REPORT ZA ZIMNÝ SEMESTER

Oboznámil som sa s problematikou kryptológie a naštudoval som si niektoré základné šifry. Presnejšie Caesarovu, Vernamovu, Vigenèrovu a Affine šifru. Následne som si ich naprogramoval v Pythone a napísal som si základné informácie o nich. Programy fungujú tak, že používateľ zadá text na zašifrovanie, program mu vypíše zašifrovaný text a následne mu vypíše aj spätne rozšifrovaný text. Funkcia spätného rozšifrovania zatiaľ funguje len na kontrolu správnosti programu, ale program sa dá používať aj ako dekóder, len jednoduchým napísaním už zašifrovaného textu a použitého kľúča. Začal som písať samotnú učebnicu, ktorá, ale ešte musí byť viac rozvitá. Zatiaľ sú tam základné pojmy v problematike, dôvod a vysvetlenie šifrovania.