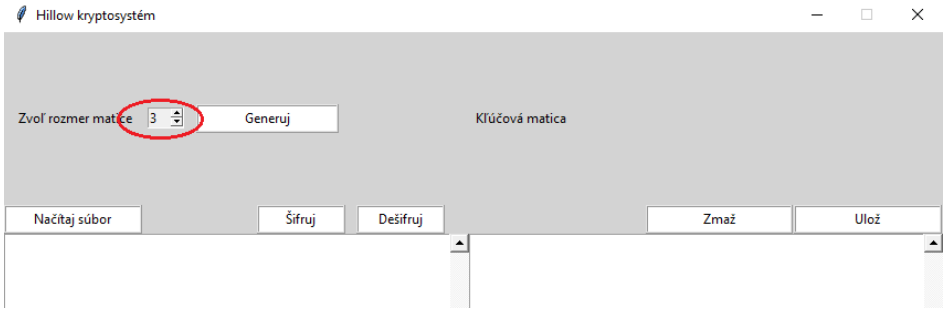
Používateľský manuál

V tomto dokumente popisujeme a názorne (pomocou obrázkov) ukazujeme prácu s našim šifrovacím softvérom. Pre spustenie programu treba otvoriť súbor s názvom *HillCipher.py*. Avšak ak nemáte nainštalovanú knižnicu *numpy*, je potrebné najskôr pristúpiť k jej inštalácii.

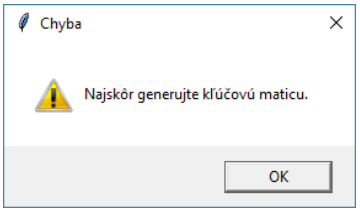
Inštalácia knižnice *numpy* na operačnom systéme windows: Stačí ak si otvoríte príkazový riadok a zadáte doň príkaz *pip install numpy*. V prípade, ak tento postup nebude stačiť, je potrebné aby ste prešli do priečinka, v ktorom máte nainštalovaný *Python*. Väčšinou sa nachádza na disku C v zložke konkrétneho používateľa. Nájdete tam skrytý priečinok *AppData*, v ktorom sa bežne nachádzajú inštalačné súbory Python-u. Prejdete do zložky *Scripts*, otvoríte príkazový riadok, vložíte doň príkaz *cd cesta*, kde cesta predstavuje celú adresu do priečinka, v ktorom sa nachádzate (napr. C:*Users**Meno**AppData**Local**Programs**Python**Python*35*Scripts*) a následne po úspešnom presunutí sa do potrebnej zložky spustíte príkaz *pip install numpy*.

Ako prvé je treba zvoliť si rozmer matice(obr. 1):



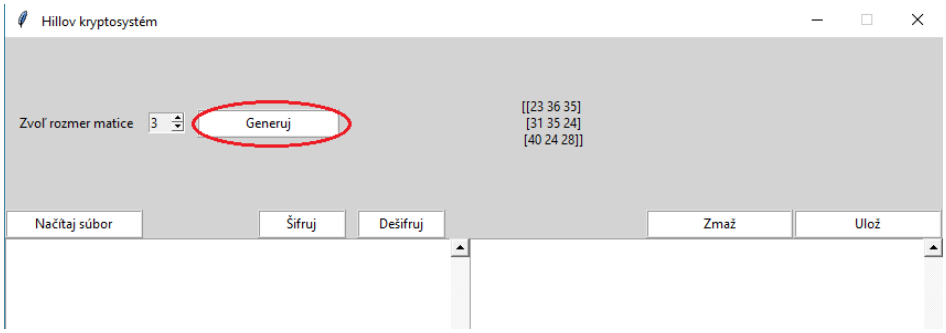
Obr. 1: Rozmer kľúčovej matice

Ak by ste nezvolili rozmer matice a klikli by ste či už na tlačilo *Šifruj* alebo *Dešifruj*, program by Vás upozornil chybou(obr. 2):



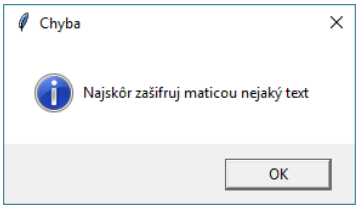
Obr. 2: Chyba č. 1: nezadaná kľúčová matica

Následne systém po stlačení tlačidla *Generuj* (obr. 3) generuje kľúčovú kódovaciu maticu, ktorá sa kontroluje a ak je invertovateľná, zobrazí sa hneď vedľa tlačidla. Ak nastane prípad, že pre vygenerovanú kľúčovú kódovaciu maticu neexistuje jej modulárny inverz, generovanie sa spustí automaticky znova.



Obr. 3: Generovanie kľúčovej kódovacej matice

Ak by ste chceli šifrovať alebo dešifrovať bez prvotného generovania kľúčovej kódovacej matice, program vás upozorní chybovou správou:



Obr. 4: Pokus o šifrovanie/dešifrovanie bez generovania kľúča

Na načítanie súboru slúži tlačidlo *Načítaj súbor*. Po kliknutí naň sa Vám zobrazí dialógové okno, ktoré Vám umožní prehliadať súbory vo vašom počítači a zvoliť si ten správny. Pre korektný beh programu je potrebné zvoliť si súbor, ktorého typ je *.txt*. (obr. 5) Ak by ste si zvolili zlý typ súboru, program by Vás na to upozornil chybou (obr. 6).

Po načítaní správeho súboru sa text zo zvoleného textového súboru zobrazí v ľavom textovom poli. Text sa po kliknutí na tlačidlo *Šifruj* zašifruje a zobrazí v textovej ploche napravo (obr. 7). Ak sa používateľ rozhodne, môže do ľavej textovej plochy namiesto načítavania už vytvoreného súboru z počítača vpisovať vlastný text.

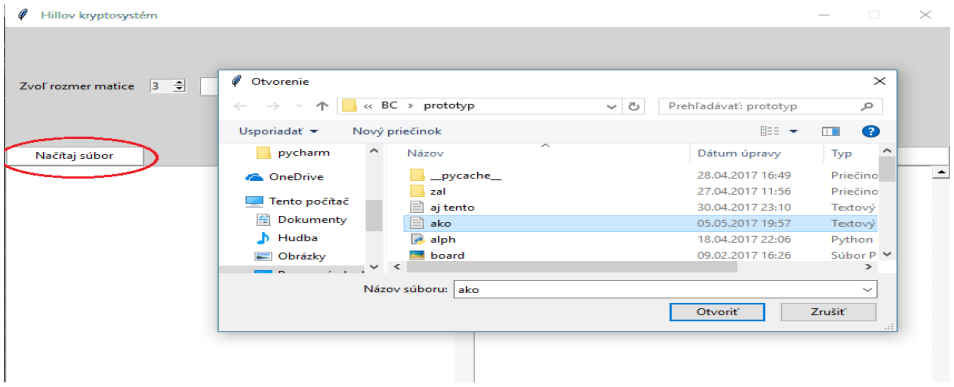
Text, ktorý chcete šifrovať musí byť minimálne dĺžky *2*, čo je minimálny rozmer kľúčovej matice. Ak by ste zadali kratší text, program vyvolá chybu. (obr. 8)

Tlačidlo *Dešifruj* slúži na dešifrovanie textu, po jeho kliknutí sa text v pravom textovom poli prepíše na jeho dešifrovanú verziu, ktorá sa zhoduje s pôvodným textom v pravom poli. (obr. 9)

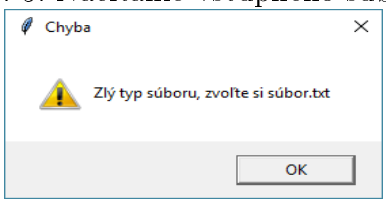
Ľavá textová plocha slúži len na zobrazenie výsledkov šifrovania a dešifrovania, nie je možné akokoľvek upravovať tento text.

Výsledky šifrovania a dešifrovania si môžete uložiť vďaka tlačidlu *Ulož* (obr. 10). Zobrazí sa Vám dialógové okno, v ktorom si určíte umiestnenie súboru a jeho názov.

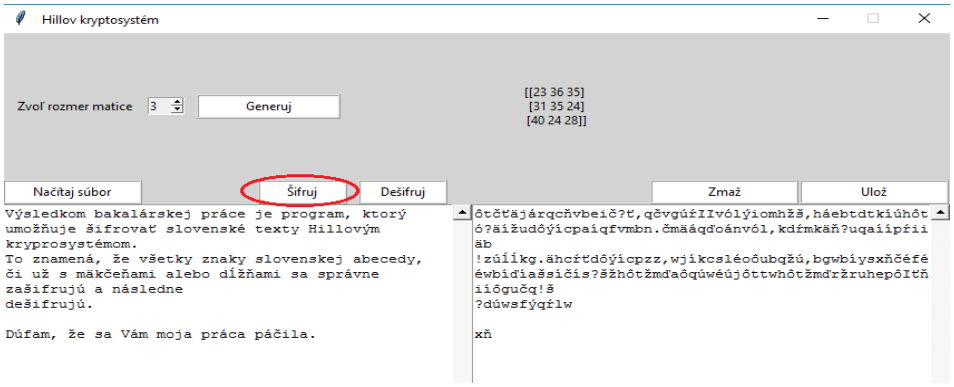
Na rýchle zmazanie oboch textových plôch slúži používateľovi tlačidlo *Zmaž* (obr. 11).



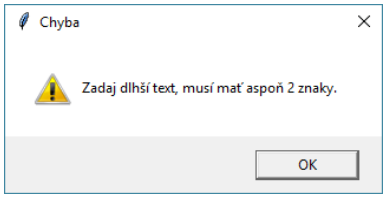
Obr. 5: Načítanie vstupného súboru



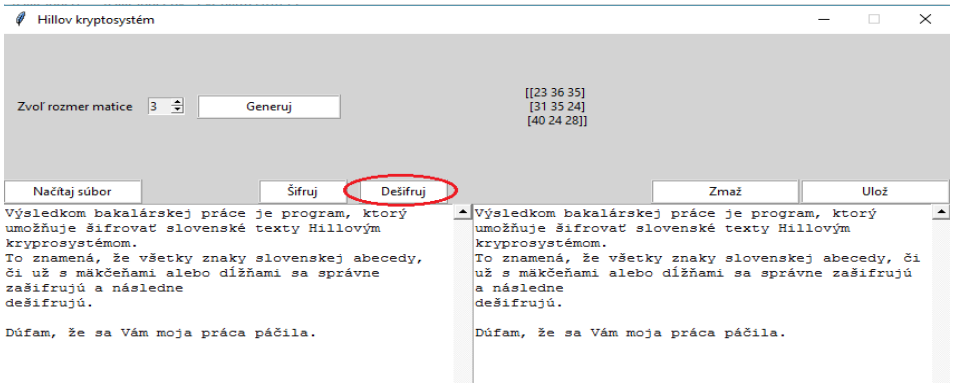
Obr. 6: Zvolený zlý typ súboru



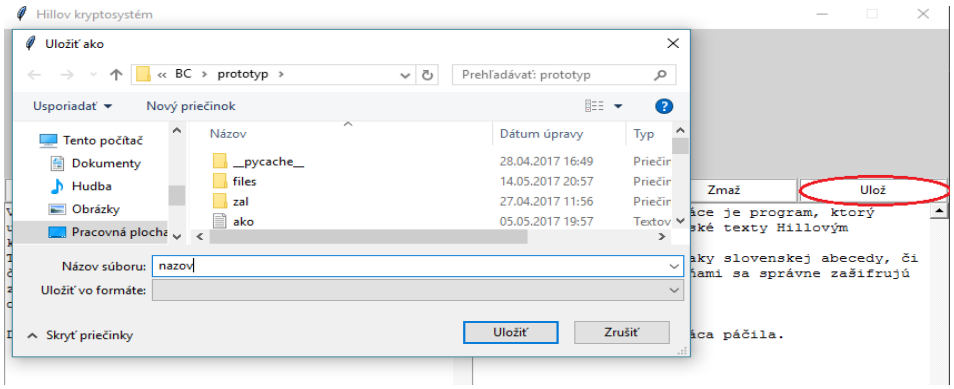
Obr. 7: Šifrovanie zvoleného textu



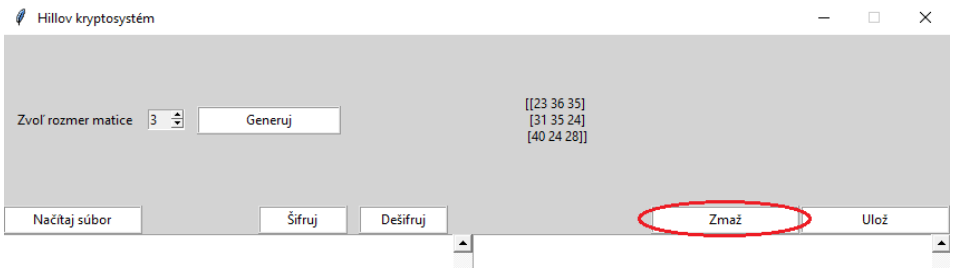
Obr. 8: Zadaný príliš krátky vstupný text



Obr. 9: Dešifrovanie textu



Obr. 10: Uloženie výsledkov šifrovania/dešifrovania



Obr. 11: Zmazanie oboch textových plôch