# Asymmetric Encryption (Asymetrické šifrování)

**Asymetrické šifrování** (šifrování s veřejným klíčem) je kryptografický systém, který používá dvojici souvisejících klíčů.

- **Veřejný klíč (Public Key):** Může být zveřejněn. Slouží k **zašifrování** dat.
- **Soukromý klíč (Private Key):** Musí zůstat utajen. Slouží k **dešifrování** dat.

## Hlavní výhoda

Na rozdíl od symetrického šifrování si strany nemusí předem bezpečně předat společné heslo. Stačí zaslat veřejný klíč, kterým druhá strana zprávu uzamkne, a odemknout ji může pouze majitel soukromého klíče.

## Příklady algoritmů

- **RSA** (nejpoužívanější).
- **ECC** (Eliptické křivky – modernější, kratší klíče při stejné bezpečnosti).

---

*Související pojmy: RSA, AES, Cryptography, Digital Signature.*