AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard), známý také pod původním názvem **Rijndael**, je standardizovaný algoritmus pro symetrické šifrování dat. Byl vybrán americkým institutem NIST v roce 2001 po mezinárodní soutěži jako náhrada za zastaralý standard DES (Data Encryption Standard).

Dnes je AES průmyslovým standardem používaným vládami, bankami a bezpečnostními protokoly po celém světě (např. v HTTPS, Wi-Fi WPA2/WPA3 nebo při šifrování disků).

Základní charakteristika

AES je **bloková šifra**, což znamená, že data nezpracovává po jednotlivých bitech, ale dělí je do bloků o pevné délce.

- **Velikost bloku:** Vždy 128 bitů (16 bajtů).
- **Délka klíče:** Podporuje tři standardní délky klíče:
  - **AES-128:** 10 cyklů (rund) zpracování.
  - **AES-192:** 12 cyklů zpracování.
  - **AES-256:** 14 cyklů zpracování (nejbezpečnější, odolný i proti teoretickým útokům kvantových počítačů).
- **Symetrie:** Stejný klíč se používá pro šifrování i dešifrování.

Jak AES funguje (Technický princip)

Algoritmus pracuje s daty v podobě dvourozměrné matice bajtů (tzv. **State**). V každém cyklu (rundě) provádí čtyři základní transformace:

1. SubBytes (Substituce)

Každý bajt v matici je nahrazen jiným bajtem podle pevně dané převodní tabulky (S-box). Tato fáze zajišťuje nelinearitu šifry a odolnost proti lineární kryptoanalýze.

2. ShiftRows (Posun řádků)

Řádky matice jsou cyklicky posunuty o určitý počet pozic (druhý řádek o jedna, třetí o dvě atd.). Tím se data „rozptýlí“ napříč blokem.

3. MixColumns (Míchání sloupců)

Lineární transformace, která kombinuje bajty v každém sloupci. Tato operace zajišťuje, že změna jednoho bajtu na vstupu se projeví v mnoha bajtech na výstupu (efekt laviny).

4. AddRoundKey (Přičtení klíče cyklu)

V této fázi je k matici dat pomocí operace **XOR** přičten podklíč odvozený z hlavního šifrovacího klíče.

Bezpečnost a výkon

AES je považován za extrémně bezpečný. Dosud nebyl nalezen žádný praktický útok, který by byl efektivnější než útok hrubou silou (brute-force).

Hardwarová akcelerace (AES-NI)

Většina moderních procesorů (Intel, AMD, ARM) obsahuje instrukční sadu **AES-NI**. To umožňuje provádět šifrování přímo na úrovni hardwaru, což je mnohonásobně rychlejší než softwarové výpočty a zároveň bezpečnější proti útokům postranními kanály.

Módy provozu (Chaining Modes)

Protože AES šifruje bloky samostatně, musí se používat tzv. módy provozu, aby stejné bloky dat nevypadaly po zašifrování stejně:

- **CBC (Cipher Block Chaining):** Každý blok závisí na předchozím.
- **GCM (Galois/Counter Mode):** Moderní, velmi rychlý a bezpečný mód, který zajišťuje i integritu dat (ověření, že data nebyla změněna).

Praktické využití

- **Komunikace:** TLS/SSL (HTTPS), VPN (IPsec, OpenVPN).
- **Úložiště:** BitLocker (Windows), FileVault (macOS), VeraCrypt.
- **Archivy:** Šifrování souborů .zip nebo .7z.
- **Bezdrátové sítě:** Zabezpečení Wi-Fi sítí pomocí WPA2-AES.

Související pojmy: Symetrické šifrování, DES, Kryptoanalýza, Klíč, HTTPS.