Mikulášská kryptobesídka / SantaCrypt 2011

http://mkb.buslab.org/

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

Program

1. prosince 2011 (čtvrtek) / December 1, 2011 (Thursday)

9:00 –	*Registrace / Registration*
10:00 – 10:10	*Zahájení workshopu / Workshop opening*
10:10 – 11:20	*Keynote* Chris Mitchell – New architectures for identity management – removing barriers to adoption
11:20 – 12:30	*Keynote* Graham Steel – Attacking and Fixing PKCS#11 Security Tokens
12:30 – 14:00	*Oběd / Lunch*
14:00 – 14:45	Klaus Schmeh – The Voynich Manuscript: The Book No-one Can Read
14:45 – 15:05	KEYMAKER (student competition) presentations I: Jan Hajný & Zdeněk Martinásek – Cryptographic System for Identity Protection
15:05 – 15:35	*Přestávka na kávu a čaj / Coffee & tea break*
15:35 – 16:15	KEYMAKER (student competition) presentations II: Viliam Hromada – Fault analysis of stream ciphers Radoslav Čagala – Algebraic cryptanalysis of GOST
16:15 – 16:55	*Rump session*
17:00 –	*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 2011

http://mkb.buslab.org/

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

2. prosince 2011 (pátek) / December 2, 2011 (Friday)

8:55 – 9:00	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:00 – 10:00	*Keynote* Viktor Fischer – Pokroky v generování náhodných čísel pro kryptografii
10:00 – 10:20	KEYMAKER (student competition) III: Martin Košdy – Útoky postrannými kanálmi na systémy založené na EC
10:20 – 10:50	*Přestávka na kávu a čaj / Coffee & tea break*
10:50 – 11:35	*Keynote* Pavel Vondruška – Šifry používané československými osobnostmi
11:35 – 12:20	*Keynote* Jozef Kollár – Československé šifry z obdobia 2. svetovej vojny
12:22 –	*Mikuláš... / Santa...*

Závěr workshopu... / Workshop ends...