Šifrování (Kryptografie)

Šifrování je proces převodu čitelných dat (**prostý text / plaintext**) pomocí algoritmu a klíče do nečitelné podoby (**šifrovaný text / ciphertext**). Cílem je zajistit, aby data mohl přečíst pouze držitel příslušného dešifrovacího klíče.

Kryptografie v IT zajišťuje čtyři základní pilíře:

1. **Důvěrnost:** Data si nepřečte nikdo nepovolaný.
2. **Integrita:** Data nebyla cestou změněna.
3. **Autentizace:** Identita odesílatele je ověřena.
4. **Nepopiratelnost:** Odesílatel nemůže tvrdit, že zprávu neposlal.

1. Symetrické šifrování

V tomto schématu používají obě strany (odesílatel i příjemce) **stejný klíč** pro šifrování i dešifrování.

- **Výhody:** Velmi rychlé, nízká zátěž na procesor.
- **Nevýhody:** Problém s bezpečnou distribucí klíče (pokud klíč někdo zachytí cestou k příjemci, může vše dešifrovat).
- **Příklady: AES** (Advanced Encryption Standard), ChaCha20, dříve DES.

[Image of symmetric vs asymmetric encryption diagram]

2. Asymetrické šifrování (Public Key Cryptography)

Používá dvojici matematicky propojených klíčů: **Veřejný klíč** (může ho mít kdokoliv) a **Soukromý klíč** (musí zůstat v tajnosti).

- Co je zašifrováno veřejným klíčem, lze dešifrovat pouze soukromým klíčem.
- Co je podepsáno soukromým klíčem, lze ověřit veřejným klíčem (digitální podpis).

- **Výhody:** Není třeba bezpečně sdílet tajný klíč; ideální pro komunikaci přes internet.
- **Nevýhody:** Výpočetně mnohem náročnější (pomalejší) než symetrické šifrování.
- **Příklady: RSA**, **ECC** (Elliptic Curve Cryptography), Diffie-Hellman.

3. Hybridní šifrování

V praxi (např. v protokolech HTTPS/TLS nebo IPsec) se používá kombinace obou metod:

```
1. Pomocí **asymetrického** šifrování si strany bezpečně předají náhodně
vygenerovaný "relační klíč" (session key).
2. Následný přenos dat probíhá pomocí **symetrického** šifrování s tímto
klíčem (kvůli rychlosti).
```

Hashování (Jednosměrné funkce)

Hashování není šifrování v pravém slova smyslu (nelze jej dešifrovat zpět), ale je nezbytnou součástí kryptografie. Převede libovolná data na pevně dlouhý řetězec znaků (otisk). * Použití: Ukládání hesel v databázích, kontrola integrity souborů. * Příklady: **SHA-256**, SHA-3, (zastaralé: MD5, SHA-1).

Moderní standardy

Algoritmus	Typ	Bezpečnostní status
AES-256	Symetrický	Standard pro vládní a bankovní sektor.
RSA-4096	Asymetrický	Bezpečný, ale vyžaduje dlouhé klíče.
Curve25519	ECC (Asym.)	Velmi rychlá a bezpečná eliptická křivka.
ChaCha20	Symetrický	Často používaný v mobilních zařízeních a VPN (WireGuard).

> **Zlaté pravidlo kryptografie:** Nikdy si nevytvářejte vlastní šifrovací algoritmus. Používejte pouze veřejně otestované a prověřené standardy, které odolaly pokusům o prolomení po mnoho let.

— **Viz také:** IPsec, IKEv2, VPN, TLS/SSL