Abstrakt (česky)

Diplomová práce popisuje a porovnává nejrozšířenější algoritmy využívané v informačních systémech. Konkrétně se jedná o algoritmy: Vernamova šifra, DES, 3DES, AES a Blowfish (symetrická kryptografie) a protokol Diffie-Hellman pro výměnu klíčů, RSA, ElGamal, McEliece a systémy založené na eliptických křivkách (asymetrická kryptografie). Dále se práce zabývá oblastí informační bezpečnosti, především jednotlivými bezpečnostními mechanismy (důvěrnost, dostupnost, integrita, autentizace, autorizace a nepopiratelnost), které bývají zajištěny právě pomocí kryptografie. Zmíněno je také téma standardizace, kde jsou především představeny odpovědné instituce tvořící normy a standardy a pak také některé normy. Popisované algoritmy jsou v závěrečné kapitole porovnány pomocí několika kritérií (čas, průchodnost, paměť potřebná pro implementaci, lavinový efekt a délky klíčů). Data, na jejichž základě je porovnáváno, jsou převzata z dalších studií a vědeckých materiálů.