2022 국민대학교 정보보안암호수학과 학술동아리 주관 경진대회

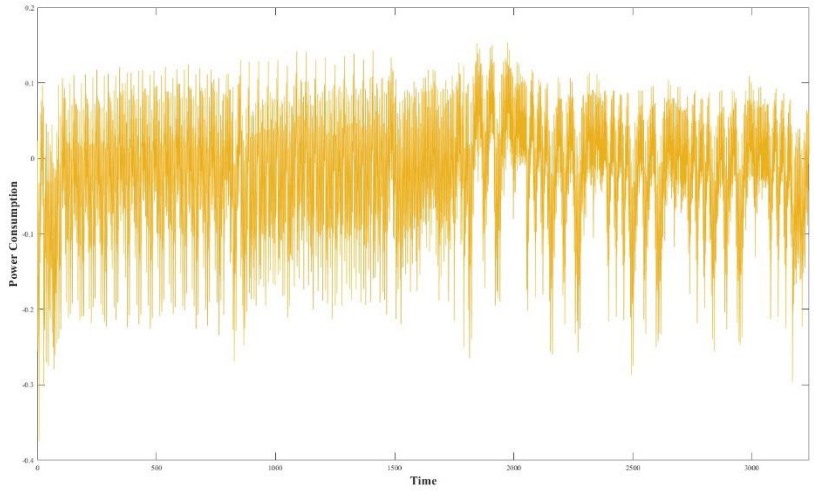
3번 문제 - 부채널 분석 (출제: 동아리 PEPSI)

부채널 분석(Side Channel Analysis)이란, 디바이스에서 암호화 알고리즘이 동작할 때 발생하는 소리, 소비전력, 전자파와 같은 부채널 정보를 활용하여 비밀정보(비밀키)를 알아내는 분석법이다. 1999년 P.Kocher 등에 의해 제안된 Differential Power Analysis(DPA)를 시작으로, 소비전력 파형과 비밀정보 사이의 상관관계를 이용한 Correlation Power Analysis(CPA) 등 다양한 부채널 분석 기법이 연구되었다.

[문제 1(20점)]

다음 그림은 AES-128 한 라운드 동작 시 발생하는 소비전력 파형이다. 주어진 파형에 Simple Power Analysis(SPA)를 적용하여 각 함수 (AddRoundKey, SubBytes, ShiftRows, MixColumns)의 연산 위치를 표시하고, 그 이유를 논리적으로 서술하라.

Hint: 문제에서 사용된 AES-128은 8-bit단위로 연산이 진행되며, SubBytes 연산의 경우 S-Box 룩업 테이블(Lookup Table)을 사용하여 구현되었다.

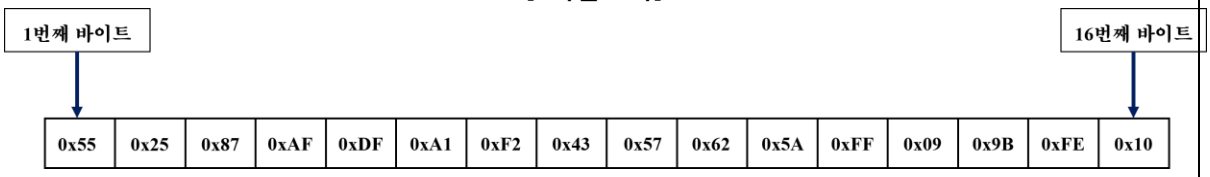


[문제 2(40점)]

1) AES-128 마스터 키 복구 (20점)

AES는 한 라운드키의 모든 바이트를 알면 마스터키를 복구할 수 있는 특징을 가진다. AES-128의 7번째 라운드키가 다음과 같이 주어졌을 때 AES-128 마스터키를 복구하는 코드를 구현하고, 마스터키 16바이트와 마스터키로 생성할 수 있는 AES-128 마지막 라운드키 16바이트를 각각 구하라.

[7라운드키]



답안에는 7라운드키를 사용한 마스터키 복구 논리, 복구할 때 사용된 코드를 제출해야 한다.

마스터키 16바이트:
마지막 라운드 키 16바이트:

2) 암호문 복구 (40점)

PEPSI_CT.bin은 1124바이트 평문을 0x80 패딩 후에 AES-CBC를 활용하여 암호화한 1136바이트 암호문을 저장한 바이너리 파일이다. **1)**에서 복구한 마스터키 16바이트를 ASCII 값으로 바꾼 값을 이용하여 빈칸을 채워 제출하라. PEPSI_CT.bin의 내용을 AES-CBC로 복호화하고 ASCII로 변환하면 얻는 1124바이트는 어떤 문서의 원본 내용 중 일부이다. 이 문서의 제목을 찾아 답안으로 제출하라. (AES-CBC 모드의 키는 **1)**의 마스터키를 사용했으며 초기 벡터(IV) 값은 해당 마스터키로 생성한 라운드 키들 중에서 마지막 라운드키 값이다.)

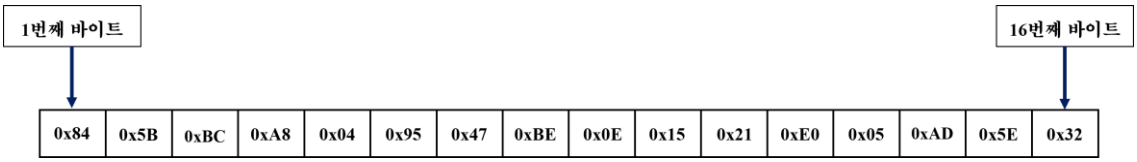
마스터키 16바이트의 아스키 변환 값 일부(전체를 완성해서 제출하라):

[redacted]I[redacted]EC[redacted][redacted]N[redacted][redacted]LP[redacted]P[redacted]I

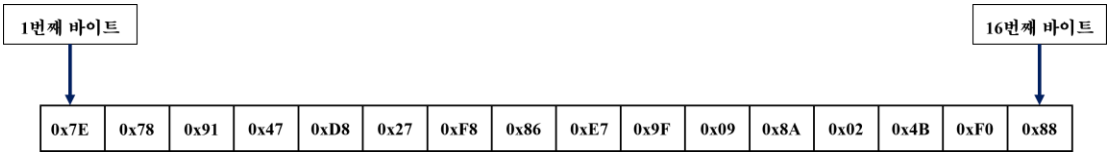
PEPSI_CT.bin에 담긴 문서의 제목은?

[문제 3(20점)]

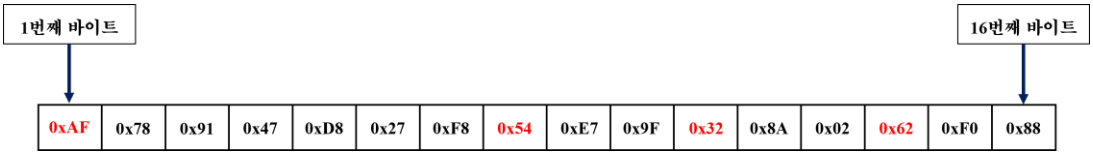
세훈이는 건희의 암호화 장비를 탈취하는데 성공했다. 탈취한 암호화 장비에서 AES를 돌린 결과 [그림 1]과 같은 평문에 대한 정상적인 암호문 값[그림 2]을 얻을 수 있었다. 그 후, 세훈이는 AES가 동작할 때 특정한 라운드 내의 특정 함수의 입력 값에 지속적으로 1바이트 전자파 오류를 주입하였는데, [그림 3]과 같이 정상적인 암호문과 비교했을 때 특정 위치의 바이트 값이 변경된 오류 암호문을 얻을 수 있었다. [그림 4]는 AES의 라운드 연산 중 일부를 그림으로 나타낸 것이다.



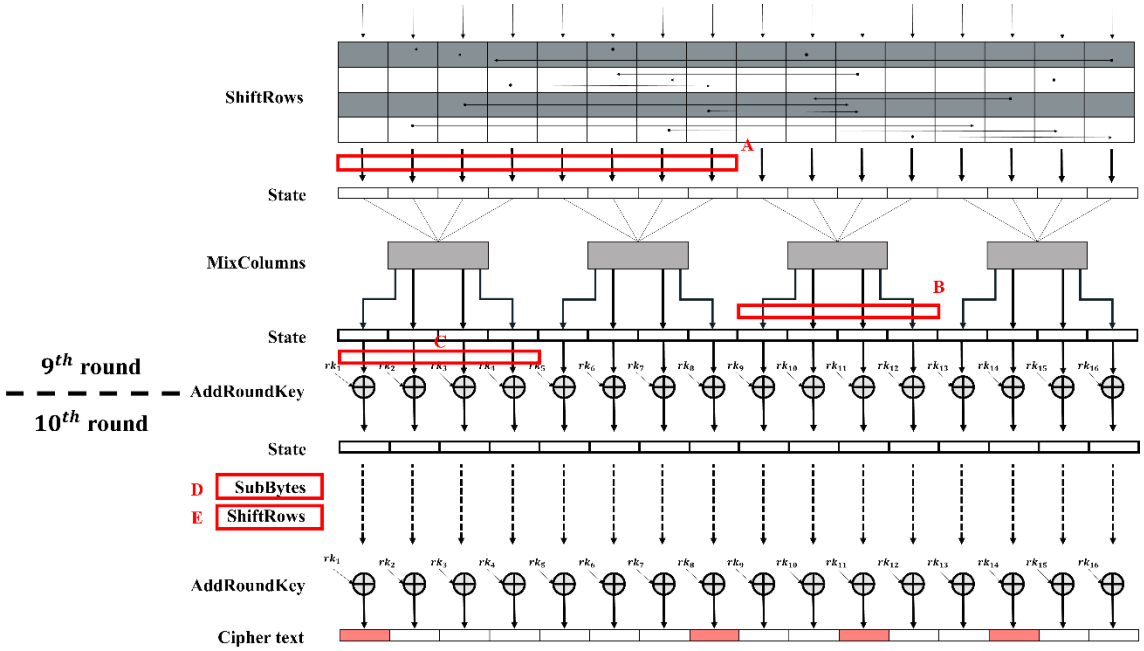
[그림 1] 평문



[그림 2] 정상 암호문



[그림 3] 오류 암호문



[그림 4] AES 라운드 연산 중 일부

[그림 4]의 표시한 영역 중에서 입력 1바이트 오류로 인하여 [그림 2]와 같은 현상이 발생할 수 있을 것이라고 기대되는 위치(A, B, C, D, E)와 이유를 논리적으로 서술하라.

● 참고 사항

1) AES-128 표준문서: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
2) SPA(Simple Power Analysis): Stefan Mangard, Power Analysis Attacks – Revealing the Secrets of Smart Cards. Chapter 5.2 Visual Inspections of Power Traces
3) Martinasek, Zdenek, and Vaclav Zeman. "Innovative method of the power analysis." Radioengineering 22.2 (2013): 586-594

문의: KMU.PEPSI @gmail.com