Co je asymetrická kryptografie

Poslední aktualizace 2 června, 2026

Asymetrická kryptografie (asymetrické šifrování) je způsob zabezpečení dat, který používá **dva klíče –** veřejný a soukromý.

Tyto klíče spolu tvoří pár – data zašifrovaná jedním klíčem lze dešifrovat pouze tím druhým. Díky tomu není potřeba sdílet tajný klíč předem, jako u klasického (symetrického) šifrování.

Jak funguje dvojice klíčů

Každý účastník má vlastní pár klíčů:

- **veřejný klíč –** může ho znát kdokoliv
- **soukromý klíč –** musí zůstat tajný

  Princip fungování si lze představit na jednoduchém příkladu – pokud chcete někomu poslat šifrovanou zprávu, použijete jeho veřejný klíč. Zprávu pak může přečíst pouze on, protože má odpovídající soukromý klíč.

Jak asymetrické šifrování funguje v praxi

Asymetrická kryptografie se běžně používá při zabezpečení komunikace na internetu, například u HTTPS.

Například při připojení na zabezpečený web:

- server pošle svůj veřejný klíč
- prohlížeč ho použije k zašifrování citlivých dat
- server data dešifruje svým soukromým klíčem

Tímto způsobem lze bezpečně navázat spojení i mezi stranami, které si předtím nic nesdílely.

K čemu se asymetrická kryptografie používá

Asymetrické šifrování se nepoužívá jen pro šifrování dat, ale i pro ověřování identity.

Příklady použití:

- zabezpečená komunikace (HTTPS, TLS)
- digitální podpisy
- přihlašování bez hesla (např. SSH klíče)

> *Například digitální podpis funguje opačně – data se podepíšou soukromým klíčem a kdokoliv si je může ověřit pomocí veřejného klíče.*

Jaký je rozdíl mezi asymetrickým a symetrickým šifrováním

Asymetrická kryptografie řeší jiný problém než symetrická – hlavně bezpečné předání klíče.

- **asymetrické šifrování** → dva klíče, není potřeba sdílet tajemství předem
- **symetrické šifrování** → jeden sdílený klíč, rychlejší přenos dat

V praxi se často kombinují – asymetrická kryptografie se použije na navázání spojení a symetrická na následný přenos dat.

> *Asymetrická kryptografie je výpočetně náročnější než symetrická. Proto se používá hlavně na začátku komunikace (např. při navázání HTTPS spojení), ne pro celý přenos dat.*