2020 암호분석경진대회

4번 문제 : 부채널 분석

암호대학교 A교수는 암호알고리즘 강의 시험문제를 한글파일(.hwp파일)로 작성한 후, AES128/CBC/PKCS#7으로 데이터 암호화를 수행하는 전용 암호장비를 통해 이 파일을 암호화 (IV[16] = {0x00, }) 하였다. 하지만, 암호화된 파일 (exam.hwp.encrypted)과 파일을 암호화하는 과정에서의 전력소비 파형 (PowerConsumption.csv)이 공격자에게 누출되었고, 공격자가 취득한 전력파형에는 CBC 운영모드로 파일 암호화가 이루어지는 동안의 AES 단위블록 연산에 대한 전력 소비량 1025개 ('exam.hwp.encrypted' 파일 크기 : 1025*16 Bytes)가 순차적으로 포함되어 있었다. 또한, 각 AES 단위블록에 대한 전력파형에는 AES128 10라운드 중 7, 8라운드(SubBytes → ShiftRows → MixColumns → KeyAddition → SubBytes → ShiftRows → MixColumns → KeyAddition)의 연산에 해당하는 전력소비량만이 측정되어 있었고, 해당 파형은 각각 20,000포인트로 구성되어 있었다.

AES128 마지막라운드의 라운드키 16바이트 중 7바이트가 다음과 같이 공격자에게 누출되었을 때, AES 마스터키 추출을 통해 원본 시험문제를 복호화하는 과정을 제시하고, 해당 파일에 작성되어 있는 문제의 정답을 찾으시오.

22	E5	*	*	E9	*	*	4C	*	*	5B	2C	*	9B	*	*

▣ 참고 사항

1) 한글파일은 Compound File Binary Format이므로 최초 8 bytes는 'D0 CF 11 E0 A1 B1 1A E1'이다.
2) 암호화 연산 도중 발생한 소비 전력을 이용하여 암호키를 찾는 부채널 분석 기법을 전력 분석이라 하며, 전력 분석 중에 일반적으로 활용되는 분석 기법이 상관 전력 분석 (CPA, Correlation Power Analysis)이다.
   - 참고문헌: "Correlation Power Analysis with a Leakage Model",
     https://www.iacr.org/archive/ches2004/31560016/31560016.pdf
3) http://opensca.sourceforge.net/ 에서 상관 전력 분석을 시행 할 수 있는 matlab 기반의 오픈 소스 및 부채널 분석 관련 내용을 확인 할 수 있다.
4) 전력파형 'PowerConsumption.csv'에서 행의 개수 20,000은 한 파형의 길이를 의미하고, 열의 개수 1,025는 파형의 개수를 의미한다. 첫 번째 열이 첫 번째 AES 단위블록 연산 시 측정된 전력파형이다.
5) https://github.com/esxgx/easy-ecc 에서 ECDSA 오픈 소스를 활용 가능하다.
6) 평가 참고사항 :
   - 본 문제는 ①파일 복호화 단계와 ②복호화된 파일 내의 시험문제인 공개키 암호(전자서명) 해독 단계의 두 단계로 구성되며 각각의 배점은 ①단계(75점), ②단계(25점)이다.
   - 본 문제의 ①단계 해결 시, 상관전력분석과 대칭키 암호키 전수조사를 함께 수행해야 할 수 있다. 암호키를 찾은 동점자 발생 시, [(전력분석에 사용한 키 전수조사 범위) * 1,025 * 20,000 + (대칭키 암호키 전수조사 범위)]의 수치가 작은 제출자에게 가점을 부여할 예정이다. (상관전력분석과 대칭키 암호키 전수조사 중 사용하지 않는 방법이 있다면 그 방법은 전수조사 범위를 1로 계산)