

Cílem této práce je porovnání některých metod šifrování souborů. Samotným cílem je vybrání nejvhodnějšího algoritmu z vybraných a na základě jejich testování a srovnat dané algoritmy. Dalším cílem je přiblížit kryptografii jako takovou, její historii a její vývoj. V teoretické části je prvně nastíněn historický vývoj kryptografie. Dále jsou v této části rozebrány a teoreticky popsány vybrané šifry, včetně těch moderních a principy jejich fungování. V praktické části jsou tyto vybrané způsoby šifrování souborů následně porovnávány svou vhodností pro určitý typ souborů (grafická data, audio soubory, dokumenty). Tyto šifry jsou testovány z hlediska jejich rychlosti při šifrování souborů a při jejich následném dešifrování.