

Symetrické šifrování

Symetrické šifrování (též **symetrická kryptografie**) je kryptografická metoda, při které se pro **šifrování** i **dešifrování** dat používá **stejný tajný klíč**. Tento přístup je jedním ze dvou základních typů šifrování (druhým je **asymetrické šifrování**) a je známý svou **vysokou rychlostí** a **nízkou výpočetní náročností**, což jej činí vhodným pro šifrování velkých objemů dat.

Princip fungování

V symetrickém šifrování komunikující strany (např. Alice a Bob) sdílejí **společný tajný klíč K**. Tento klíč musí být znám pouze těmto stranám a musí být předáván **bezpečným kanálem** – jinak může být celý systém kompromitován.

Proces probíhá takto:

1. **Šifrování:** Odesílatel vezme otevřený text (**plaintext**) **P** a pomocí algoritmu **E** a klíče **K** vytvoří šifrovaný text (**ciphertext**) **C**:
 - $C = E(K, P)$ - Dešifrování: Příjemce vezme ciphertext **C**, aplikuje dešifrovací algoritmus **D** se stejným klíčem **K** a získá původní zprávu: $P = D(K, C)$ Klíčovým požadavkem je, aby bez znalosti klíče **K** bylo výpočetně nemožné z ciphertextu zrekonstruovat původní zprávu. ===== **Výhody a nevýhody** ===== ^ **Výhody** ^ **Nevýhody** ^ | Vysoká rychlost - vhodné pro šifrování velkých datových proudů (např. souborů, komunikace v reálném čase). | Problém s distribucí klíčů - obě strany musí mít stejný klíč, což vyžaduje bezpečný způsob jeho výměny. | | Nízká výpočetní náročnost - dobře škáluje i na zařízeních s omezenými zdroji (IoT, mobilní zařízení). | Škálovatelnost - v síti s n uživateli je potřeba $n(n-1)/2$ klíčů pro vzájemnou komunikaci, což rychle roste. | | Dobře ověřené algoritmy - mnoho standardizovaných a dlouhodobě testovaných šifer. | Žádná vestavěná autentizace - symetrické šifry samy o sobě neověřují totožnost odesílatele (vyžadují doplnění, např. MAC nebo digitální podpis). | ===== **Typy symetrických šifer** ===== **Blokové šifry (Block ciphers)** ===== Blokované šifry zpracovávají data po pevně stanovených blocích (např. 64 nebo 128 bitů). Pokud vstupní data nejsou násobkem velikosti bloku, použije se doplnění (padding). **Známé blokové šifry:** * DES (Data Encryption Standard) - 64bitové bloky, 56bitový klíč; dnes považován za nebezpečný. * 3DES (Triple DES) - třikrát aplikovaný DES s různými klíči; pomalejší, ale bezpečnější než DES. * AES (Advanced Encryption Standard) - moderní standard; bloky 128 bitů, klíče 128/192/256 bitů; široce používaný v praxi (TLS, diskové šifrování, Wi-Fi, atd.). * Blowfish, Twofish - alternativní šifry, méně běžné, ale bezpečné. Aby blokové šifry mohly šifrovat data delší než jeden blok, používají se tzv. režimy provozu: * ECB (Electronic Codebook) - každý blok se šifruje nezávisle; nevhodný pro opakující se data (odhaluje vzory). * CBC (Cipher Block Chaining) - každý blok se před šifrováním XORuje s předchozím ciphertextem; vyžaduje inicializační vektor (IV). * CTR (Counter) - převádí blokovou šifru na streamovou; vhodná pro paralelizaci. * GCM (Galois/Counter Mode) - poskytuje šifrování i ověření integrity (AEAD - Authenticated Encryption with Associated Data). ===== **Streamové šifry (Stream ciphers)** ===== Streamové šifry generují pseudonáhodný klíčový proud (keystream), který se bit po bitu (nebo bajt po bajtu) kombinuje s otevřeným

textem - obvykle pomocí operace XOR. Výhody: * Nevyžadují padding. * Ideální pro reálný čas a proudová data (např. audio/video streamy). **Příklady:** * RC4 - dříve široce používaná (např. v SSL/TLS), ale dnes považována za nebezpečnou kvůli slabostem. * ChaCha20 - moderní, rychlá a bezpečná streamová šifra; často používána spolu s Poly1305 pro autentizaci (ChaCha20-Poly1305). * Salsa20 - předchůdce ChaCha20. ===== **Použití v praxi =====** Symetrické šifrování je základem většiny moderních bezpečnostních protokolů: * TLS/SSL: Po výměně klíčů pomocí asymetrické kryptografie (např. RSA nebo ECDH) se komunikace přenáší pomocí symetrické šifry (AES-GCM, ChaCha20-Poly1305). * Diskové šifrování: BitLocker (Windows), FileVault (macOS), LUKS (Linux) - všechny využívají AES. * Wi-Fi zabezpečení: WPA2 a WPA3 používají AES v režimu CCMP nebo GCMP. * Šifrované zálohy, e-mailové klienty, messengerové aplikace (např. Signal) - vnitřně využívají symetrické šifry pro efektivitu. ===== **Bezpečnostní doporučení =====** * Nikdy nepoužívej ECB režim pro citlivá data - odhaluje strukturu zprávy. * Používej náhodný inicializační vektor (IV) pro režimy jako CBC nebo CTR - nikdy stejný IV s tím samým klíčem! * Pro nové projekty upřednostňuj AES-128 nebo AES-256 v bezpečném režimu (GCM, CTR). * Alternativně zvaž ChaCha20-Poly1305, zejména na platformách bez hardwarové podpory AES. * Nikdy neimplementuj vlastní šifrovací algoritmus - používej ověřené knihovny jako OpenSSL, libsodium, Bouncy Castle**.

Související pojmy

- [EEPROM](#)
- [Asymmetric Encryption \(Asymetrické šifrování\)](#)
- [AES \(Advanced Encryption Standard\)](#)
- [Šifrování](#)
- [Hašovací funkce](#)
- [MAC \(Message Authentication Code\)](#)

Viz také

- [Blokové šifry](#)
- [Streamové šifry](#)
- [Režimy provozu blokových šifer](#)
- [SSH \(Secure Shell\)](#)

From:
<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:
https://www.serviceit.cz/doku.php?id=symetricke_sifrovani&rev=1767214732

Last update: 2025/12/31 21:58

