Kódování a šifrování: Caesarova šifra

Informatika, ZŠ Broumovská

Petr Socha, 2022
petr.socha@zsbroumovska.cz

Kódování

- Kód je **způsob zápisu informace**, například:
  - Informaci „Radost“ můžeme zakódovat jako emoji „☺“
  - Informaci „Smutek“ můžeme zakódovat jako emoji „☹“
  - V Morseově abecedě můžeme písmenko „A“ zakódovat jako „tečka čárka“
- Kódování používáme ke **zjednodušení a usnadnění** zápisu nebo přenosu informace
  - Emoji nám pomůže předat informaci, jak se cítíme
  - Morseova abeceda nám pomůže přenést text pomocí jednoduchých tónů

Šifrování

- Na rozdíl od kódování, šifrování používáme pro **utajení informace**
  - Například: posíláme tajnou zprávu na papírku kamarádovi, a nechceme, aby si ji někdo jiný přečetl
  - Šifra má vždy svůj „**šifrovací klíč**“: jen člověk, který zná klíč, dokáže snadno rozšifrovat text a přečíst informaci… ostatní vidí jen nesmyslná písmena
- Občas dokážeme šifru „prolomit“: to znamená, že přečteme zašifrovanou informaci i bez klíče – o tom až za chvíli, nejdřív si ukážeme příklad šifry

Caesarova šifra

- **Caesarova šifra** je jednoduchá šifra, kterou používal ve starověkém Římě Julius Caesar při svých vojenských taženích během Galských válek
- Nejprve, abychom mohli zašifrovat zprávu, ji musíme digitalizovat: zakódovat písmena do čísel. K tomu použijeme kódovací tabulku
- Začneme tím, že si zašifrujeme svoje vlastní jméno

Kódovací tabulka

- Každému písmenku přiřadíme číslo podle tabulky

- Například:
  - ALFONZ
  - 0,11,5,14,13,25

A	B	C	D	E	F
0	1	2	3	4	5

G	H	I	J	K	L
6	7	8	9	10	11

M	N	O	P	Q	R
12	13	14	15	16	17

S	T	U	V	W	X
18	19	20	21	22	23

Y	Z
24	25

Zašifrování

- Teď známe digitální kód jména „ALFONZ“, tedy „0,11,5,14,13,25“
- V dalším kroku si **vybereme svůj šifrovací klíč**. Může to být **jakékoliv číslo**… teď si vybereme třeba číslo „3“
- Jméno zašifrujeme tak, že přičteme náš klíč ke každému písmenku:
  - **0**+3=3, **11**+3=14, **5**+3=8, **14**+3=17, **13**+3=16, **25**+3=28
  - Zašifrované jméno má tedy kód „3,14,8,17,16,28“
- Pozor, v tabulce máme ale jen čísla od 0 do 25! **Pokud nám někde vyšlo číslo větší než 25, musíme od něj odečíst 26**:
  - Zašifrované jméno má tedy kód „3,14,8,17,16,2“
  - Podle tabulky převedeme čísla zpátky na písmena: „DOIRQC“

Dešifrování

- **Jméno „ALFONZ“ zašifrované klíčem „3“ je tedy „DOIRQC“**
  - Takhle můžeme zašifrovat jakoukoliv zprávu
- Jak budeme zprávu dešifrovat? Přesně opačným postupem
  - Převedeme si „DOIRQC“ na čísla podle tabulky
    - „3,14,8,17,16,2“
  - Odečteme od každého písmenka šifrový klíč
    - „0,11,5,14,13,-1“
  - Pokud nám někde vyjde číslo menší než 0, přičteme k němu 26
    - „0,11,5,14,13,25“
  - Převedeme čísla zpátky na písmena podle tabulky
    - „ALFONZ“

Cvičení I

- Zkuste si zašifrovat a dešifrovat vlastní jméno
- Šifrovací klíč je „**4**“, dešifrujte následující zprávu:

MRJSVQEXMOE

Prolomení šifry

- Dokážeme prolomit šifru i bez znalosti klíče?
  - Ano, ale dá nám to více práce!
- Co se vlastně stane se zašifrovanou zprávou, když ke každému písmenku přičteme šifrovací klíč?
  - Posuneme abecedu! S klíčem „1“ se každé písmenko posune v abecedě
    - A → B
    - B → C
    - C → D
    - …
    - Z → A, protože posouváme dokola abecedy

Prolomení šifry II

- Ve skutečnosti tedy posouváme abecedu
- Kolik máme různých šifrovacích klíčů?
  - Klíč „0“ nám nic nezašifruje, protože abecedu neposuneme
  - Klíč „26“ nám taky nic nezašifruje, protože A se nám zase posune na A
  - **Máme tedy 25 různých šifrových klíčů**, neboli 25 různých posunů abecedy

- Jak dešifrovat zprávu bez znalosti klíče? Můžeme **vyzkoušet všechny klíče (všech 25 klíčů)**, pro jeden z nich nám vyjde správný výsledek
- Tomu říkáme **Útok hrubou silou** (anglicky *brute-force attack*)

Prolomení šifry III

- Vyzkoušet všech 25 klíčů nám zabere hodně času… uměli bychom to i rychleji?
- Představme si, že máme klíč „3“… potom se nám každé písmenko „A“ přepíše na písmenko „D“
- Co když známe nejčastější písmenko v nezašifrované zprávě?
  - Nejčastější písmenko v zašifrované zprávě nám hned prozradí, jaký byl klíč!
  - Pokud víme, že nejčastější písmenko v původní zprávě je „A“ (kód „0“) a nejčastější písmenko v zašifrované zprávě je „D“ (kód „3“), znamená to, že klíč musel být „3“! Abeceda je totiž posunutá o tři písmenka
- Tomu říkáme **Útok frekvenční analýzou**

Cvičení II

- Víte, že v původní (nezašifrované) zprávě bylo nejčastější písmeno „A“
- Rozšifrujte následující zprávu:

IGKYGXUBG YOLXG

Nápověda:
Jaký kód má písmenko „A“?
Jaké je nejčastější písmenko v zašifrované zprávě a jaký má kód? Jaký šifrový klíč jsme museli přičíst, aby vzniklo?

Závěr

- Kód a šifra je něco jiného
  - Kód slouží ke **zjednodušení zápisu nebo přenosu** informace
  - Šifra slouží k **utajení** informace, oproti kódu používá **šifrovací klíč**
- Bezpečnost šifry spočívá v šifrovacím klíči, ne v postupu šifrování
- Téměř každou šifru lze prolomit **hrubou silou**, kdy útočník zkouší všechny možné klíče, ale zabere mu to zpravidla hodně času
  - Čím více existuje různých klíčů, tím je to obtížnější
- Některé šifry lze prolomit i snáz a rychleji, než hrubou silou
  - Ukázali jsme si, že Caesarova šifra jde snadno prolomit *frekvenční analýzou*