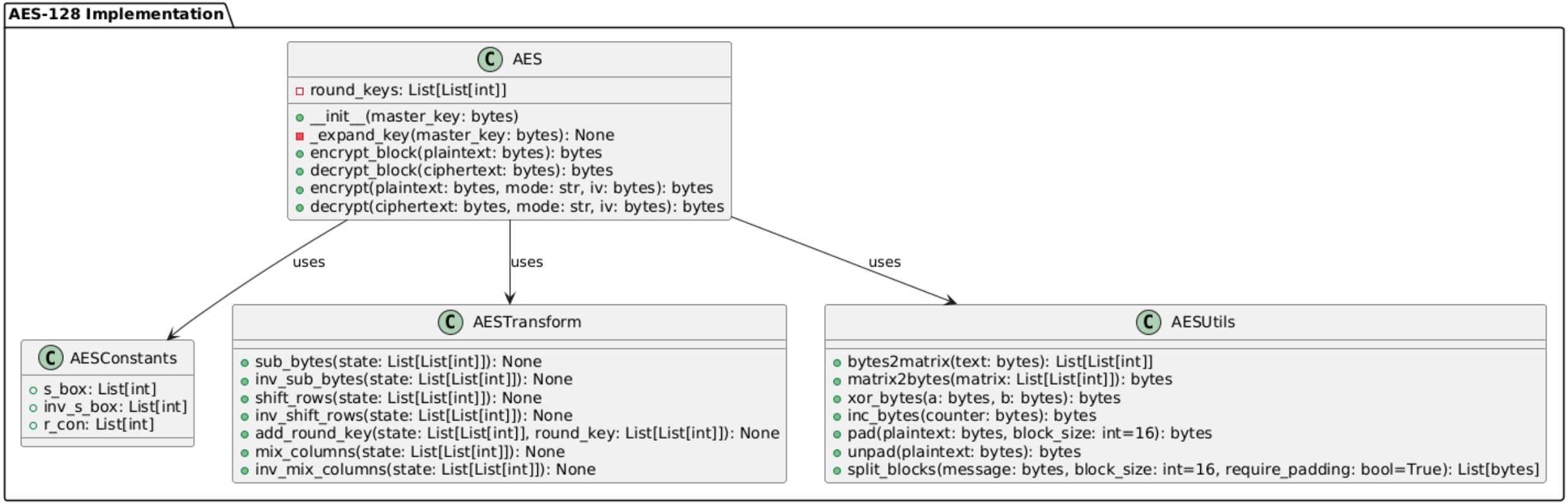
DGIST 여름인턴 1주차 주간 보고서

3조 권태완, 조후연, 박준석

1주차: 7/7 –
7/11

- AES 알고리즘 이해 및 분석 진행
- LiberateFHE에 존재하는 연산 구분

기존 AES 구현 in python (예시)



2주차: 7/14 – 7/18 계획

- 각 모듈은 우선적으로 python numpy를 통해 구현
- Liberate에서의 구현이 메인이므로 이를 고려하여 알고리즘 위주로 진행
- XOR 처럼 직접 구현해야하는 경우, Liberate로 바로 구현 (LUT!!)

Question

Q1: Mode 고정? (ECB, CTR, CBC, etc…)

끝