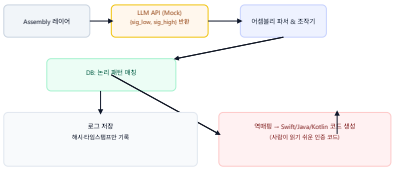
A

LLM ↔ Assembly 기반 1회성 시그니처 인증 — 다이어그램 & 데모

흐름: Assembly → LLM API → 시그니처 추출 → 저수준 조작 → DB 논리 패턴 검사 → Swift/Java/Kotlin 역매핑 인증

흐름 다이어그램



알고리즘 단계

1. 어셈블리 레벨에서 소켓을 열고 LLM API로 POST 요청 전송
2. JSON 응답을 수신 후 필요한 키(sig_low, sig_high)만 파싱
3. 어셈블리(자동화·딥러닝·머신러닝)으로 sig_low 조작
4. 조작된 토큰을 DB로 전달하여 논리 패턴 매칭 수행
5. 매칭 성공 시 sig_high를 이용해 사람 친화적 고수준 코드(Swift/Java/Kotlin) 생성

보안 환경 가정

- sig_low는 매 요청마다 달라지는 1회성 값
- 어셈블리는 하드웨어 엔트로피(cpuid, timestamp) 사용
- DB는 원본 시그니처가 아닌 패턴 해시만 저장