Moderní kryptoanalytické metody – poznámky z výzkumu & praxe
Lektor: Tomáš Rosa, doktorand K336, kryptolog

Cílem přehledové přenášky je představit současnou podobu kryptoanalýzy, neboli vědní disciplíny zabývající se útoky na kryptografické metody ochrany informačních systémů. Hlavní pozornost bude věnována teorii postranních kanálů, ze které vycházejí téměř všechny dnešní prakticky proveditelné útoky. Vybrané výsledky výzkumu v této oblasti budou demonstrovány na asymetrickém schématu RSA. Toto schéma je použito ve většině současných informačních systémů a to jednak pro přenos symetrických šifrovacích klíčů, jednak pro účely digitálního podepisování.

Osnova:
1. Současná kryptografie - přehled schémat a jejich kombinací.
2. Kryptoanalýza – matematizace pojmu „útok“, odvozené úlohy a jejich řešení.
3. Postranní kanály – rozšířený model kryptografického modulu, hledání útoků v takovém modelu.
4. Obrana proti útokům postranními kanály – základní aspekty.