

Am 2. Oktober 2000 hat die US-Standardisierungsbehörde NIST den Sieger in einem drei-jährigen 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, 29.06.2001

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 beinhaltet 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 veranstaltet das Seminar. Diese Arbeitsgruppe ist am NRW-Forschungsverband „Sicherheit in der Informationstechnologie“ beteiligt.

Programm

09 ⁰⁰ –09 ¹⁰	Begrüßung
09 ¹⁰ –10 ¹⁰	VINCENT RIJMEN: AES — The selection process
10 ²⁰ –11 ⁰⁰	JOACHIM VON ZUR GATHEN: Grundlagen der Rijndael Funktionen
11 ⁰⁰ –11 ³⁰	Kaffee
11 ³⁰ –12 ²⁰	VINCENT RIJMEN: Design philosophy of Rijndael
12 ²⁰ –14 ⁰⁰	Mittagessen
14 ⁰⁰ –14 ⁵⁰	JOACHIM VON ZUR GATHEN: Sicherheitsaspekte von Rijndael
15 ⁰⁰ –16 ³⁰	AG Algorithmische Mathematik: Experimentieren mit Rijndael
16 ³⁰ –17 ⁰⁰	Kaffee
17 ⁰⁰	Führung durchs Heinz Nixdorf MuseumsForum

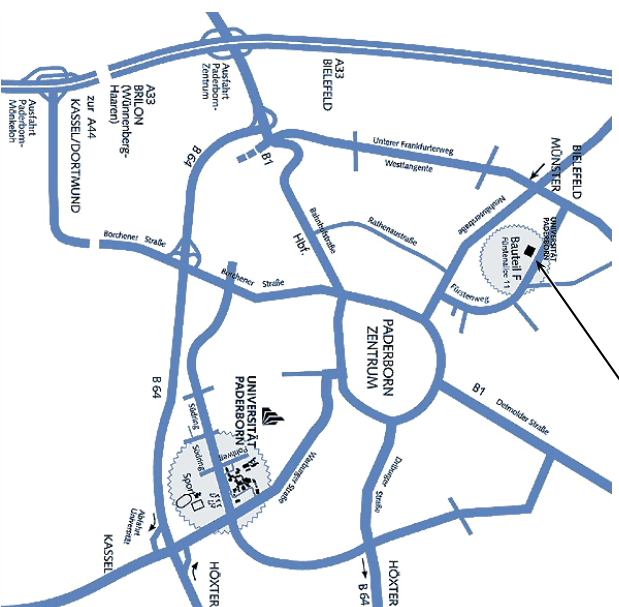
Anmeldung

Die Teilnahmegebühr beträgt DM 400,00; Teilnehmer aus dem akademischen Bereich erhalten eine Rückerstattung. Anmeldungen bitte bis 15. Juni 2001 an:

Sekretariat „Algorithmische Mathematik“
Prof. Dr. Joachim von zur Gathen
Fachbereich Mathematik, Informatik
Universität Paderborn
D-33095 Paderborn, Germany
Tel.: +49/5251/603069
Fax: +49/5251/603516
Email: crypto@upb.de

Tagungsort

Seminar Rijndael



Universität Paderborn
Informatik-Gebäude (Bauteil F)
Raum F0.530
Fürstenallee 11
33102 Paderborn

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

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

Seminar Rijndael

29. Juni 2001

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

veranstaltet durch



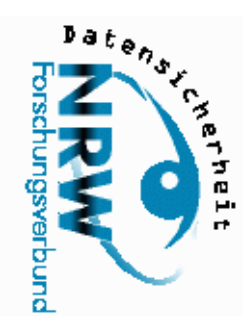
Universität Paderborn

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