호기심의 시작, 국민암호페스티벌

우리가 사용하는 암호는 과연 안전할까?

전공 수업: 이론적 완벽함

수학적으로 안전하다고 배운 AES, RSA 암호 알고리즘

전환점: 국민암호페스티벌

PEPSI 부스에서 본 ChipWhisperer 시연

충격: 파형 분석으로 비밀키 노출

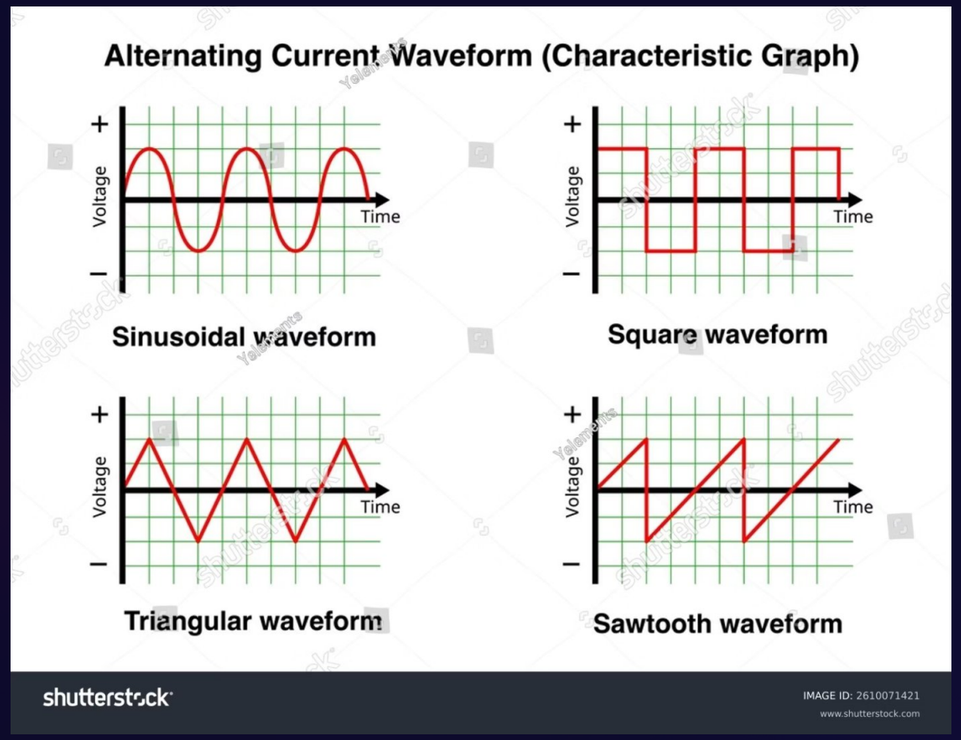
이론과 현실의 괴리, 하드웨어 취약점 목격

이론을 넘어 실제 하드웨어 취약점을 직접 분석하고 검증하며, 정보보안 분야에 대한 깊은 호기심과 열정을 키우게 되었습니다.

준비된 기초 역량: Coding & Analysis

암호 구현 경험

Python(SageMath)으로 **RSA 알고리즘** 직접 구현 및 연산 시간 차이 분석. 부채널 정보의 개념을 체득했습니다.



분석 실습 기초

C언어로 펌웨어 및 하드웨어 메모리 구조 이해. **Python**으로 대용량 파형 데이터 전처리 및 분석 자동화 스크립트 작성을 연습했습니다.

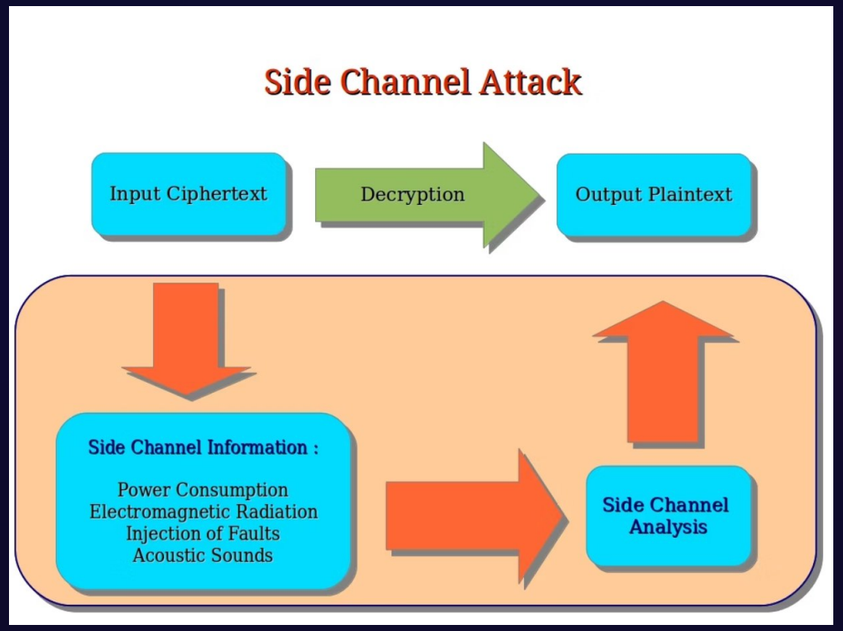
이러한 경험은 PEPSI 동아리 활동에 큰 도움이 될 것이라고 확신합니다. 이론을 코드로 구현하고 실제 데이터를 분석하는 능력은 정보보안 연구에 필수적입니다.

커리큘럼에 맞춘 단계별 성장 계획

상반기: Attack & Analysis

AES 암호 알고리즘 구현 및 소비 전력 측정

CPA(상관전력분석) 실습을 통한 비밀키 추출 성공



하반기: Defense & Research

부채널 공격 대응 기법 학습: 하이딩 & 마스킹

심화 연구: 딥러닝 기반 분석 또는 PQC 스터디 참여

PEPSI의 체계적인 커리큘럼을 따라 공격과 방어 기술을 익히고, 나아가 새로운 연구 분야에 도전하며 정보보안 전문가로 성장하고 싶습니다.