

## Call for Papers Mikulášská kryptobesídka

1.-2. prosince 2016, Praha

<http://mkb.tns.cz>

### Základní informace

Mikulášská kryptobesídka se letos bude konat už po šestnácté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek 1. prosince a (b) půldne prezentací příspěvků a diskusí v pátek 2. prosince 2016. Pro workshop jsou domluveny zvané příspěvky od:

- Ueli Maurer (ETH Zurich, Švýcarsko).
- Karsten Nohl (Německo).
- Krzysztof Pietrzak (IST Austria, Rakousko).
- Tomáš Rosa (Raiffeisenbank & MFF UK, ČR).

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: <http://mkb.tns.cz>.

### Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž se zajímavými finančními odměnami pro finalisty) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: <http://mkb.tns.cz>. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do 30. září 2016. Pro podávání příspěvků prosím použijte adresu matyas.ZAVINAC@fi.muni.cz a do předmětu zprávy uveďte „MKB 2016 – návrh příspěvku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do 31. října. Příspěvek pro sborník workshopu pak musí být dodán do 13. listopadu.

### Důležité termíny

Návrhy příspěvků:	30. září 2016
Oznámení o přijetí/odmítnutí:	31. října 2016
Příspěvky pro sborník:	13. listopadu 2016
Konání MKB 2016:	1.-2. prosince 2016



### Programový výbor

Peter Gaži, IST Austria, AT  
Jan Hajný, FEKT VUT v Brně, CZ  
Michal Hojsík, Honeywell & MFF UK, Praha, CZ

Marek Kumpošt, NetSuite & FI MU, Brno, CZ  
Vašek Matyáš, FI MU, Brno, CZ – předseda  
Bohuslav Rudolf, NBÚ & MFF UK, Praha, CZ