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.

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)