Kryptografie a šifrování

Kryptografie (z řeckého *kryptos* – skrytý a *graphein* – psát) je věda o metodách utajování obsahu zpráv a zajištění jejich bezpečnosti. V rámci oboru **Bezpečnost a Data** tvoří kryptografie základní kámen ochrany soukromí, integrity dat a digitální identity.

1. Základní cíle (CIA Triáda a další)

Moderní šifrování neslouží jen k „utajení textu“, ale zajišťuje čtyři klíčové vlastnosti:

- **Důvěrnost (Confidentiality):** Data si může přečíst pouze ten, kdo má příslušný klíč.
- **Integrita (Integrity):** Záruka, že data nebyla během přenosu nebo uložení změněna.
- **Autentizace (Authentication):** Ověření, že odesílatel je skutečně ten, za koho se vydává.
- **Nezpochybnitelnost (Non-repudiation):** Odesílatel nemůže později popřít odeslání zprávy (např. u digitálního podpisu).

2. Hlavní pilíře kryptografie

A. Symetrické šifrování

Používá **jeden stejný klíč** pro šifrování i dešifrování. Obě strany se na něm musí předem bezpečně shodnout.

- **Výhody:** Velmi rychlé, vhodné pro velké objemy dat (např. šifrování disků).
- **Příklady:** AES (standard), ChaCha20.

B. Asymetrické šifrování (Veřejný klíč)

Používá dvojici klíčů: **veřejný** (pro šifrování, může ho znát kdokoliv) a **soukromý** (pro dešifrování, musí zůstat v tajnosti).

- **Výhody:** Odpadá problém s bezpečným předáním klíče. Umožňuje digitální podpisy.
- **Příklady:** RSA, ECC (kryptografie na bázi eliptických křivek).

C. Hašovací funkce (Hashing)

Jednosměrná transformace dat na fixně dlouhý řetězec (otisk). Nelze z něj získat původní data.

- **Využití:** Kontrola integrity souborů, bezpečné ukládání hesel.
- **Příklady:** SHA-256, SHA-3.

3. Kryptografie v praxi

V moderním IT systémech se tyto metody kombinují do tzv. **kryptosystémů**:

- **SSL/TLS (HTTPS):** Zajišťuje bezpečné prohlížení webu kombinací asymetrického (pro navázání spojení) a symetrického (pro přenos dat) šifrování.
- **End-to-End Encryption (E2EE):** Šifrování, kde klíče mají pouze koncoví uživatelé (např. v aplikacích Signal nebo WhatsApp).
- **Disk Encryption:** Ochrana dat na fyzických nosičích (např. BitLocker, FileVault).

4. Budoucí výzvy

- **Kvantové počítače:** Vývoj strojů, které by mohly prolomit současné asymetrické šifry (RSA).
- **Post-kvantová kryptografie:** Vývoj nových algoritmů odolných vůči útoku kvantových počítačů.
- **Homomorfní šifrování:** Umožňuje provádět výpočty přímo nad zašifrovanými daty, aniž by se musela dešifrovat.

Související články:

- Správa hesel a MFA
- Síťová bezpečnost a TLS
- Fyzikální základy a kvantové výpočty

Tagy: security cryptography data_protection aes rsa hashing