Breaking the Substitution Cipher: Coding an Automatic Cipher Solver

Knap, Jasa (School: Gimnazija Bezigrad)

Despite the advancements in cryptography, breaking ciphers by hand remains a tedious and demanding work. The goal of this research was to write a computer program which would facilitate breaking the monoalphabetic substitution cipher. Prior to this research such programs were inefficient at solving Slovene ciphertexts due to few speakers and unique language features. The problem was approached by using two different methods. Firstly, the ciphertext was analyzed in order to obtain valuable information, such as character pair frequency, relative frequency between characters, etc. .Secondly, a brute-force attack was designed which suggested how characters are most likely encrypted in a ciphertext. The brute-force attack was able to decipher 200-character ciphertexts with an accuracy of 82%. Around 500 characters were needed for the attack based on statistical analysis to reach the same precision. This was likely due to statistical deviations in short ciphertexts. This research showed that the brute-force attack is better at breaking the substitution cipher than pure statistical analysis. Further improvements to the attack should be possible but would require additional research.

Awards Won:
Innopolis University : Full tuition scholarships for the Bachelor program in Computer Science