Mikulášská kryptobesídka / SantaCrypt 2016

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU, Podpora NetSuite / Organized by TNS, a.s. and CROCS MU, Support by NetSuite

Programme

1. prosince 2016 (čtvrtek) / December 1, 2016 (Thursday)

9:00 –	*Registrace / Registration*
9:55 – 10:00	*Zahájení workshopu / Workshop opening*
10:00 – 11:00	*Keynote* Ueli Maurer: Constructive Cryptography
11:00 – 12:00	*KEYMAKER I* Jakub Klemsa: Exploiting Linearity in Chow's WBAES with Side-Channel Attack Tools Radovan Bezák: µEliece: a lightweight QC-MDPC McEliece cryptosystem
12:00 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Krzysztof Pietrzak: Memory-Hard Functions
14:30 – 14:55	*KEYMAKER II* Michala Gulášová: Steganalysis of StegoStorage
14:55 – 15:30	*Přestávka na kávu a čaj / Coffee & tea break*
15:30 – 16:20	Petr Švenda: The Million-Key Question – Investigating the Origins of RSA Public Keys
16:20 – 16:50	*KEYMAKER III* Matúš Nemec: RSA key generation in cryptographic libraries
16:50 – 17:22	*Rump session*
17:30 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2016

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS MU, Podpora NetSuite / Organized by TNS, a.s. and CROCS MU, Support by NetSuite

2. prosince 2016 (pátek) / December 2, 2016 (Friday)

9:00 – 9:10	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:10 – 10:10	*Keynote* Tomáš Rosa: Zranitelnosti radionavigací typu GPS
10:10 – 10:45	*Přestávka na kávu a čaj / Coffee & tea break*
10:45 – 11:45	*KEYMAKER IV* Tomáš Sovič: Comparison of selected rotor ciphers Radka Cieslarová: An impact of cryptographic function's blocks on the randomness properties Lukáš Hellebrandt: URI-based HBAC in FreeIPA
11:45 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...