

Am 2. Oktober 2000 hat die US-Standardisierungsbehörde NIST den Sieger in einem dreijährigen Wettbewerb um den neuen Krypto-Standard verkündet: **Rijndael**, entworfen von den beiden belgischen Kryptologen Joan Daemen und Vincent Rijmen. In den nächsten Jahren wird dieses System als AES (Advanced Encryption Standard) in der kommerziellen Kryptographie eine zentrale Rolle spielen; natürlich werden andere Kryptosysteme wie RSA und elliptische Kurven weiterhin ihre Bedeutung behalten.

Dieses eintägige Seminar am

Freitag, 12. April 2002

wendet sich an Manager und Entwickler von kommerziellen Kryptosystemen und an Forscher, die dieses neue System kennen lernen wollen. Professor Rijmen wird persönlich zwei Vorträge halten. Spezielle Vorkenntnisse sind nicht erforderlich.

In Vorträgen wird der Hintergrund dargestellt, das System im Detail erklärt, und die Möglichkeit zum Experimentieren gegeben, in einer Softwareumgebung und eventuell auch in Hardware. Das Seminar findet im Informatik-Gebäude der Universität Paderborn statt. Das direkt daneben liegende Heinz Nixdorf MuseumsForum beherbergt das größte Computermuseum Deutschlands. Es wird Gelegenheit zum Besuch des

Museums geboten, individuell und auch mit Führung, und anschließend zum gemeinsamen Abendessen.

Die Arbeitsgruppe „Algorithmische Mathematik“ im Fachbereich Mathematik, Informatik der Universität Paderborn ist am NRW-Forschungsverbund „Sicherheit in der Informationstechnologie“ beteiligt und veranstaltet das Seminar.

Programm

09 ⁰⁰ –09 ¹⁰	Begrüßung
09 ¹⁰ –10 ¹⁰	VINCENT RIJMEN: AES — The selection process
10 ²⁰ –10 ⁴⁵	JOACHIM VON ZUR GATHEN: Grundlagen der Rijndael Funktionen
10 ⁴⁵ –11 ¹⁵	Kaffee
11 ¹⁵ –12 ⁰⁰	VINCENT RIJMEN: Design philosophy of Rijndael
12 ⁰⁰ –13 ⁴⁵	Mittagessen
13 ⁴⁵ –14 ³⁰	VOLKER KRUMMER: Der SQUARE Angriff
14 ³⁰ –15 ²⁰	JOACHIM VON ZUR GATHEN: Sicherheitsaspekte von Rijndael
15 ²⁰ –15 ⁵⁰	Kaffee
15 ⁵⁰ –16 ³⁰	AG Algorithmische Mathematik: Experimentieren mit Rijndael

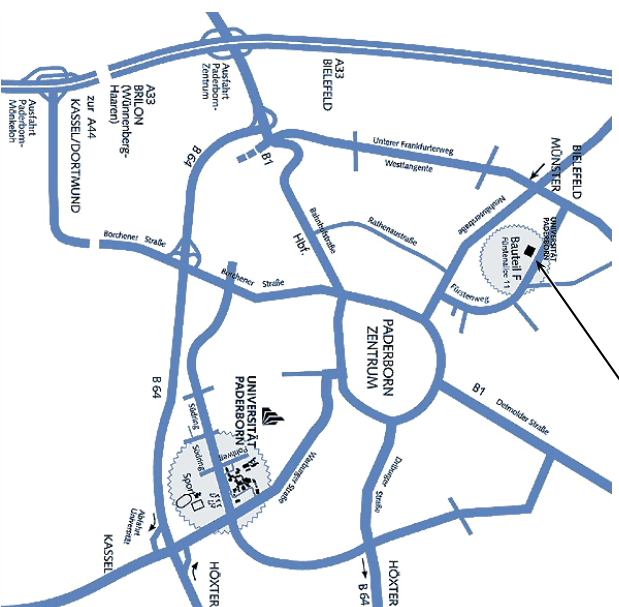
Anmeldung

Die Teilnahmegebühr beträgt 250 €, und für Universitätsangehörige 25 €. Anmeldungen bitte bis 4. April 2002 an:

Sekretariat „Algorithmische Mathematik“
Prof. Dr. Joachim von zur Gathen
Fachbereich Mathematik, Informatik
Universität Paderborn
D-33095 Paderborn, Germany
Tel.: +49-5251-603068
Fax: +49-5251-603516
Email: crypto@upb.de

Tagungsort

Seminar Rijndael



Universität Paderborn
Raum E.3.327
Warburger Strasse
33098 Paderborn

Weitere Informationen und Links zu
Übernachtungsmöglichkeiten und Ver-
kehrverbindungen finden Sie über unsere
Webseite.

<http://www-math.upb.de/~aggathen/rijndael/>

Seminar Rijndael

12. April 2002

<http://www-math.upb.de/~aggathen/rijndael/>

veranstaltet durch



Universität Paderborn

Fachbereich Mathematik & Informatik

Arbeitsgruppe Algorithmische Mathematik

Joachim von zur Gathen

in Zusammenarbeit mit



NRW Forschungsverbund Datensicherheit

Gefördert durch das Ministerium für
Schule, Wissenschaft und Forschung des
Landes Nordrhein-Westfalen