Substituční šifry

Úkoly celkem max. 3 body

Úkoly

- Stáhněte si pracovní soubor bez-lab1.nb pro aplikaci Mathematica.
- Spusťte Mathematiku a otevřete pracovní soubor.
- Připomeňte si ovládání programu Mathematica (2. slide)
- Podle návodu v jednotlivých slidech samostatně vypracujte příklady označené „Úkol n:“.
- U afinní šifry: Kolik existuje unikátních klíčů? Porovnejte s Caesarovou šifrou. Jak byste mohli prostor klíčů ještě zvětšit?
- U transpoziční šifry je očividně slabým místem způsob doplnění zprávy (padding). Jak byste toto slabé místo ošetřili?