Lekce 25. – šifrování

Pavel Kryl

ARCIG SIVT 14.4.2025

- kódování znaků
- translační šifra
- práce se soubory
- šifrovací klíč

Kódování znaků

- základní otázka: jak reprezentovat znak textu?
- ascii, iso-8859-2, CP-1250
- princip utf-8

Kódování znaků – Python

- funkce pro práci se znaky:
  - ord(): *převádí* znak na číslo
  - chr(): *převádí* číslo na znak
- experimentujeme

1. Úkol: Posun písmene

- napište funkci pro zakódování znaku o daný počet míst doprava
- co musíme zajistit:
  - vstup je v doméně znaků
  - přetečení: po převodu zůstáváme v doméně znaků

2. Úkol: Zakódování textu

- pro každý znak textu:
  - písmenný znak: voláme naši funkci
  - nepísmenný znak: budeme psát tak, jak je

3. Úkol: Dešifrátor

- pojďme udělat obrácenou funkci: encode → decode
  - znak
  - text

Slabiny

- ?

Slabiny

- vytipování předvídatelných frází/slov

Slabiny

- vytipování předvídatelných frází/slov
- statistická analýza bude dávat pravděpobodnost

Slabiny

- vytipování předvídatelných frází/slov
- statistická analýza bude dávat pravděpobodnost
- hrubou silou stačí vyzkoušet 25 možností

4. Úkol: Dešifrovat zprávu bez znalosti klíče

- máte zprávu
- zjistěte její originální znění

Šifrování s variabilním posunem

- zavedeme *klíč*
- klíč určuje variabilní posun pro každé písmeno zprávy zvlášť
- čemu předcházíme ?

Šifrování s variabilním posunem

- zavedeme *klíč*
- klíč určuje variabilní posun pro každé písmeno zprávy zvlášť
- čemu předcházíme:
  - vytipování předvídatelných frází/slov
  - statistická analýza bude dávat pravděpobodnost
  - hrubou silou stačí vyzkoušet 25 možností

Šifrování čehokoliv

- proč se omezovat na text?
- chceme umět zašifrovat cokoliv
- předmět šifrování: ?
- výsledek šifrování: ?

Šifrování čehokoliv

- proč se omezovat na text?
- chceme umět zašifrovat cokoliv
- předmět šifrování:
  - posloupnost čísel/bytů
- výsledek šifrování:
  - posloupnost čísel/bytů
- jednoduchá implementace

Práce se soubory

- otevření souboru pro čtení:

```
file = open("soubor.pdf", 'rb')
...
obsah_souboru = file.read()
...
file.close()
```

- `rb`: read, binary
- `file.read()`: objekt typu `bytes`, pole bytů/čísel

Práce se soubory

- otevření souboru pro zápis:

```
file = open("soubor.pdf", 'wb')
...
file.write(novy_obsah)
...
file.close()
```

- `wb`: write, binary
- `novy_obsah`: objekt typu `bytearray`

5. Úkol: Zašifrujte dané PDF

- vstup: PDF soubor
- výstup: binární soubor
- postup: každý byte souboru posuňte o počet bytů daný šifrovacím klíčem

Díky!