Kódování a šifrování: Mřížková šifra

Informatika, ZŠ Broumovská

Petr Socha, 2022
petr.socha@zsbroumovska.cz

Mřížková šifra

- Pro mřížkovou šifru nepotřebujeme převádět písmena na čísla
- **Šifrovací klíč** je číslo, které nám určí šířku mřížky/tabulky (počet sloupců)
- Jako příklad si zašifrujeme zprávu „Tajná zpráva“ klíčem „3“

Šifrování

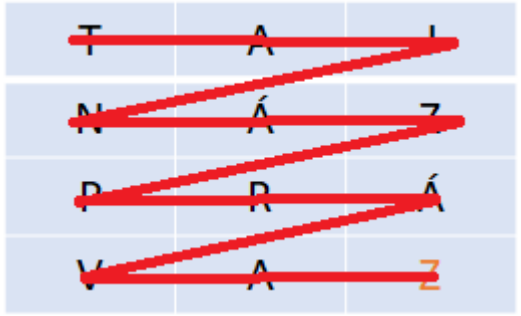
- Klíč „3“ říká, že použijeme mřížku o třech sloupcích
- Do tabulky napíšeme po řádcích tajnou zprávu, kterou pak vyčteme ven po sloupcích:

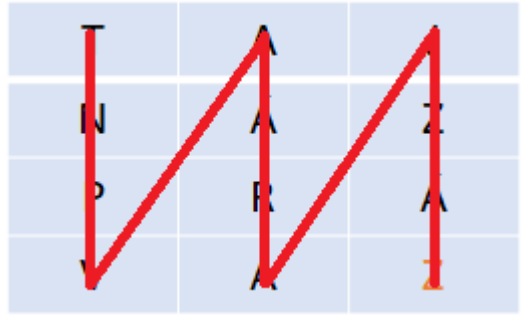
TAJNÁZPRÁVA → Zapíšeme po řádcích

T	A	J
N	Á	Z
P	R	Á
V	A	Z

Přečteme po sloupcích → TNPVAÁRAJZÁZ

Tabulku musíme dovyplnit náhodnými písmenky (tady Z)



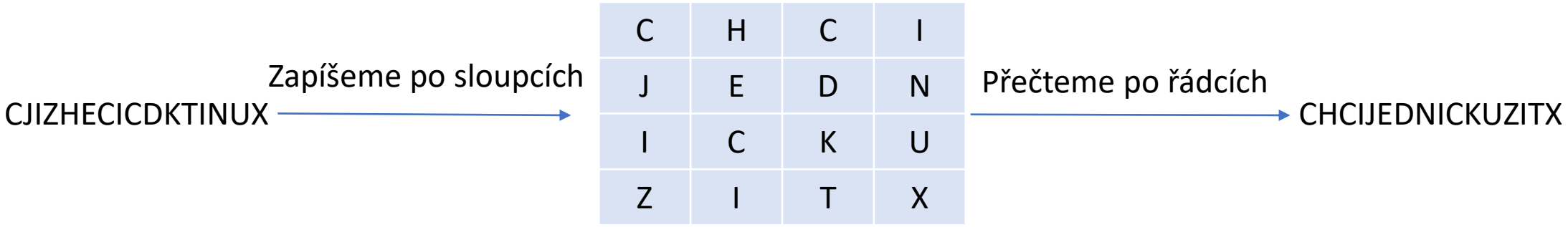


Dešifrování

- Při dešifrování musíme zjistit, kolik řádků má mít naše tabulka
- Víme, že klíč je „3“ a naše zpráva „TNPVAÁRAJZÁZ“ má 12 písmen
- Tabulka pro dešifrování bude mít tedy 12 děleno 3 řádků: 12:3=**4**
- Zašifrovanou zprávu zapíšeme po sloupečcích, a přečteme po řádcích

Příklad dešifrování

- Zašifrovaná zpráva je „CJIZHECICDKTINUX“ a klíč je „4“
- Klíč je „4“, takže tabulka bude mít čtyři sloupečky
- Zpráva má 16 písmen, takže tabulka bude mít 16:4=**4** řádky



Zašifrovaná zpráva tedy byla „Chci jedničku z IT“ a písmenko X uhodneme, že bylo použito pro doplnění tabulky