Kryptografie

Kryptografie (z řeckého *kryptós* – „skrytý“ a *gráphein* – „psát“) je vědecká disciplína zabývající se zabezpečením informací prostřednictvím jejich utajení, ověřením integrity, autentizací původu zpráv a zajištěním důvěrnosti při přenosu nebo ukládání dat. Je základním pilířem kybernetické bezpečnosti a moderních informačních technologií.

Historie kryptografie

Kryptografie má kořeny v hluboké historii lidské komunikace. Již ve starověku se používaly různé šifrovací techniky k utajení válečných, politických či osobních zpráv.

- **Starověk**: Nejstarší známé metody zahrnují například **Skytalé** (Sparta, 5. století př. n. l.) – mechanické zařízení využívající pásku navinutou na dřevěný válec – nebo **Caesarovu šifru**, která posunuje písmena abecedy o pevně daný počet míst (např. o 3).
- **Středověk a renesance**: Rozvoj kryptoanalýzy (loupež šifer) vedl k vytváření sofistikovanějších šifer, jako je například **Vigenèrova šifra** (16. století), která používala klíčové slovo pro proměnný posun.
- **Druhá světová válka**: Kryptoanalýza hrála klíčovou roli – například dešifrování německého šifrovacího stroje **Enigma** v Bletchley Parku díky práci Alana Turninga a jeho týmu.
- **Moderní éra**: Od 70. let 20. století se kryptografie přesunula ze světa vojenské tajnosti do veřejné sféry. Vznik standardů jako **DES** (Data Encryption Standard, 1977) a později **AES** (Advanced Encryption Standard, 2001) položil základy moderní kryptografie.

Základní pojmy

- **Šifrování (Encryption)** – proces převodu **otevřeného textu** (plaintext) na **šifrovaný text** (ciphertext) pomocí algoritmu a klíče.
- **Dešifrování (Decryption)** – opačný proces: převod ciphertextu zpět na plaintext.
- **Kryptografický algoritmus** – matematický postup určující, jak probíhá šifrování a dešifrování.
- **Klíč** – tajná informace (číslo, řetězec, soubor), která řídí šifrovací/dešifrovací proces.
- **Kryptoanalýza** – věda o lomení šifer bez znalosti klíče.
- **Kryptosystém** – kompletní sada pravidel, algoritmů a protokolů pro zabezpečenou komunikaci.

Typy kryptografie

Symetrická kryptografie

U symetrické kryptografie se pro šifrování i dešifrování používá **stejný klíč**. Je rychlá a efektivní, ale vyžaduje bezpečný způsob sdílení klíče mezi komunikujícími stranami.

Příklady algoritmů:

- **DES** (Data Encryption Standard) – dnes považován za nebezpečný kvůli krátké délce klíče (56

bitů).
- **3DES** – zpevněná verze DES používající tři průchody šifrováním.
- **AES** (Advanced Encryption Standard) – moderní standard, podporuje délky klíčů 128, 192 a 256 bitů. Široce používán v praxi (např. v TLS, diskovém šifrování).
- **ChaCha20** – moderní streamovací šifra často používaná v mobilních prostředích a webových protokolech.

Asymetrická kryptografie

Asymetrická kryptografie (tzv. **veřejná kryptografie**) využívá **dvojici klíčů**: veřejný klíč (public key) a soukromý klíč (private key). Co je zašifrováno veřejným klíčem, lze dešifrovat pouze soukromým klíčem, a naopak.

Výhody:

- Žádná potřeba sdílení tajného klíče před komunikací.
- Možnost digitálního podpisu a ověření identity.

Nevýhody:

- Výpočetně náročnější než symetrické metody.
- Není vhodná pro šifrování velkých objemů dat.

Příklady algoritmů:

- **RSA** (Rivest–Shamir–Adleman) – založen na obtížnosti faktorizace velkých čísel.
- **ECC** (Elliptic Curve Cryptography) – využívá vlastnosti eliptických křivek; poskytuje stejnou bezpečnost při mnohem kratších klíčích než RSA.
- **DSA** (Digital Signature Algorithm) – zaměřen specificky na digitální podpisy.

Hašovací funkce

Kryptografická hašovací funkce převádí libovolně dlouhý vstup na pevně dlouhý řetězec znaků (tzv. **hash** nebo **otisk**). Je to jednosměrná funkce – z hashu nelze rekonstruovat původní vstup.

Vlastnosti bezpečné hašovací funkce:

- **Deterministická**: stejný vstup vždy dá stejný výstup.
- **Odolnost vůči kolizím**: velmi těžké najít dva různé vstupy se stejným hashem.
- **Odolnost vůči preimage útokům**: nelze najít vstup odpovídající danému hashi.

Příklady funkcí:

- **MD5** – dnes považován za nebezpečný kvůli nalezeným kolizím.
- **SHA-1** – oslaben, již nedoporučován pro bezpečnostní účely.
- **SHA-2** (např. SHA-256, SHA-512) – současný standard používaný v TLS, digitálních certifikátech, blockchainu atd.
- **SHA-3** – nový standard založený na jiném principu (sponge construction).

Aplikace kryptografie

Kryptografie je nedílnou součástí dnešní digitální společnosti. Mezi hlavní aplikace patří:

- **Zabezpečená komunikace** – protokoly jako **TLS/SSL** (používané v HTTPS) kombinují symetrickou a asymetrickou kryptografii pro zabezpečení webového provozu.
- **Digitální podpisy** – umožňují ověřit autenticitu a integritu dokumentu (např. ve finančních transakcích, softwarových aktualizacích).
- **Šifrování disků** – technologie jako BitLocker (Windows), FileVault (macOS) nebo LUKS (Linux) chrání data před fyzickým přístupem.
- **Blockchain a kryptoměny** – využívají kryptografii pro ověření transakcí, generování adres a zajištění integrity řetězce bloků.
- **Autentizační protokoly** – např. OAuth, Kerberos, nebo dvoufaktorová autentizace (2FA) často využívají kryptografické principy.

Post-kvantová kryptografie

S rozvojem **kvantových počítačů** hrozí, že některé dnešní kryptografické algoritmy (zejména RSA a ECC) mohou být prolomeny pomocí **Shorova algoritmu**. Proto se intenzivně vyvíjí tzv. **post-kvantová kryptografie** (Post-Quantum Cryptography, PQC), která by měla být odolná i vůči útokům kvantových systémů.

NIST (National Institute of Standards and Technology) aktuálně vybírá standardy pro post-kvantové algoritmy, mezi které patří například:

- **CRYSTALS-Kyber** (pro šifrování)
- **CRYSTALS-Dilithium** (pro digitální podpisy)

Bezpečnostní doporučení

- Nikdy nepoužívej zastaralé algoritmy (MD5, SHA-1, DES).
- Vždy používej dostatečně dlouhé klíče (např. RSA ≥ 3072 bitů, AES ≥ 128 bitů).
- Využívej ověřené kryptografické knihovny (např. OpenSSL, libsodium, Bouncy Castle) – neprogramuj vlastní šifry.
- Pravidelně aktualizuj systémy a certifikáty.
- Uchovávej soukromé klíče v bezpečném prostředí (HSM – Hardware Security Module).

Související pojmy

- Bezpečnost informací
- Šifrování
- Digitální_podpis
- Certifikační_autorita
- TLS
- Blockchain

Reference

- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
- Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.
- NIST. (2023). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography
- Stallings, W. (2021). *Cryptography and Network Security: Principles and Practice*. Pearson.

Viz také

- Kryptoanalýza
- Symetrické šifrování
- Asymetrické šifrování
- Hašovací funkce