Co je symetrická kryptografie

Poslední aktualizace 2 června, 2026

Symetrická kryptografie (symetrické šifrování) je způsob zabezpečení dat, při kterém se používá **jeden společný klíč** pro šifrování i dešifrování.

> *To znamená, že stejný klíč, kterým data zašifrujete, musíte použít i pro jejich přečtení. Právě to je hlavní rozdíl oproti asymetrické kryptografii, kde se používají klíče dva.*

Jak symetrické šifrování funguje v praxi

Představte si, že dvě strany chtějí komunikovat bezpečně. Nejprve si musí předat společný tajný klíč – a až poté mohou začít šifrovat data.

Například:

- odesílatel zašifruje zprávu pomocí tajného klíče
- zpráva se odešle přes síť
- příjemce ji stejným klíčem dešifruje

Pokud by útočník tento klíč získal, mohl by komunikaci přečíst i upravovat.

Kde se symetrická kryptografie používá

Symetrické šifrování se používá všude tam, kde je potřeba rychle šifrovat větší objemy dat.

Typické příklady:

- šifrování přenosu dat (např. HTTPS po navázání spojení)
- šifrování disků nebo souborů
- zabezpečení databází nebo záloh

> *Při načtení zabezpečeného webu se po úvodním navázání spojení data přenášejí právě symetricky, protože je to rychlejší než asymetrické šifrování.*