decode 활동내역

* Feistel cipher 등 block cipher 알고리즘, 대칭키 암호화 공부
* Feistel cipher에 기반한 block cipher 알고리즘 구현, 어떻게 암호문이 조작되었는지 확인할 수 있고, 어떻게 평문을 조작하면 동일한 암호화 결과를 낼 수 있는지 연구.
* Blockchain, merkle tree, SHA-256 등 hash functions 공부
* 특정 block의 정보가 오염되었는지 빠르게 판단할 수 있는 알고리즘 연구 및 구현
* AES, DES 암호화 알고리즘 공부
* Arduino Uno에서 구현된 경량 암호화 알고리즘 속도 개선 연구
* Hierarchical deterministic wallet 원리 (BIP-0039, BIP-0032) 공부
* Wordlist와 master public key가 주어졌을 때 그에 상응하는 master private key 알아내는 알고리즘 구현
* 2022년 암호분석경진대회 우수상 수상
* 2022년 2학기에는 정보보안 수업을 기반으로 매주 스터디를 진행하고 있음.

Decode 연혁

* 2022년 4월 결성
* 2022년 7월 14일 부산대학교 정보의생명공학대학 정보컴퓨터공학부 소속 동아리 등록
* 2022년 9월 20일 2022년 암호분석경진대회 우수상 수상

동아리가 궁금한 사람들에게 한마디 (의견 낸 순서대로 적었음)

* 정윤서: 수학 동아리 같아요….
* 이홍석: 다 같이 공부하고 코딩도 하는 동아리니까 일단 들어만 오세요!!!! 저희 결코 무섭지 않습니다 😊
* 문정윤: 김호원 교수님의 열정으로 개설된 암호 집중 동아리