Report za letný semester

Počas letného semestra pokračoval vývoj projektu zameraného na implementáciu klasických kryptografických šifier a ich využitie pri šifrovaní, dešifrovaní a základnej kryptoanalýze textu.

V rámci dokumentačnej časti projektu bola vytvorená používateľská príručka, ktorá obsahuje návod na inštaláciu, spustenie a používanie programu. Zároveň bola rozšírená kryptografická príručka o podrobnejší opis implementovaných šifier, ich matematického základu, princípov fungovania a možností kryptoanalýzy. Dokumentácia tak poskytuje používateľovi aj teoretický prehľad potrebný na pochopenie fungovania jednotlivých algoritmov.

V praktickej časti projektu bol vytvorený hlavný program v jazyku Python (main.py), ktorý slúži ako riadiaca časť aplikácie. Program využíva modulárnu architektúru, pričom jednotlivé šifrovacie algoritmy sú implementované v samostatných moduloch. Hlavný program zabezpečuje komunikáciu s používateľom, výber šifry, spracovanie vstupov a volanie príslušných funkcií na šifrovanie a dešifrovanie textu.

Do projektu boli integrované implementácie Caesarovej šifry, afinnnej šifry, Vernamovej šifry, Vigenèrovej šifry a permutačnej šifry. Používateľ môže prostredníctvom jednotného rozhrania vykonávať šifrovanie a dešifrovanie správ pomocou ľubovoľnej z implementovaných metód.

Súčasťou programu bola taktiež implementácia základných nástrojov kryptoanalýzy. Program umožňuje vykonať frekvenčnú analýzu textu, výpočet indexu náhodnosti a v prípade Caesarovej šifry aj útok hrubou silou (bruteforce). Tieto funkcionality slúžia na demonštráciu základných princípov kryptanalýzy.

Výsledkom práce za letný semester je funkčný modulárny softvér, ktorý spája implementáciu klasických kryptografických algoritmov s nástrojmi na ich analýzu a je doplnený o používateľskú a kryptografickú dokumentáciu.