Mikulášská kryptobesídka - Předběžný program

10. prosince 2001 (Pondělí)
Pizzeria PIZZA IL CARNE, Seydlerova 2148/9, Praha 13

15:00 - 16:00 Registrace
16:00 - 18:00 Panel discussion "Cryptography - from standards to applications"

Panelists: Tonda Beneš, SAP, Czech Rep.
Julien Marcil, RSA Security, UK
Vašek Matyáš, ecom-monitor.com a FI MU Brno, Czech Rep. - moderator
Fabien Petitcolas, Microsoft Research Cambridge, UK
Vladimír Pračke, Eracom Technologies, Czech Rep.
Bart Preneel, Katholieke Universiteit Leuven, Belgium

Následuje série neformálních diskuzí v prostorách pizzerie, která je vyhrazena pouze pro účastníky kryptobesídky.

11. prosince 2001 (Úterý)
Školící středisko SAP, Pekařská 621/7, Praha 5 - Stodůlky

8:00 - 8:55 Registrace
9:00 - 9:15 Uvítání účastníků

Nové algoritmy a postupy

9:15 - 10:00 Bart Preneel, Katholieke Universiteit Leuven, Belgium - New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report
Prostor pro diskuzi k tématu

± 10:15 - 10:35 Karel Burda, VA Brno - AES a jeho implementace
Prostor pro diskuzi k tématu

± 10:50 - 11:10 Jiří Dvorský, Eliška Ochodková, Václav Snášel, VŠB Ostrava - Hashovací funkce založená na kvazigrupách
Prostor pro diskuzi k tématu

Do 11:45 Přestávka na kávu

Mediální partneři:

CryptoWorld




Praktické problémy a trendy I

11:45 - 12:30 Fabien Petitcolas, Microsoft Research Cambridge, UK - Steganography, watermarking and cryptography

Prostor pro diskuzi k tématu

± 12:50 - 13:25 Lenka Fibíková, Univ. Essen, Germany; Jozef Vyskoč, VaF, Bratislava, Slovakia - Practical cryptography - the key size problem

Prostor pro diskuzi k tématu

13:45 - 14:45 Oběd

Kryptanalýza

14:45 - 15:25 Vlastimil Klíma, Decros - ICZ; Tomáš Rosa, Decros - ICZ a ČVUT Praha - O postranních kanálech, nové maskovací funkci a jejím konkrétním použití proti Mangerovu útoku na PKCS#1

Prostor pro diskuzi k tématu

Do 16:00 Přestávka na kávu

Praktické problémy a trendy II

16:00 - 16:30 Luděk Novák, GiTy - Aplikovaná kryptografie a Společná kritéria

Prostor pro diskuzi k tématu

± 16:40 - 17:10 Daniel Cvrček, VUT Brno; Petr Švéda, MU Brno - Hardwarové a softwarové řešení bezpečnosti

Prostor pro diskuzi k tématu

± 17:20 - 18:45 Panelová diskuze „e-podpis a praxe pohledem odborníků“

Panelisté: Petr Hanáček, VUT Brno
Ján Matejka, Ústav pro stát a právo ČAV
Daniel Olejár, UK Bratislava
Michal Sasínek, NBÚ MV SR
Luděk Smolík, seculab
Pavel Vondruška, ÚOOÚ - moderátor

Závěr těsně před Večerníčkem... :-)

Mediální partneři:


CryptoWorld