Abstrakt:
Tato bakalářská práce pojednává o bitové dělící vlastnosti se třemi podmnožinami. Nejprve představíme důležité pojmy jako bloková šifra, integrální útok a standardní dělící vlastnost. Potom zavedeme definici bitové dělící vlastnosti se třemi podmnožinami a dokážeme tři souvislá tvrzení pravidla propagace: funkce kopírování, AND-komprese a XOR-komprese. V kryptografii využíváme tyto funkce často, proto v této práci dokážeme, jak se šíří bitová dělící vlastnost se třemi podmnožinami po aplikaci těchto funkcí.