Mikulášská kryptobesídka / SantaCrypt 2019

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS FI MU / Organized by TNS, a.s. and CROCS FI MU

Programme

5. prosince 2019 (čtvrtek) / December 5, 2019 (Thursday)

9:00 –	*Registrace / Registration*
9:44 – 9:45	*Zahájení workshopu / Workshop opening*
9:45 – 10:45	*Keynote* Bart Preneel: Post-Snowden cryptography
10:45 – 11:55	*KEYMAKER I* Jakub Klemsa: Security Notions for the VeraGreg Framework and Their Reductions Matěj Grabovský: Usability Insights from Establishing TLS Connections Ondřej Kupka: Building an Enigma simulator with Lego Technic
12:00 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Christian Cachin: Consensus with Asymmetric Trust
14:30 – 15:00	*KEYMAKER II* Martin Ukrop: Will You Trust This TLS Certificate?
15:00 – 15:30	*Přestávka na kávu a čaj / Coffee & tea break*
15:30 – 16:30	*Keynote* Eli Biham: Breaking the Bluetooth pairing – or How a Minor Detail Affects a Major Protocol?
16:30 – 17:22	*Rump session*
17:30 –	*Večeře / Dinner*

Mikulášská kryptobesídka / SantaCrypt 2019

http://mkb.tns.cz/

Pořádá TNS, a.s., a CROCS FI MU / Organized by TNS, a.s. and CROCS FI MU

6. prosince 2019 (pátek) / December 6, 2019 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	*Keynote* Eugen Antal & Otokar Grošek: O šifrách, ktoré sa používali počas „Slovenského štátu“
10:05 – 10:35	*Přestávka na kávu a čaj / Coffee & tea break*
10:35 – 11:55	*KEYMAKER III* Jakub Machovec: Lúštenie šifrovanej korešpondencie Marie Antoinetty Peter Švec: Video Steganography Based on Synchronization Timestamps Michal Firča: Porovnanie metód identifikácie samohlások v texte a ich využitie pri lúštení klasických šifier Ľubor Pernický: Integrácia postkvantovej kryptografie do Android aplikácie
11:55 –	*Mikuláš / Santa*

Závěr workshopu... / Workshop ends...