Abstract (in English):

This thesis describes and compares the most popular algorithms used in information systems. Specifically, there are: Vernam cipher, DES, 3DES, AES, and Blowfish (symmetric cryptography) and Diffie-Hellman key exchange, RSA, ElGamal, McEliece and systems based on elliptic curves (asymmetric cryptography). The thesis deals with the areas of information security, in particular the various security mechanisms (confidentiality, availability, integrity, authentication, authorization and non-repudiation), which are secured by using cryptography. There is also mentioned the theme of standardization, where the responsible institutions and some standards are presented. Described algorithms are compared using several criteria (time, throughput, memory needed for implementation, avalanche effect and key lengths) in the final chapter. Data used for comparison are taken from other studies and scientific materials.