Co je kryptografie

Poslední aktualizace 1 června, 2026

Kryptografie (šifrování) je způsob, jak chránit data tak, aby k nim měl přístup pouze ten, kdo má správný klíč.

V praxi to znamená, že čitelný text (např. zpráva nebo heslo) se převede na zašifrovanou podobu, kterou bez správného klíče nelze rozluštit.

Jak šifrování funguje

Při šifrování se data převedou pomocí algoritmu a klíče do nečitelné podoby. Příjemce pak použije odpovídající klíč k jejich přečtení.

Například při odeslání zprávy:

- zpráva se zašifruje pomocí klíče
- odešle se přes síť v nečitelné podobě
- příjemce ji dešifruje pomocí klíče

Bez správného klíče není možné obsah zprávy jednoduše získat.

Kde se kryptografie používá

Kryptografie je základ většiny bezpečnostních mechanismů na internetu i v aplikacích.

Typicky se s ní setkáte při:

- přenosu dat (HTTPS, zabezpečené připojení)
- ukládání hesel
- podepisování dokumentů
- zabezpečení disků nebo záloh

Například při načtení webu s HTTPS se kryptografie používá k ochraně komunikace mezi prohlížečem a serverem.

Základní typy kryptografie

Kryptografie se dělí podle toho, jak pracuje s klíči.

- **symetrická kryptografie** → jeden sdílený klíč
- **asymetrická kryptografie** → dvojice klíčů (veřejný a soukromý)

V praxi se oba přístupy často kombinují – každý řeší jinou část zabezpečení.

> *Kryptografie zahrnuje i další techniky, například hashování nebo digitální podpisy. Šifrování je jen jednou z jejích částí.*