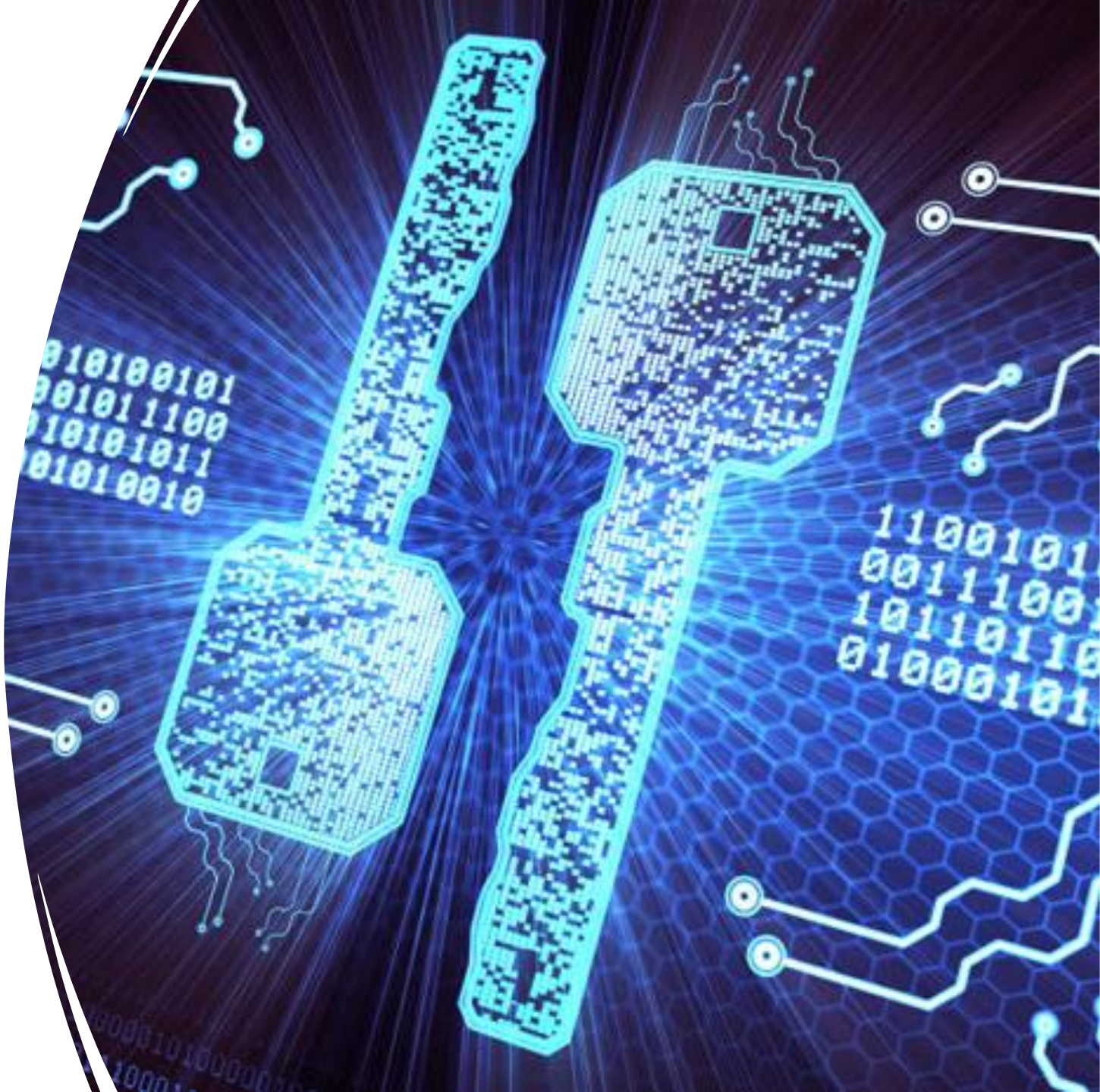
Kryptografie

Jakub Prokeš

4.TB

Kryptografie

- Je věda, zabývající se metodami šifrování dat
- Používá se k ochraně důvěrnosti a integrity dat při jejich přenosu nebo ukládání
- Převod čitelných dat na šifrovaná data
- Čitelná data = plaintext
- Šifrovaná data = ciphertext
- Data jsou čitelná pouze s klíčem k dešifrování



Kryptoanalýza

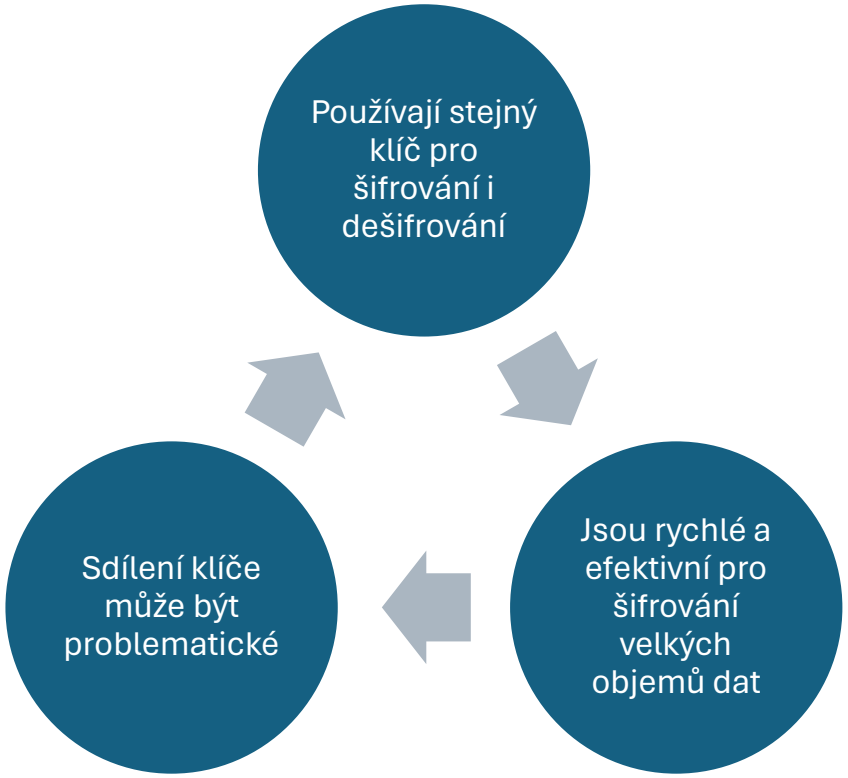
- Je věda zabývající se metodami získávání obsahu šifrovaných informací bez znalosti přístupu (příslušného klíče)
- Je to umění dešifrování
- Je protiváhou kryptografie

Steganografie

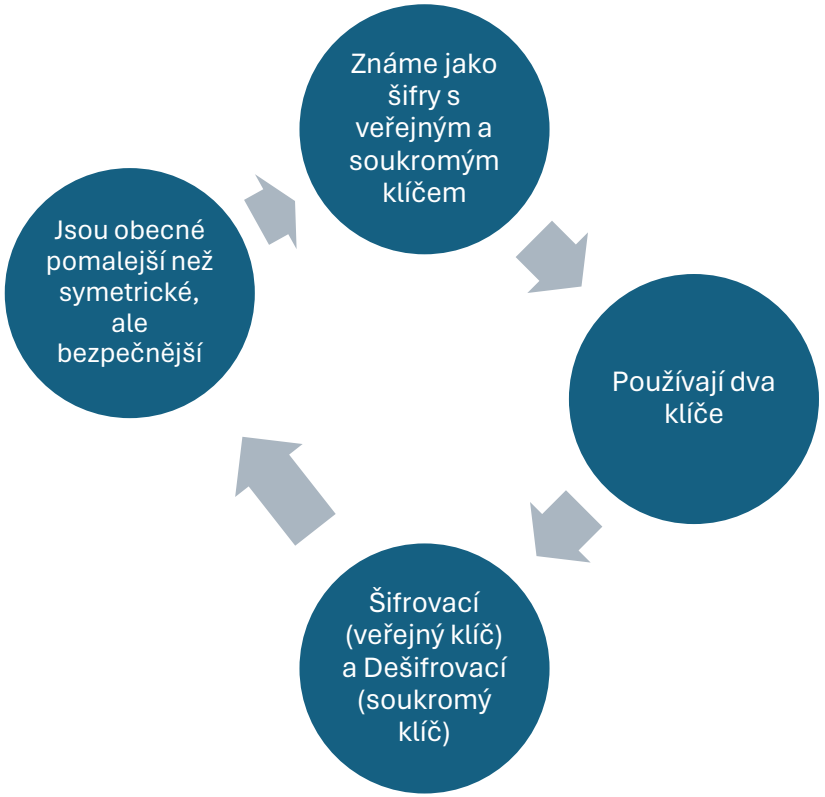
- Je technika skrývání informací uvnitř jiných, neškodných souborů, obrázků, videí nebo textů
- Provádí se tak, aby skrytá zpráva informace nebyla na prví pohled zřejmá
- Na rozdíl od kryptografie, která informace zabezpečuje, Steganografie je spíše o jejich skrytí

Šifry symetrické a asymetrické

Symetrické

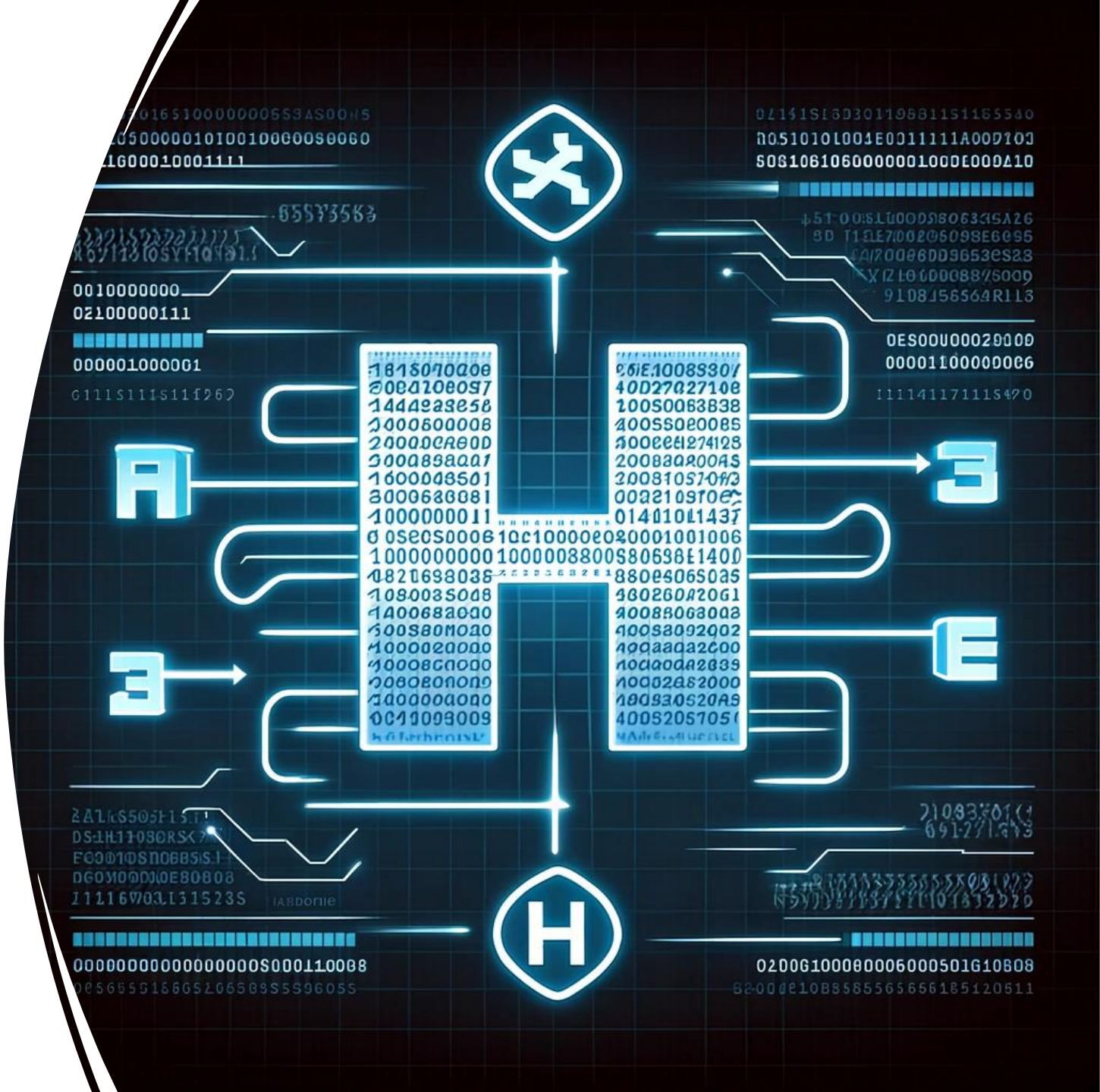


Asymetrické



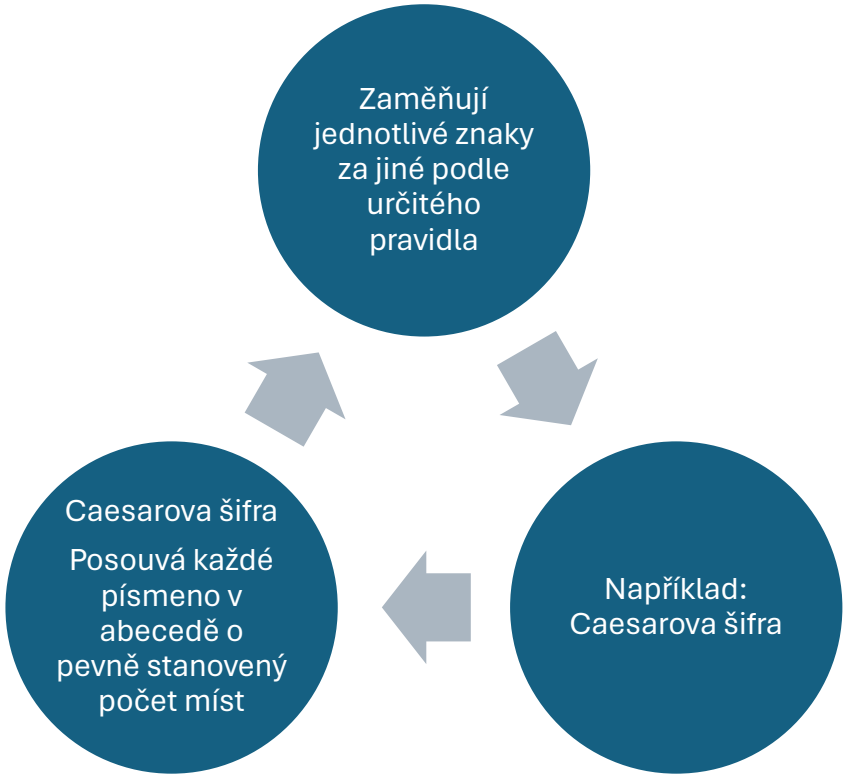
Hashovací funkce

- Převádí vstupní data libovolné délky na výstup pevné délky, známý jako hash
- Je to jednosměrný proces (z hash hodnoty nelze získat zpět původní data
- Hashovací funkce jsou důležité pro ověření integrity dat
- Jsou široce používány v kryptografii

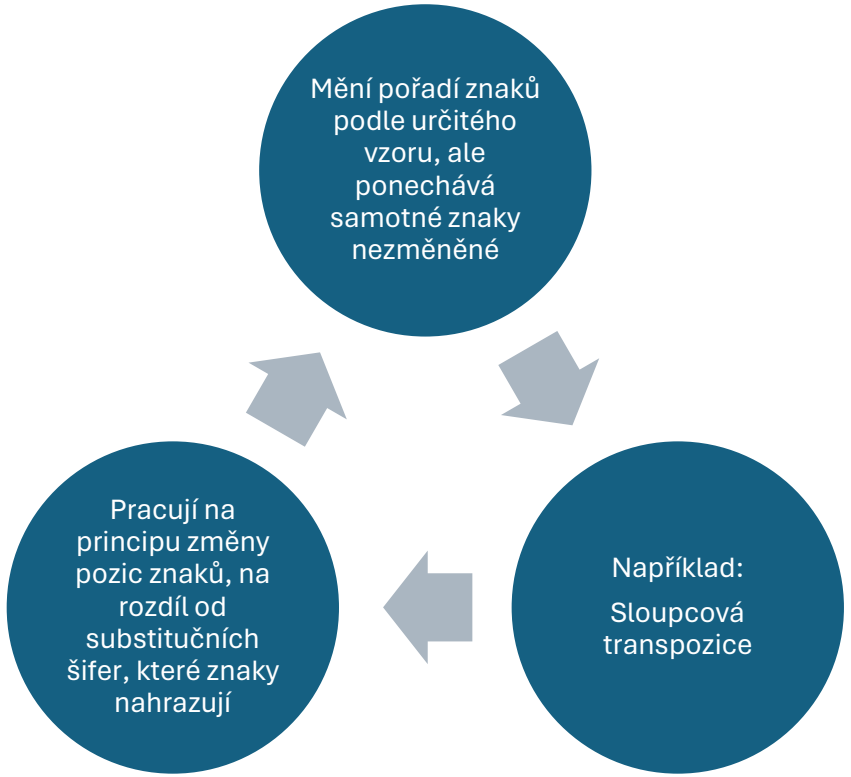


Šifry substituční a transpoziční

Substituční

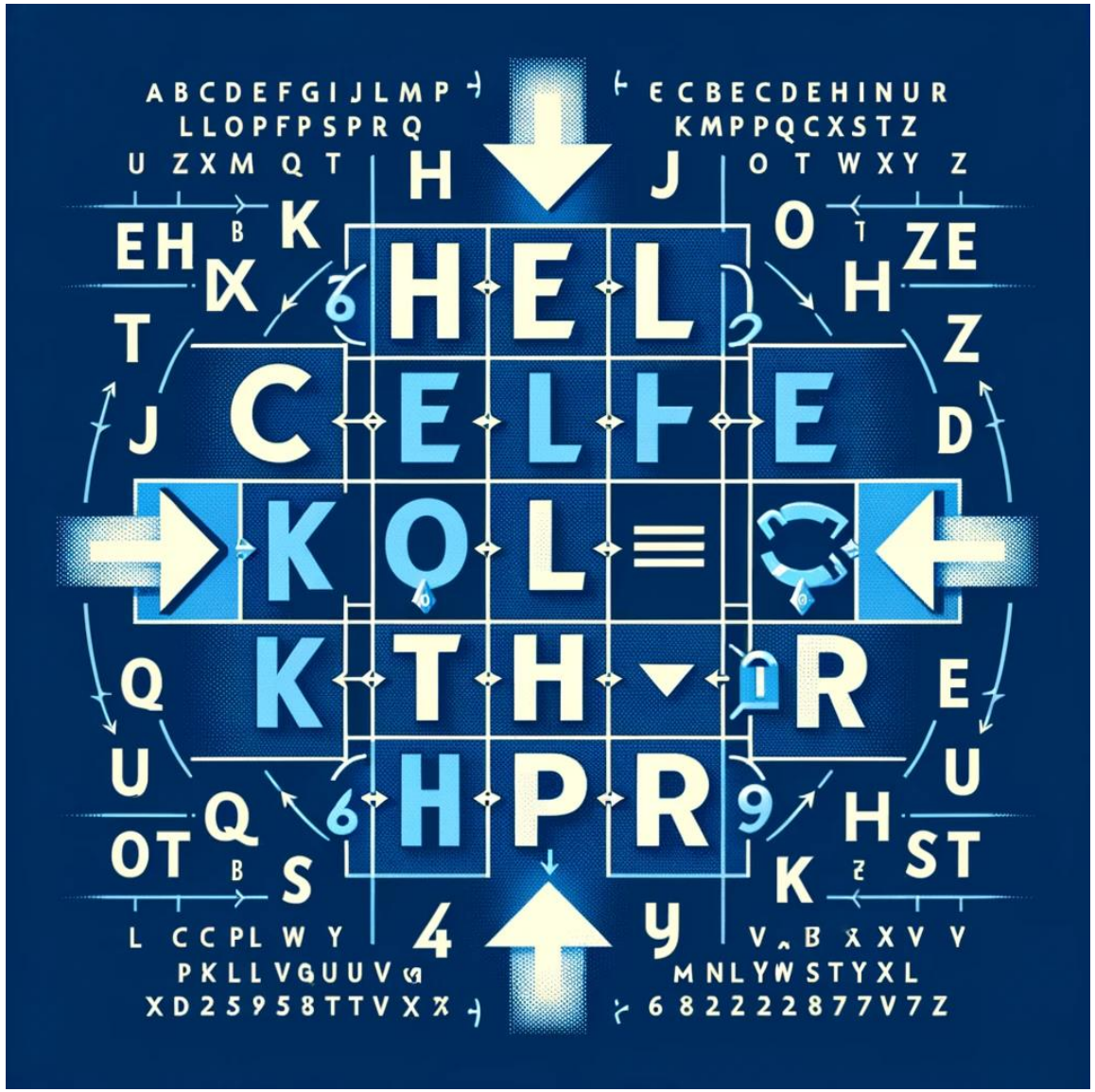


Transpoziční



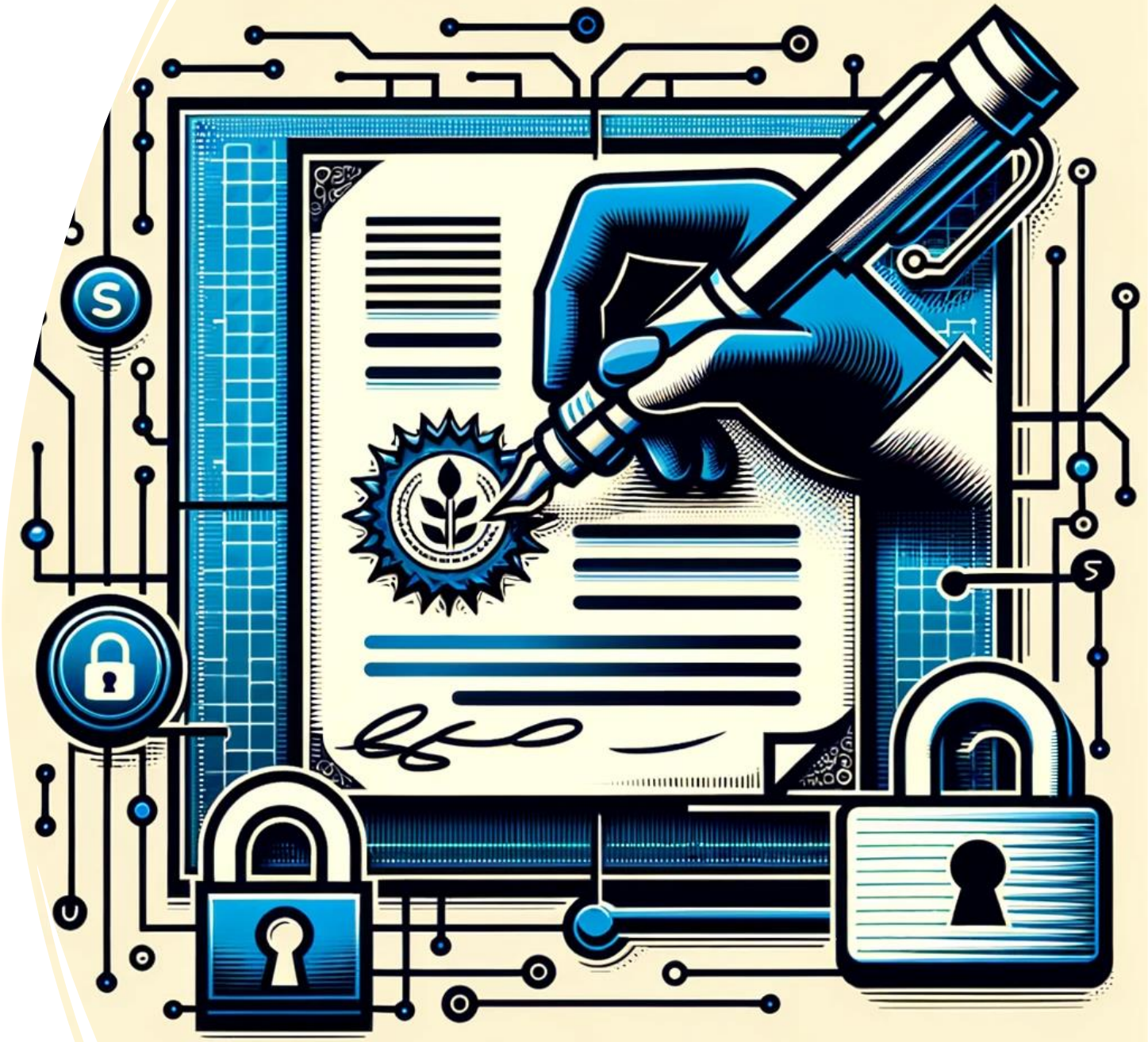
Caesarova šifra

- Posun: 3
- Původní zpráva: „HELLO“
- Šifrovaná zpráva: „KHOOR“
- Posunutí každého písmena o tři pozice doprava v abecedě.
- H se stalo K, E se stalo H, atd.



Digitální podpis

- Je elektronická forma podpisu
- Využívá kryptografické algoritmy k ověření autenticity a integrity digitálně podepsaných dat
- Je široce používán pro zabezpečení elektronických transakcí – elektronické smlouvy, emaily, online platby



Proces digitálního podpisu