Prolomení Vigenerovy šifry

Martin Klíma

October 2, 2024

1 Teorie

K prolomení vigeneroy šifry je prvně zapotřebí získat délku klíče, který byl použit pro zašifrování. K tomu se dá využít friedmanuv test. Při znalosti délky klíče se zašifrovaný text rozdělí do skupin podle délky klíče (např. pro klíč délky 3 se rozdělí text do tří skupin). Poté je zapořebí pro každou skupinu zjistit posun vůči původní abecedě (pomocí frekvenční analýzy) a tím určit písmeno klíče.