# Kódování a šifrování: Vigenèrova a Vernamova šifra

Informatika, ZŠ Broumovská

Petr Socha, 2022
petr.socha@zsbroumovska.cz

# Vigenèrova šifra

- Rozšíření Caesarovy šifry
  - Tato prezentace předpokládá znalost Caesarovy šifry!
- Na rozdíl od Caesarovy šifry používá Vigenèrova šifra jako klíč víc čísel
  - Klíč můžeme definovat pomocí slova/hesla
- Pro příklad zašifrujeme „ALFONZKARASEK“ pomocí klíče „HESLO“
  - Nejprve opět převedeme jak zprávu, tak klíč, do digitální podoby

# Kódovací tabulka

- Zpráva:
  - ALFONZKARASEK
  - 0,11,5,14,13,25, 10,0,17,0,18,4,10
- Šifrovací klíč
  - HESLO
  - 7,4,18,11,14

| 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 Vigenèrovou šifrou

- Zpráva „ALFONZKARASEK“ má kód 0,11,5,14,13,25,10,0,17,0,18,4,10
- Klíč „HESLO“ má kód 7,4,18,11,14
- Zprávu zašifrujeme velmi obdobným způsobem, jako u Caesarovy šifry, ale používáme postupně všechna čísla z klíče:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Zpráva | A: **0** | L: **11** | F: **5** | O: **14** | N: **13** | Z: **25** | K: **10** | A: **0** | R: **17** | A: **0** | S: **18** | E: **4** | K: **10** |
| Klíč | H: **7** | E: **4** | S: **18** | L: **11** | O: **14** | H: **7** | E: **4** | S: **18** | L: **11** | O: **14** | H: **7** | E: **4** | S: **18** |
| Součet zpráva + klíč | 7 | 15 | 23 | 25 | 27 | 32 | 14 | 18 | 28 | 14 | 25 | 8 | 28 |
| Odečtení 26 u čísel > 25 | 7 | 15 | 23 | 25 | 1 | 6 | 14 | 18 | 2 | 14 | 25 | 8 | 2 |
| Zašifrovaná zpráva | H | P | X | Z | B | G | O | S | C | O | Z | I | C |

Písmeno „A“ se zašifrovalo pokaždé jinak, snadná frekvenční analýza jako u Caesarovy šifry není možná

# Dešifrování Vigenèrovy šifry a shrnutí

- Dešifrování proběhne opět velmi obdobně, jako u Caesarovy šifry
- Namísto jednoho čísla se šifrovací klíč skládá z několika čísel, která se dokola opakují (viz příklad na předchozím slajdu)
- Pořád platí, že když vyjde číslo větší než 25, odečtu 26
  a když vyjde číslo menší než 0, přičtu 26
- Na rozdíl od Caesarovy šifry, jednoduchá **frekvenční analýza již není možná** (složitější statistikou to však stále jde)
- Útok hrubou silou zabere mnohem více času, a **čím delší heslo, tím bude složitější**

# Vernamova šifra

- Vernamova šifra je speciální případ Vigenèrovy šifry
- **Šifrovací klíč/heslo je stejně dlouhé, jako šifrovaná zpráva**
  - Tedy se nemusí opakovat
- Šifrovací klíč by měl být pro různé zprávy **vždy různý**, a **vždy náhodně zvolený**
  - Potom je Vernamova šifra **neprolomitelná** (ani hrubou silou)
- Používala se například pro šifrování „horké linky“ mezi Washingtonem a Moskvou během studené války

# Další zdroje informací

- Caesarova šifra (https://cs.wikipedia.org/wiki/Caesarova_%C5%A1ifra)
- Vigenerova šifra (https://cs.wikipedia.org/wiki/Vigen%C3%A8rova_%C5%A1ifra)
- Vernamova šifra (https://cs.wikipedia.org/wiki/Vernamova_%C5%A1ifra)
- Útok hrubou silou (https://cs.wikipedia.org/wiki/%C3%9Atok_hrubou_silou)