2. Substituční šifry

Úkoly celkem max. 2 body

Úkoly

1. Stáhněte si pracovní soubor bez-lab1.nb (../media/tutorials/02/bez-lab1v5.nb) pro aplikaci Mathematica.
2. Spusťte Mathematiku a otevřete pracovní soubor.
3. Připomeňte si ovládání programu Mathematica (2. slide)
4. Podle návodu v jednotlivých slidech samostatně vypracujte příklady označené „Úkol *n*:“.
5. U afinní šifry: Kolik existuje unikátních klíčů? Porovnejte s Caesarovou šifrou. Jak byste mohli prostor klíčů ještě zvětšit?
6. U transpoziční šifry je očividně slabým místem způsob doplnění zprávy (padding). Jak byste toto slabé místo ošetřili?