Kryptografie a šifrování

Kryptografie (z řeckého *kryptos* – skrytý a *graphein* – psát) je věda o metodách utajování obsahu zpráv a zajištění jejich integrity. V moderním IT je kryptografie základním pilířem **informační bezpečnosti**, který umožňuje bezpečné bankovnictví, e-commerce a soukromou komunikaci.

1. Základní cíle kryptografie (CIA Triáda)

Moderní kryptografie neřeší pouze utajení, ale zaměřuje se na čtyři klíčové aspekty:

- **Důvěrnost (Confidentiality):** Zprávu si může přečíst pouze oprávněný příjemce.
- **Integrita (Integrity):** Záruka, že zpráva nebyla během přenosu změněna.
- **Autentizace (Authentication):** Ověření identity odesílatele.
- **Nezpochybnitelnost (Non-repudiation):** Odesílatel nemůže popřít, že zprávu odeslal (digitální podpis).

2. Symetrické šifrování

U symetrické kryptografie používá odesílatel i příjemce **stejný tajný klíč** pro šifrování i dešifrování.

- **Výhody:** Velmi vysoká rychlost výpočtu, nízká náročnost na hardware.
- **Nevýhody:** Problém s bezpečným doručením klíče mezi stranami.
- **Hlavní algoritmy:**
  - **AES (Advanced Encryption Standard):** Celosvětový standard, prakticky neprolomitelný při délce klíče 256 bitů.
  - **ChaCha20:** Moderní a velmi rychlá šifra, populární v mobilních zařízeních.

3. Asymetrické šifrování (Veřejný klíč)

Asymetrická kryptografie využívá **dvojici klíčů**: **veřejný klíč** (pro šifrování) a **soukromý klíč** (pro dešifrování). Soukromý klíč nesmí nikdy opustit zařízení majitele.

- **Princip:** Co je zašifrováno veřejným klíčem, lze rozšifrovat pouze příslušným soukromým klíčem.
- **Využití:** Výměna klíčů, digitální podpisy, SSL/TLS certifikáty pro HTTPS.
- **Hlavní algoritmy:**
  - **RSA:** Založeno na obtížnosti rozkladu velkých čísel na prvočísla.
  - **ECC (Elliptic Curve Cryptography):** Modernější přístup, nabízí stejnou bezpečnost jako RSA při mnohem kratších klíčích.

4. Hašovací funkce (Hashing)

Hašování není šifrování (je to jednosměrný proces). Vytváří z libovolně velkých dat fixně dlouhý

„otisk“ (hash). Pokud se v datech změní jediný bit, hash bude úplně jiný.

- **Použití:** Ukládání hesel (neukládá se heslo, ale jeho hash), kontrola integrity souborů.
- **Standardy:** SHA-256 (používaný i v Bitcoinu), SHA-3, Argon2 (pro hesla).

5. Moderní hrozby a post-kvantová kryptografie

S rozvojem kvantových počítačů hrozí, že algoritmy jako RSA nebo ECC budou prolomeny v reálném čase.

- **Kvantová odolnost:** Vývoj nových algoritmů (např. založených na mřížkách), které odolají útokům kvantových počítačů.
- **End-to-End Encryption (E2EE):** Šifrování, kde klíče drží pouze koncoví uživatelé, nikoliv poskytovatel služby (např. Signal, WhatsApp).

Srovnávací tabulka

Vlastnost	Symetrická	Asymetrická
Rychlost	Velmi vysoká	Pomalá
Distribuce klíčů	Obtížná	Snadná (veřejný klíč)
Vhodné pro	Velké objemy dat (disky, TLS tunel)	Digitální podpisy, navázání spojení

Související články:

- Síťová bezpečnost a Firewally
- Správa hesel a MFA
- Fyzikální limity a kvantové výpočty

Tagy: security cryptography encryption aes rsa hashing data_protection