Úvod do kryptografie 2023/24 – Zkouškové otázky

Zkouška je ústní. Student si vylosuje dvojici otázek a dostane čas na přípravu poznámek. Pravděpodobnostní rozdělení a bodové hodnocení otázek není rovnoměrné. Některé slouží jen jako doplňující otázky v případě, kdy známka je na hraně bodového hodnocení.

Shannonova teorie

- Dokažte, že $\mathrm{H}(\mathbf{K} \mid \mathbf{C}) = \mathrm{H}(\mathbf{K}) + \mathrm{H}(\mathbf{P}) - \mathrm{H}(\mathbf{C})$.
- Definujte pojem *redundance jazyka* a vysvětlete jeho význam. Formulujte a dokažte větu o střední hodnotě počtu možných klíčů pro šifrový text délky n bloků.
- Definujte pojem *absolutně bezpečná šifra*. Dokažte, že Vernamova šifra je absolutně bezpečná.
- Definujte pojem *absolutně bezpečná šifra*. Formulujte a dokažte Shannonovu větu o absolutně bezpečné šifře, včetně pomocného lemmatu. Co nám tato věta říká o efektivitě Vernamovy šifry?

Blokové šifry

- Popište množinu klíčů šifry DES a algoritmus expanze klíče v šifře DES.
- Popište Feistelovo schéma a vysvětlete, jakým způsobem se provádí dešifrování. Musí být rundovní funkce ve Feistelově schématu bijektivní, prostá nebo surjektivní?
- Popište rundovní funkci šifry DES a vysvětlete komplementární vlastnost šifry DES, tj. $\mathrm{DES}(\overline{k}, \overline{x}) = \overline{\mathrm{DES}(k, x)}$.
- Popište šifru AES včetně expanze klíče.
- Vysvětlete konstrukci S-boxu šifry AES.
- Popište meet-in-the-middle útok na součinovou šifru a vysvětlete jeho časovou a paměťovou složitost na příkladu šifer Double DES a two-key Triple DES.
- Vysvětlete nevýhody ECB režimu.
- Popište operační režim CBC/CFB/OFB/CTR. Uveďte, jaké vlastnosti musí mít IV a vysvětlete proč. Vysvětlete, jak se v dešifrovaném textu projeví výpadek bloku šifrového textu a jak se projeví chyba v jednom bitu šifrového textu. Vysvětlete, zda je šifrování a dešifrování paralelizovatelné a zda lze operace šifry předpočítat.
- Popište, jak funguje „bit padding“, PKCS #7 padding a ciphertext stealing v CBC režimu.

Hashovací funkce

- Vysvětlete, jakým způsobem se používají hashovací funkce k ukládání hesel na straně ověřovatele hesla.
- Spočítejte složitost nalezení prvního vzoru hashovací funkce hrubou silou.
- Formulujte a dokažte tvrzení o narozeninovém paradoxu. Vysvětlete, co nám říká o složitosti nalezení kolize hashovací funkce hrubou silou.
- Popište Merkleovo-Damgårdovo schéma a dokažte tvrzení o jeho kolizivzdornosti.
- Vysvětlete složitost nalezení kolize hrubou silou pro hashovací funkci s houbovitou konstrukcí.
- Vysvětlete složitost nalezení prvního vzoru hrubou silou pro hashovací funkci s houbovitou konstrukcí, včetně odhadu úspěšnosti algoritmu. (Vysvětlení stačí omezit na vstup o délce 3 bloků.)

Asymetrická kryptografie

- Popište kryptografický systém RSA a dokažte jeho korektnost. Vysvětlete, jakým způsobem se používá pro šifrování a pro podepisování zpráv. Vysvětlete, proč dvě entity nesmějí sdílet stejný modulus N.
- Vysvětlete, jaká je časová složitost operací kryptografického systému RSA (generování klíčů, šifrování a dešifrování). Popište, jakým způsobem lze zrychlit dešifrování, známe-li prvočíselný rozklad RSA modulu N.
- Popište Håstadův útok na kryptografický systém RSA s malým veřejným exponentem e.
- Popište, jak funguje slepý podpis založený na RSA.
- Popište Diffieho-Hellmanův protokol ustanovení klíče a vysvětlete, jakým způsobem se konstruuje Schnorrova grupa.
- Vysvětlete pojem *perfect forward secrecy* a popište, jak se používá Diffieho-Hellmanův protokol k zajištění perfect forward secrecy.
- Popište Schnorrovo identifikační schéma a vysvětlete, proč se musí volit tajná nonce a náhodná výzva. Ukažte, že zná-li útočník efektivní algoritmus, kterým se může v rámci schématu vydávat za libovolnou osobu, která se identifikuje, pak umí útočník stejně efektivně řešit problém diskrétního logaritmu.
- Popište Schnorrovo podpisové schéma.
- Popište algoritmus DSA a ověřte jeho úplnost. Vysvětlete, proč podepisující osoba musí volit tajnou nonci.

Ostatní

- Vysvětlete Shamirovo schéma sdílení tajemství.
- Vysvětlete Kerckhoffsův princip.
- Definujte Fibonacciho a Galoisovu reprezentaci LFSR a vysvětlete, jakým způsobem spolu tyto dvě reprezentace souvisí.
- Dokažte, že jestliže charakteristický polynom LFSR je primitivní, pak výstup LFSR má maximální možnou periodu.
- Vysvětlete, k čemu v kryptografii slouží MAC algoritmy. Definujte HMAC.