Kryptografie, kryptoanalýza, steganografie

Kryptografie

- Věda o šifrování informací pro zajištění jejich důvěrnosti
- Cílem je skrytí určených informací před neoprávněnou stranou, zajištění jejich autentičnosti, zabránění jejich odmítnutí (popření) nebo zabránění jejich neoprávněnému použití
- Dva základní typy

  - Kryptografie s asymetrickým klíčem (též s veřejným klíčem) – Kryptografické algoritmy založené na asymetrických šifrách

  - Kryptografie se symetrickým klíčem (též s tajnými klíči) – Kryptografické algoritmy založené na symetrických šifrách.

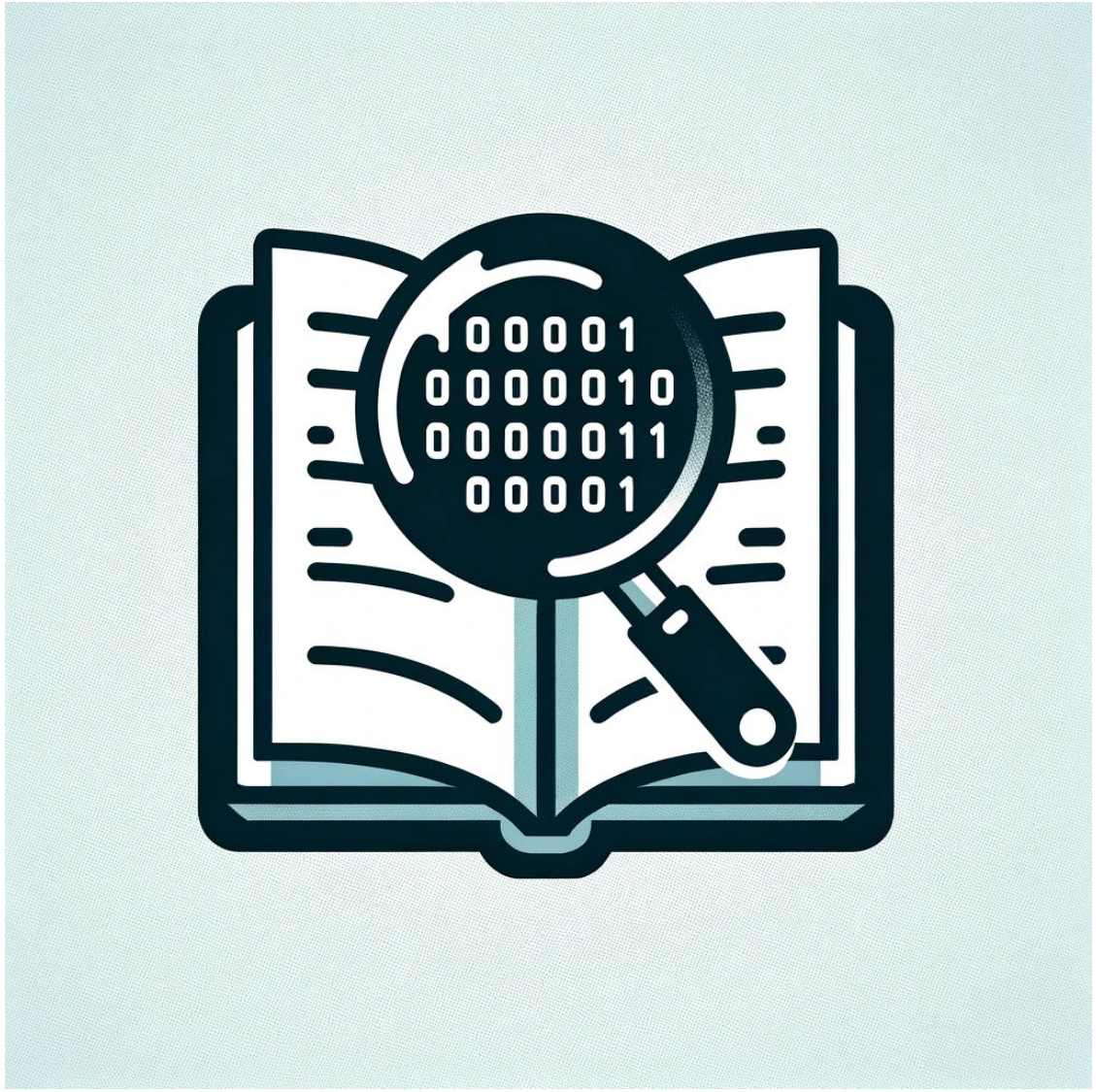
- Kryptografie se využívá na ochranu dat, zabezpečení komunikace nebo u elektronických transakcí

Kryptoanalýza

- Studium metod pro prolomení šifrovacích algoritmů a získání přístupu k šifrovaným informacím
- Jedná se o opak kryptografie, která šifry vytváří
- Cílem kryptoanalýzy je identifikovat slabiny v šifrovacích systémech pro jejich zlepšení a zajištění větší bezpečnosti.

Steganografie

- Umění skrývání informací uvnitř jiných, nešifrovaných informací
- Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá
- Síla této komunikace stojí a padá na jejím utajení, a proto zachycení skryté zprávy prakticky znamená její prolomení
- Historicky se používalo utajení existence zprávy pomocí neviditelného inkoustu, mikroteček a jiných metod ukrytí
- V současnosti se často používá vnoření bitů zprávy do nezávadných počítačových souborů, například fotografií krajiny atp.



Symetrická šifra

- Též šifra s tajnými klíči
- Jedná se o šifru, kde je možné ze znalosti jednoho ze dvojice párových klíčů, tj. klíče pro zašifrovaní a příslušného klíče pro dešifrování, v rozumném čase vypočítat druhý klíč
- Bezpečnost závisí na tajnosti klíče, pokud je klíč kompromitován, šifrování je prolomeno
- Vhodné pro šifrování velkých objemů dat
- Příklady algoritmů
  - Advanced Encryption Standard – AES
  - Data Encryption Standard - DES

Asymetrická šifra

- Též šifra s veřejným klíčem
- Šifra, kde ze znalosti jednoho z dvojice párových klíčů, tj. klíče pro zašifrování a příslušného klíče pro dešifrování, nelze v rozumném čase vypočítat ten druhý
- Bezpečnost je zajištěna složitostí matematických problémů, jako je faktorizace velkých čísel nebo výpočet diskrétního logaritmu
- Použití: Digitální podpisy, šifrování e-mailů, zabezpečené spojení (SSL/TLS)
- Příklady algoritmů
  - RSA – Rivest-Shamir-Adleman
  - ECC – Ecliptic Curve Cryptography

Hashovací funkce

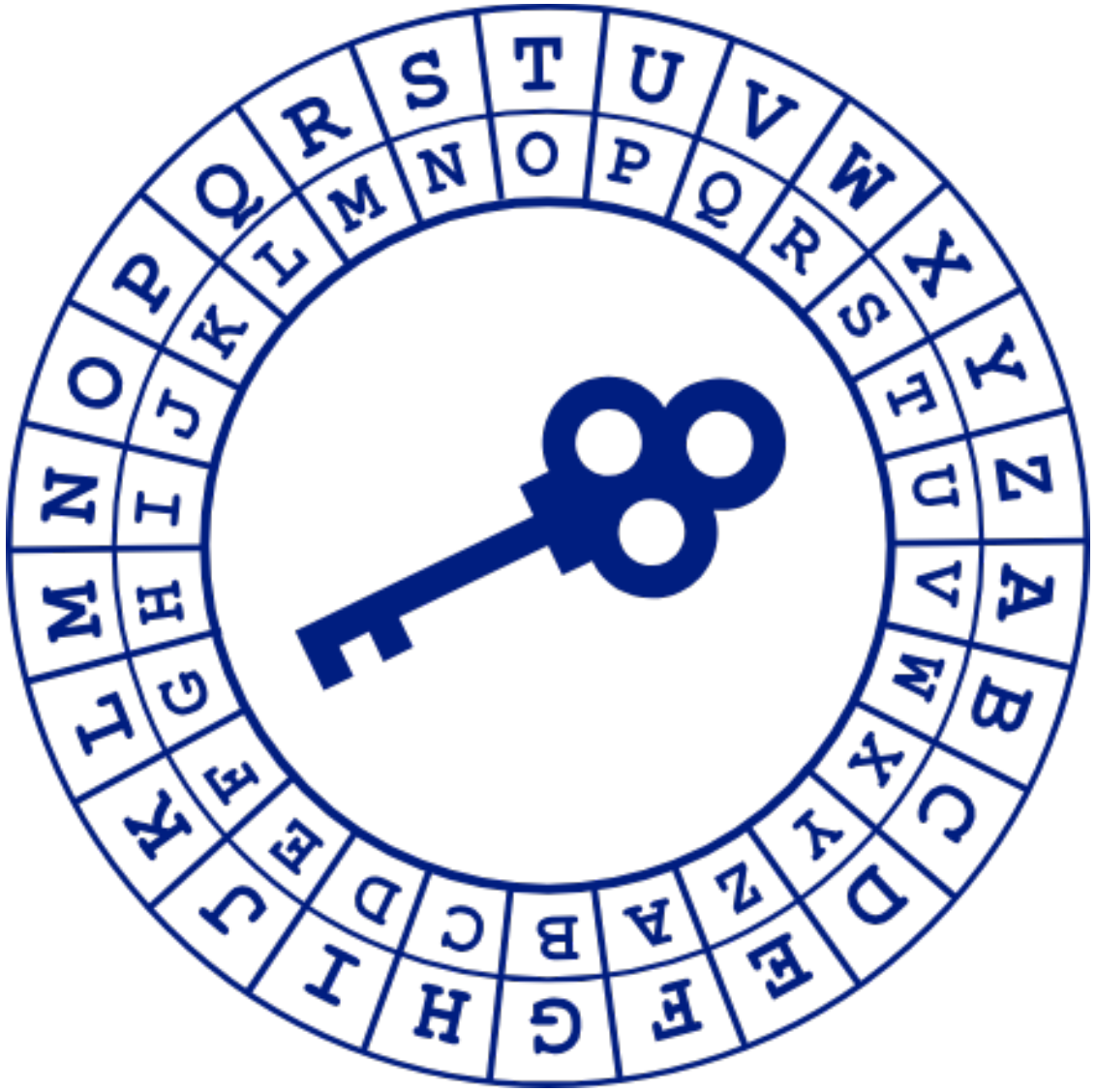
- Algoritmus, který převádí libovolně dlouhý vstup na výstup pevné délky, zvaný hash
- Klíčové vlastnosti
  - Determinismus – stejný vstup vždy produkuje stejný výstup
  - Rychlost – Hashování je rychlý proces, což je klíčové pro zpracování velkých objemů dat
  - Nemožnost reverzního inženýrství – Z hash hodnoty prakticky nelze získat původní vstup
  - Odpornost proti kolizím – Velmi nepravděpodobné, že dva odlišné vstupy vyprodukují stejný hash

Příklady a využití hashovací funkce

- Použití
  - Ověření integrity dat – Změna i jediného bitu vstupních dat způsobí radikální změnu hash výstupu
  - Ukládání hesel – hesla se ukládají ve formě hashů pro zvýšení bezpečnosti
- Příklady
  - SHA-256 (Secure Hash Algorithm 256bit) – často používaný pro zabezpečení transakcí a dat v blockchainu
  - MD5 (Message Digest Algorithm 5) – starší hashovací funkce, dnes se nedoporučuje kvůli bezpečnostním slabostem

Substituční šifry

- Šifrovací metoda, kde jsou jednotlivé znaky nebo skupiny znaků v plaintextu nahrazeny jinými znaky nebo skupinami znaků
- Princip
  - Každý znak z plaintextu je přemapován na jiný znak podle předem definovaného pravidla
- Příklady
  - Caesarova šifra
- Výhody – jednoduchost a přímá implementace
- Nevýhody – Relativně snadno prolomitelná, zejména při znalosti jazyka plaintextu



Transpoziční šifry

- Šifrovací metoda, která zachovává původní znaky plaintextu, ale mění jejich pořadí podle určitého systému
- Princip
  - Znaky z plaintextu jsou přeuspořádány, což vytváří šifrový text
  - Klíčem je metoda, kterou jsou znaky přeuspořádány, například podle pravidelného vzoru nebo pomocí mřížky
- Příklady
  - Sloupcová transpozice
  - Šikmá mřížka
- Výhody – Obtížnější k rozluštění než jednoduché substituční šifry
- Nevýhody – Vyžaduje pečlivou přípravu a často i více času na šifrování a dešifrování

Digitální podpis

- Elektronický ekvivalent fyzického podpisu, využívající asymetrickou kryptografii
- Jeho funkcí je zajištění autenticity, integrity a neodvolatelnosti elektronických dokumentů
- Proces digitálního podpisu spočívá ve vytvoření hashe z dokumentu, který je poté zašifrován soukromým klíčem odesílatele

Děkuji za pozornost ☺