ACMEv2 Certificate Automation Project

Built a complete **ACMEv2** client system to automate **X.509 certificate issuance, domain validation**, and **revocation** according to RFC 8555, fully simulating the lifecycle between client and CA.

Key Components:

- **ACME Client:**
    - Implements full ACMEv2 flow (*newAccount, newOrder, finalize, certificate, revokeCert*) with strict nonce management and *badNonce* retry logic.
    - Supports *dns-01* and *http-01* challenges with fresh cryptographic material per session.
- **Cryptography Layer:**
    - Developed a *CryptoManager* module handling:
        - JWK generation (RSA and EC keys: RS256, ES256, ES384, ES512).
        - JOSE-compliant request signing and payload encoding.
        - CSR creation with proper SAN extensions.
    - Fully managed certificate parsing and HTTPS chain setup.
- **Server Infrastructure:**
    - **Custom DNS server** (*dnslib*-based) dynamically answering A and TXT queries for ACME validation.
    - **HTTP Challenge server** for http-01 responses (*FastAPI* +).
    - **HTTPS Certificate server** serving the obtained certificates with correct SSL context.
    - **Shutdown server** to gracefully terminate all components post-validation.
- **Protocol Engineering:**
    - Ensured strict sequencing and timing between ACME protocol steps.
    - Managed nonce handling, replay protections, and Pebble compliance for CI integration.
    - Handled concurrent operations and clean shutdown across multiple async servers.

Skills Trained:

- **Public Key Infrastructure (PKI)** and **certificate lifecycle management**
- **TLS/SSL deployment and chain validation**
- **Asynchronous programming** (asyncio, aiohttp)
- **Cryptographic primitives** (ECDSA, RSA, JWK, CSR)
- **Networking protocols** (HTTP, HTTPS, DNS)
- **Concurrent systems engineering** and **resilient server orchestration**