EIDMA/DIAMANT Cryptography Working Group

Friday May 4, 2007

Regardz Meeting Center La Vie
Lange Viestraat 351, Utrecht

See http://www.lavie.nl/ (Contact en route) for a route description and information about parking possibilities.

PROGRAM

10.45 – 11.30 hrs. **Dirk Verkerk** (Ministerie van Defensie),
On “New message differences for MD4”.
Paper presented by Sasaki, Wang, Ohta en Kunihiro at FSE 2007.

11.30 - 11.45 hrs. *Coffee / tea break.*

11.45 - 12.30 hrs. **Wil Michiels** (Philips),
White-box cryptography.

12.30 - 14.00 hrs. *Lunch break (lunch not included).*

14.00 - 14.45 hrs. **Ellen Jochemsz** (TU/e),
Attacks on RSA variants using small roots of polynomials.

14.45 - 15.00 hrs. *Coffee / tea break.*

15.00 - 15.45 hrs. **Ebo van der Laan** (NBV),
Steganography: security vs capacity.

Dates of the seminar in 2007:
February 2, May 4, October 5, and December 7.

EIDMA, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Telephone: +31 40 247 3121, Telefax: +31 40 243 5810, E-mail: eidma@tue.nl, http://www.win.tue.nl/math/eidma