Prolomení Vigenerovy šifry

Martin Klíma

October 7, 2024

1 Rychlo 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 posun písmena klíče. Při znalosti klíče stačí pouze text pouze dešifrovat.

2 Teorie

2.1 Friedmanův test / Index koincidence

Pro zjištění délky hesla lze využít Friedmanův test. Tento test spočívá v porovnávání indexu koincidence skopin vytovřených ze zašifrovaného textu s indexem koincidence jazyka, kterým je psaný otevřený text. Index koincidence je pravděpodobnost, že dvě náhodně vybraná písmena z textu budou stejná. Pro opravdu náhodný text je index koincidence 1/26. Každý jazyk má svůj index koincidence, pro češštinu se odává hodnota 0.058.

Pro výpočet indexu koincidence skupiny písmen délky n se používá vzorec: $IK = \sum_{i=1}^{26} \frac{n_i(n_i-1)}{n(n-1)}$
Abychom udělali průměr pro všechny skupiny, použijeme vzorec: $IK_{prum} = \frac{1}{n} \sum_{i=1}^{n} IK_i$