**Téma přednášky Card Forum 2009: Současná kryptologie a hashovací funkce v praxi**

**Abstrakt:**

Digitální otisky znamenají velký praktický přínos kryptografie. Jsou jedním z mnoha možných využití hashovacích funkcí. Ty jsou zase jedním z mnoha používaných kryptografických nástrojů. Kryptografie nabízí těchto nástrojů a funkcí pro informační bezpečnost celou řadu, a proto přirozeně a rychle do informačních a komunikačních technologií prorostla. Současně s technologickým pokrokem v těchto oblastech a v elektronice vůbec se ale nutně požaduje i technologický pokrok v oblasti kryptografických funkcí. Požaduje se vyšší rychlost, menší nároky na spotřebu, paměť a vyšší bezpečnost, což jsou obvykle protichůdné požadavky. V oblasti hashovacích funkcí kryptografie dočasně ztratila náskok a nyní dohání rostoucí potřeby IT průmyslu a praxe. Na kryptology je vyvíjen velký tlak na nová technologická řešení, a to pod širokou mezinárodní kontrolou. Na kvalitě těchto funkcí závisí bezpečnost elektronického bankovnictví a komunikací a informačních technologií vůbec na celém světě. To je i příklad technologií čipových karet, kontaktních i bezkontaktních nebo samostatných čipů. Do této oblasti vstoupila kryptografie velmi brzo, ale byly to opět nové technologie (RFID je jedním z řady příkladů), které začaly klást nové požadavky na kvalitu a rychlost kryptografických technik. Přednáška se zabývá nejen stavem v kryptografii a jak tato čelí novým výzvám, ale konkrétně také stavem mezinárodní soutěže na nový hashovací standard, z níž má vzejít nová hashovací funkce SHA-3, rychlejší a bezpečnější než její předchůdci. Tyto funkce budou masově používány i v kartových technologiích, a proto soutěž na SHA-3 obeslaly svými návrhy nejen světoznámí kryptologové, Univerzity a elektronické giganty, ale i největší světoví výrobci z oblasti karetních technologií a čipů vůbec. Přednáška nevyžaduje od posluchačů matematické ani kryptografické zázemí, naopak seznamuje je s kryptografií a přináší přehled klíčových oblastí a nástrojů kryptografie, včetně novinek a hodnotí situaci v praxi.