Mikulášská kryptobesídka / SantaCrypt 2009

http://mkb.buslab.org/

Pořádá TNS, a.s., a BUSLab za podpory / Organized by TNS, a.s. and BUSLab with support of

Program

3. prosince 2009 (čtvrtek) / December 3, 2009 (Thursday)

9:00 –	*Registrace / Registration*
10:00 – 10:10	*Zahájení workshopu / Workshop opening*
10:10 – 11:20	*Keynote* Kenny Paterson – Cryptography and secure channels
11:20 – 12:20	Jiří Kůr & Petr Švenda – Improving Resiliency of JavaCard Code Against Power Analysis
12:30 – 13:45	*Oběd / Lunch*
13:45 – 14:55	*Keynote* Otokar Grošek – Latin squares and cryptography
14:55 – 15:30	KEYMAKER (student competition) presentations I: Stefan Köpsell – Secure logging of retained data
15:30 – 16:00	*Přestávka na kávu a čaj / Coffee & tea break*
16:00 – 17:00	KEYMAKER (student competition) presentations II: Petr Švenda – Evolutionary Design of Secrecy Amplification Protocols... Jan Krhovják – Generating Random and Pseudorandom Sequences...
17:00 – 17:30	*Rump session*
17:30 –	*Večeře / Dinner*

Následují neformální diskuze v prostorách vyhrazených pouze pro účastníky kryptobesídky. / Followed by informal discussions in the hall available only to the workshop participants.

Mikulášská kryptobesídka / SantaCrypt 2009

http://mkb.buslab.org/

Pořádá TNS, a.s., a BUSLab za podpory / Organized by TNS, a.s. and BUSLab with support of

4. prosince 2009 (pátek) / December 4, 2009 (Friday)

8:55 – 9:00	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:00 – 10:10	*Keynote* Danilo Gligoroski &Vlastimil Klima – Hašovací funkce: SHA-3 & Blue Midnight Wish
10:10 – 10:40	*Přestávka na kávu a čaj / Coffee & tea break*
10:40 – 11:50	*Keynote* Pavel Vondruška – Vývoj kryptografických zařízení v ČS(S)R
11:50 – 12:20	KEYMAKER (student competition) III: Jiří Kůr – Evoluční návrh strategií útoku Vojtěch Brtník – Rekonstrukce šifrovacího stroje ŠD-2
12:22 –	*Mikuláš – přináší Microsoft / Santa supported by Microsoft*

Závěr workshopu... / Workshop ends...