	Kap. im Buchmann-Buch
01.) Grundlagen der Kryptographie	1-2	1-2	3
02.) Rijndael/AES	-	12	-
03.) RSA und Angriffe	4	5	7.2/7.3
04.) Kryptographische Hashfunktionen	7	6	10
05.) Digitale Signaturen	6	7	11
06.) Schlüsselaustausch und Zertifikate	8	8	-
07.) Kryptographische Protokolle	-	10	-
08.) Secret Sharing	11	-	-
09.) Zero-Knowledge	13	11	-
10.) Disappearing Cryptography/Steganographie	eigenständiges	Buch von Peter Wayner	

Die Proseminarteilnehmerzahl ist 20. Die insgesamt 10 Vorträge werden daher jeweils von zwei Studierenden in Zusammenarbeit gehalten werden.

Gewünscht ist, dass die Vorträge per Beamer gehalten werden. Ein Notebook sowie ein Beamer für die Präsentationen steht jeweils zur Verfügung. Die Dateien zu den Präsentationen werden anschließend in einem allen Teilnehmern zugänglichen Webverzeichnis gesammelt.

Eine Besprechung der Vortragenden mit mir im Vorfeld des Vortrags ist erwünscht. Es empfiehlt sich, mir ca. 1-2 Wochen vor dem Vortrag eine vorläufige Version des Vortrags per email zuzusenden sowie einen Termin mit mir zu vereinbaren, damit bei Änderungswünschen noch genügend Zeit verbleibt, diese in die Tat umzusetzen.

Viel Spaß beim Proseminar!

Thomas Hofmeister