Call for Papers
Mikulášská kryptobesídka

3. – 4. prosince 2026, Praha
https://mkb.tns.cz

Základní informace

Letos se uskuteční jubilejní 25. ročník workshopu Mikulášská kryptobesídka. Akce 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 *3. 12.* a (b) půldne prezentací příspěvků a diskusí v pátek *4. 12. 2026*. Pro workshop jsou domluveny zvané příspěvky od:

- Vadim Lyubashevsky, IBM Research, CH: On lattice cryptography or zero-knowledge.
- Kenny Paterson, ETH Zurich, CH: TBD.
- Petr Švenda, FI MU, ČR: Do not trust. SCRUTINY! A toolset for better testing of crypto implementations.
- Felix Lange, Sven Hebrok, Univ. Paderborn, D: Usable large-scale evaluations of TLS servers and clients with TLS-Scanner
- Matteo Busi, Ca' Foscari Univ. of Venice, I: On ALVIE and its use to support FPGA security.
- Vašek Matyáš, FI MU: On sec-certs and its support for more transparent use of crypto.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: https://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 přes www stránky workshopu: https://mkb.tns.cz. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF a tak, aby přišly nejpozději do *24. června 2026*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2026 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny programovým výborem workshopu a autoři budou informováni o přijetí/odmítnutí do *24. srpna*. Příspěvek pro sborník workshopu pak musí být dodán do *30. září*.

Důležité termíny

Návrhy příspěvků:	24. června 2026
Oznámení o přijetí/odmítnutí:	24. srpna 2026
Příspěvky pro sborník:	30. září 2026
Konání MKB 2026:	3. – 4. prosince 2026

Programový výbor

Peter Gaži, IOG Research, SR
Jan Hajný, FEKT VUT v Brně, ČR
Vašek Matyáš, FI MU, ČR – předseda
Bohuslav Rudolf, NÚKIB & MFF UK, ČR
Martin Stanek, UK, Bratislava, SR
Adolf Středa, Gen Digital, ČR
Petr Švenda, FI MU, Brno, ČR