# 23. Šifrování a hashování

## 1. Hashování

- hashovací funkce jsou matematické funkce, které slouží pro převod dat do relativně malého čísla
- výstupem funkce je otisk, fingerprint, hash
- jakýkkoliv dlouhý vstup generuje pokaždé stejně dlouhý otisk
- nezávisí na povaze změny vstupu, výstup bude vždy relativně stejně náhodný
- nelze zpětně rekonstruovat původní zprávu
- v praxi nepravděpodobné, že dvě různé zprávy budou mít stejný hash, tato pravděpodobnost se zvyšuje tím, že se ke vstupu přidává random string
- **hashovací tabulka**: vyhledávací datová struktura, která asociuje hashovací klíč s příslušnou hodnotou
- **rainbow tabulka**: obsahuje předem vypočtené hodnoty, slouží k prolomení hashovací funkce
- **otisk**: často se hashe používají při komparaci dat

## 2. Symetrické a asymetrické šifry

- **symetrická šifra**: též konvenční, k šifrování a dešifrování se používá stejný klíč (informace, která určuje průběh algoritmu), *proudové šifry* zpracovávají zprávu bit po bitu, zatímco *blokové* rozdělí zprávu do bloků, ty se potom modifikují, náhodnost generování klíčů je zajištěna dostatečně vyskou entropií, *Blowfish, AES, ROT*
- **asymetrická šifra**": při šifrování a dešifrování je zapotřebí dvojice klíčů, pro šifrování se využívá veřejného klíče, dešifrování potom soukromým klíčem, využívají se jednocestné funkce - nejběžnější příklad je násobení; je snadné vynásobit dvě velká čísla, avšak rozklad součinu na jednotlivé činitele je velice obtížné, přece jenom jsou klíče spolu vázány, nicméně je teoreticky možné klíče dešifrovat, ale zabere to hodně času, *RSA*

## 3. Rozdíly a použití

- symetrické šifry mají jednoduchou HW implementaci, využívají se třeba jako generátory pseudonáhodných čísel, hashovací funkce, digitální podpisy, pro silnější účinek je vhodné je kombinovat, problém spočívá, když je nutné si klíč předat, to je nejzranitelnější část, nutné často obměňovat
- asymetrické šifry mají výhodu, že není třeba posílat nikomu klíče, veřejný je útočníkovi k ničemu, slouží pouze k šifrování, jsou ale mnohem pomalejší než šifry symetrické, další nevýhoda spočívá v nutnosti verifikace klíče, certifikační úřady
- PGP - pretty good privacy, program sloužící k šifrování a dešifrování RSA, open-source varianta GnuPG, nejčastěji k šifrování e-mailů