Report

Implementační postup

- Vytvoření relativní přechodové matice bigramů
- Vytvoření funkce pro výpočet věrohodnosti textu/klíče
- Vytvoření šifrovací funkce s mapováním, při kterém se každému písmenu z abecedy přiřadí odpovídající znak z klíče
- Vytvoření dešifrovací funkce s mapováním, při kterém se každému písmenu z klíče přiřadí odpovídající znak z abecedy
- Výpočet pravděpodobnosti na základě aktuálního a kandidátního klíče v intervalu <0, 1>
- Implementace Metropolis-Hastings algoritmu, který konverguje k nejlepšímu klíči podle výsledné pravděpodobnosti

Použité metody

- Zaznamenávání relativního počtu výskytů bigramů pomocí přechodové matice
- Prohození dvou náhodně vybraných znaků v klíči
- 20000 iterací M-H algoritmu, přičemž při každé z těchto iterací se zaznamená klíč s nejvyšší pravděpodobností

Dosažené výsledky

- Zjistili jsme, že na správné nalezení vhodného klíče pro dešifrování má největší vliv podmínka přijetí klíče ve chvíli, kdy je pravděpodobnost < 1.
- Např. pokud vygenerujeme náhodné číslo a klíč ještě přijmeme, když je toto číslo < 0.01, tak je výsledkem text: “VK_VO_VUSMRE_NEZMUA_OCBUR...”.
- Po omezení výběru na 0.0005 poté algoritmus vrací výrazně lepší výsledek: “TY_TO_TAKHLE_NECHAS_OZVAL...”.