

# Kryptografické systémy 2015/16 – Zkouškové otázky

## Shannonova teorie

- Formulujte a dokažte větu o maximální entropii.
- Formulujte a dokažte větu o sdružené entropii.
- Dokažte, že  $H(X | Y) = H(X, Y) - H(Y)$ .
- Formulujte a dokažte Shannonovu větu o absolutně bezpečné šifře.
- Formulujte a dokažte dolní odhad na střední hodnotu počtu všech možných klíčů.

## Blokové šifry

- Popište šifru DES.
- Popište šifru AES.
- Popište meet-in-the-middle útok a jeho časovou a paměťovou složitost na příkladu šifer Double DES a Triple DES.
- Popište operační režimy blokových šifer ECB, CBC, CFB, OFB a CTR a porovnejte jejich vlastnosti.

## Hashovací funkce

- Vysvětlete, jakým způsobem se používají hashovací funkce k ukládání hesel na straně ověřovatele hesla. Vysvětlete, proč je pro tento účel lepší využít funkci jako PBKDF2.
- Spočítejte složitost hledání prvního vzoru hashovací funkce hrubou silou.
- Formulujte a dokažte tvrzení o narozeninovém paradoxu. Vysvětlete, co nám říká o složitosti hledání kolize hashovací funkce hrubou silou.
- Popište Merkleovo-Damgårdovo schéma a dokažte tvrzení o jeho bezkoliznosti.

## Asymetrická kryptografie

- Popište kryptografický systém RSA a dokažte jeho korektnost. Vysvětlete, jakým způsobem se používá, tj. volba parametrů a použití v součinnosti se symetrickou šifrou. Vysvětlete, proč dvě entity nesmějí sdílet stejný modulus  $N$ .
- Popište Håstadův útok na kryptografický systém RSA s malým veřejným exponentem.
- Vysvětlete, co je digitální podpis, tj. jaké na něho klademe požadavky a jakým způsobem se používá v součinnosti s hashovací funkcí. Popište, jakým způsobem se vytvoří podpisové schéma z asymetrické šifry.
- Popište slepý podpis založený na RSA.
- Popište Diffieho-Hellmanův protokol ustanovení klíče. Vysvětlete, jakým způsobem se volí parametry protokolu. Vysvětlete v této souvislosti pojem *perfect forward secrecy*.
- Popište algoritmus DSA, dokažte jeho korektnost a porovnejte ho s ElGamalovým podpisovým schématem. Vysvětlete, proč podepisující osoba musí volit tajnou nonci.