# BEZIT – 2. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

22. 2. 2024

# Posuvná šifra (1 / 2)

- Pro posuvnou šifru zvolte vhodný klíč a zašifrujte řetězec: *Za svitani zacnete s utokem*

# Posuvná šifra (2 / 2)

- Bez znalosti klíče dešifrujte text, který byl zašifrován posuvnou šifrou
- *Gl eq fqeuy zm anqp*

# Posuvná šifra (2 / 2)

- Bez znalosti klíče dešifrujte text, který byl zašifrován posuvnou šifrou
- *Gl eq fqeuy zm anqp*
- Klíč je 12

# Posuvná šifra (2 / 2)

- Bez znalosti klíče dešifrujte text, který byl zašifrován posuvnou šifrou
- *Gl eq fqeuy zm anqp*
- Klíč je 12
- Kryptogram byl: *Uz se tesim na obed*

# Vigenèrova šifra (1 / 2)

- Pro Vigenèrovu šifru zvolte vhodný klíč a zašifrujte řetězec: *Kupujte procesory s Apple Silicon!*

# Vigenèrova šifra (2 / 2)

- Dešifrujte text, který byl zašifrován posuvnou šifrou s klíčem `KAFE`
- *Naq ficm ws cmpobngok*

# Vigenèrova šifra (2 / 2)

- Dešifrujte text, který byl zašifrován posuvnou šifrou s klíčem `KAFE`
- *Naq ficm ws cmpobngok*

# Vigenèrova šifra (2 / 2)

- Dešifrujte text, který byl zašifrován posuvnou šifrou s klíčem `KAFE`
- *Naq ficm ws cmpobngok*
- Kryptogram byl: *Dal bych si chlebicek*

# Substituční šifra (1 / 2)

- Pro substituční šifru zvolte vhodný klíč a zašifrujte řetězec: *Upolnicek je nejlepsi system na domaci ukoly*

# Substituční šifra (2 / 2) – frekvenční analýza

- Na čem je založena kryptoanalýza substituční šifry?

# Substituční šifra (2 / 2) – frekvenční analýza

- Na čem je založena kryptoanalýza substituční šifry?
- Permutace nemění četnosti výskytů jednotlivých znaků
- $\Rightarrow$ Přirozený jazyk má téměř pevně danou četnost výskytů jednotlivých znaků $\Rightarrow$ Frekvenční analýza

# Substituční šifra (2 / 2) – frekvenční analýza

- Na čem je založena kryptoanalýza substituční šifry?
- Permutace nemění četnosti výskytů jednotlivých znaků
- $\Rightarrow$ Přirozený jazyk má téměř pevně danou četnost výskytů jednotlivých znaků $\Rightarrow$ Frekvenční analýza
- Jak zpřesnit frekvenční analýzu?

# Substituční šifra (2 / 2) – frekvenční analýza

- Na čem je založena kryptoanalýza substituční šifry?
- Permutace nemění četnosti výskytů jednotlivých znaků
- $\Rightarrow$ Přirozený jazyk má téměř pevně danou četnost výskytů jednotlivých znaků $\Rightarrow$ Frekvenční analýza
- Jak zpřesnit frekvenční analýzu?
- Pravděpodobnosti výskytů znaků jsou ovlivněny předchozími znaky
- $\Rightarrow$ Můžeme spočítat výskyty digramů a trigramů
- Např: `https://en.wikipedia.org/wiki/Bigram` `https://en.wikipedia.org/wiki/Trigram`

# Úkol

- Ve vašem oblíbeném programovací jazyce spočítejte hash `SHA256` ze zřetězení jména příjmení
- Najděte první číslici zleva
- Stáhněte si text z `https://apollo.inf.upol.cz/~janostik/slides/bezit/[cislice].txt`
- Dešifrujte daný text, který vznikl substituční šifrou
- Automatické dešifrátory jsou zakázány
  - Pro odevzdání potřeba nejen klíče, ale i postup

# Úkol

- Ve vašem oblíbeném programovací jazyce spočítejte hash `SHA256` ze zřetězení jména příjmení
- Najděte první číslici zleva
- Stáhněte si text z `https://apollo.inf.upol.cz/~janostik/slides/bezit/[cislice].txt`
- Dešifrujte daný text, který vznikl substituční šifrou
- Automatické dešifrátory jsou zakázány
  - Pro odevzdání potřeba nejen klíče, ale i postup
- Když budete v koncích, zkuste verzi s mezerami: `https://apollo.inf.upol.cz/~janostik/slides/bezit/[cislice]_spaces.txt`