Úvod do kryptografie

- **Definice:** Kryptografie je věda o šifrování dat, která umožňuje jejich ochranu před neoprávněným přístupem.
- **Historie:** První formy kryptografie sahají až do starověkého Egypta, Řecka a Říma (např. Caesarova šifra).
- **Cíl:** Zajistit důvěrnost, integritu, autentizaci a nepopiratelnost informací.
- **Příklady použití:** Šifrování e-mailů, bankovních transakcí, bezpečné přihlašování.

Hlavní principy kryptografie

- **Šifrování a dešifrování:** Transformace původní zprávy (plaintext) na šifrovanou podobu (ciphertext) a zpět pomocí klíče.
- **Druhy šifrování:**
  - **Symetrické:** Používá stejný klíč pro šifrování i dešifrování (např. AES).
  - **Asymetrické:** Používá veřejný a soukromý klíč (např. RSA).
- **Význam:** Kryptografie chrání data i během přenosu.

Co je steganografie?

- **Definice:** Umění a věda o skrývání existence zprávy uvnitř jiných dat.
- **Hlavní cíl:** Skrýt skutečnost, že nějaká komunikace probíhá.
- **Metody:** Skrytí zprávy do obrázků, zvukových nebo video souborů.
- **Příklad:** Skrytí tajného textu v nejméně významných bitech obrázku (LSB steganografie).
- **Rozdíl od kryptografie:** Steganografie se snaží ukrýt **existenci zprávy**, zatímco kryptografie ukrývá pouze **obsah zprávy**.

Co je obfuskace?

- **Definice:** Technika záměrného zkomplikování dat nebo kódu, aby byly obtížně pochopitelné.
- **Hlavní cíl:** Ztížit analýzu nebo reverzní inženýrství dat/kódu.
- **Použití:** Ochrana softwarového kódu, zamaskování citlivých dat.
- **Příklad:** Nahrazení srozumitelného zdrojového kódu za obtížně čitelný, ale stále funkční.
- **Rozdíl od kryptografie a steganografie:** Obfuskace nezakrývá existenci dat, ale činí jejich interpretaci složitou.

Rozdíly mezi kryptografií, steganografií a obfuskací

Aspekt	Kryptografie	Steganografie	Obfuskace
Hlavní cíl	Skrýt obsah zprávy	Skrýt existenci zprávy	Ztížit pochopení zprávy
Viditelnost	Data jsou šifrovaná a viditelná	Data jsou ukryta v nosiči	Data jsou viditelná, ale nesrozumitelná
Použití	Šifrované komunikace	Skrytá komunikace	Ochrana kódu, maskování dat

Praktické příklady použití

1. **Kryptografie:**
    - Šifrování souborů pomocí AES.
    - Použití asymetrických klíčů pro zabezpečenou výměnu dat (TLS).
2. **Steganografie:**
    - Skrytí tajné zprávy v obrázku pomocí LSB.
    - Digitální vodotisky k ochraně autorských práv.
3. **Obfuskace:**
    - Zkomplikování kódu softwaru proti reverznímu inženýrství.
    - Maskování citlivých dat v testovacích prostředích.

Kombinace technik pro vyšší bezpečnost

- **Společné použití:**
  - Kryptografie a steganografie: Zpráva je šifrována a následně skryta pomocí steganografie, což zvyšuje její bezpečnost.
  - Kryptografie a obfuskace: Šifrovaný kód je dále obfuskován, aby bylo obtížné jej analyzovat.
- **Výhody kombinace:**
  - Zajišťuje více vrstev ochrany.
  - Snižuje riziko odhalení nebo zneužití informací.

Závěr

- Kryptografie, steganografie a obfuskace jsou klíčové techniky ochrany dat.
- Každá má jiný cíl:
  - Kryptografie: Chrání obsah.
  - Steganografie: Skrývá existenci.
  - Obfuskace: Ztěžuje pochopení.
- Kombinace těchto technik poskytuje robustní zabezpečení moderních datových systémů.

Úvod do steganografie

- **Definice**: Skrytí zpráv nebo informací v jiných médiích tak, aby jejich existence nebyla zjevná.
- **Historie**:
  - Starověk: skryté zprávy na voskových tabulkách
  - Moderní doba: digitální steganografie
- **Steganografie vs kryptografie**:
  - Kryptografie chrání obsah zprávy.
  - Steganografie skrývá existenci zprávy.

Princip steganografie

- **Nosné médium (Carrier)**: Soubor, do kterého je zpráva skryta (např. obrázek, zvuk).
- **Skrytá zpráva (Payload)**: Informace, které chcete ukrýt.
- **Stego-médium**: Výsledek, který obsahuje skrytou zprávu.
- **Stego-klíč**: Klíč pro vložení/extrakci zprávy.

Typy médií používaných ve steganografii

- **Obrázky**: Formáty PNG, JPEG
- **Zvukové soubory**: MP3, WAV
- **Video soubory**
- **Texty**: Skrytí zpráv v mezerách nebo formátování
- **Síťová data**: Manipulace s pakety

Techniky steganografie

- **LSB (Least Significant Bit)**: Nahrazování nejméně významných bitů.
- **Maskování a filtrování**: Použití vizuálních efektů (např. průhlednost).
- **Skrytí v redundanci**: Využití nevyužitých částí dat.
- **Kombinace se šifrováním**: Šifrování zprávy před jejím vložením.

Praktické příklady

1. **Skrytí textu v obrázku**
    - Manipulace bitů pixelů.
2. **Skrývání dat v audiu**
    - Vkládání do zvukových vzorů.
3. **Použití nástrojů**:
    - Steghide
    - OpenPuff

Výhody steganografie

- Skrytí samotné existence komunikace.
- Nízká detekovatelnost.
- Lze kombinovat s kryptografií pro větší bezpečnost.

Nevýhody a omezení

- **Kapacita**: Omezené množství dat, která lze skrýt.
- **Náchylnost na destrukci**: Ztráta dat při úpravách (komprese, změna formátu).
- **Robustnost**: Nutnost odolnosti proti manipulaci.

Steganalýza

- **Definice**: Proces odhalení skrytých informací.
- **Metody detekce**:
  - Histogramová analýza.
  - Statistické modely.
- **Nástroje pro detekci**: Např. stegdetect.

Aplikace steganografie

- **Bezpečnostní a vojenské účely**.
- **Ochrana autorských práv**: Digitální vodoznaky.
- **Skrytá komunikace** v restriktivních režimech.
- **Kyberkriminalita**: Zneužití v malware.

Závěr

- **Shrnutí**:
  - Steganografie je užitečná i riziková.
  - Kombinace se šifrováním zvyšuje bezpečnost.
- **Budoucnost**:
  - Nové techniky a ochranné mechanismy.
- **Diskuze**: Otázky a odpovědi.