**HW2번 보고서-20192233박진철**

**1. 파일 암호화 프로그램: 10주차 파일 입출력 소스코드를 활용하여 다음 프로그램을 작성하라.**

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

-복호화를 할 때, 패딩된 부분을 제거하기 위한 함수

-0x80이 패딩의 시작이라는 점을 이용하여 0x80 0x00 이후의 부분을 제거함

**(a) ECB모드로 파일을 암호화, 복호화하는 프로그램**

텍스트이(가) 표시된 사진

자동 생성된 설명

-ECB모드로 AES 암호화

텍스트이(가) 표시된 사진

자동 생성된 설명

-ECB모드로 AES 복호화

**(b) CBC모드로 파일을 암호화, 복호화하는 프로그램**

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

-CBC모드로 AES 암호화

**텍스트이(가) 표시된 사진

자동 생성된 설명**

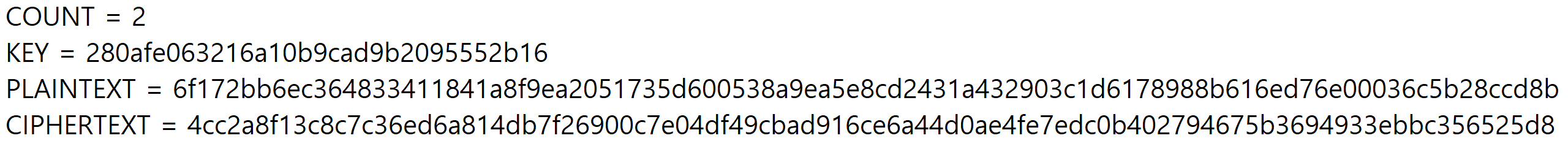
**텍스트이(가) 표시된 사진

자동 생성된 설명**

-CBC모드로 AES 복호화

**(c) “AESAVS”의 테스트 벡터를 찾아 만족함을 보여라.**

-ECB모드 MMT 테스트 벡터 예시



-ecb\_test\_plain.txt의 바이너리 코드

텍스트이(가) 표시된 사진

자동 생성된 설명

-ECB구현을 위한 main 함수

텍스트이(가) 표시된 사진

자동 생성된 설명

=main 함수 실행

-패딩된 파일을 집어넣은 AES\_ECB\_Padded.bin의 바이너리 코드

텍스트이(가) 표시된 사진

자동 생성된 설명

-암호화한 파일인 ecb\_test\_cipher.txt의 바이너리 코드

텍스트이(가) 표시된 사진

자동 생성된 설명

=패딩된 마지막 블록을 제외하면, 테스트 벡터와 동일함

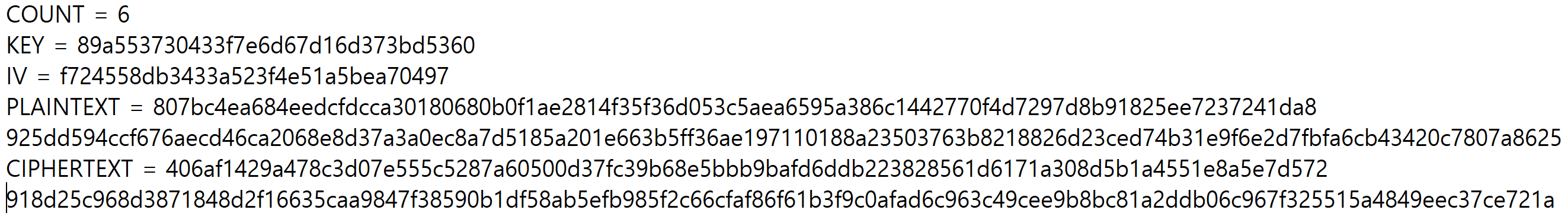
-파일을 복호화한 ecb\_test\_decipher.txt의 바이너리 코드

텍스트이(가) 표시된 사진

자동 생성된 설명

=패딩된 부분도 잘 지워져 원래 평문파일과 동일해짐

-CBC모드 MMT 테스트 벡터 예시



-cbc\_test\_plain.txt의 바이너리 코드

테이블이(가) 표시된 사진

자동 생성된 설명

-CBC구현을 위한 main 함수

텍스트이(가) 표시된 사진

자동 생성된 설명

=main 함수 실행

-패딩된 파일을 집어넣은 AES\_CBC\_Padded.bin의 바이너리 코드

테이블이(가) 표시된 사진

자동 생성된 설명

-암호화한 파일인 cbc\_test\_cipher.txt의 바이너리 코드

테이블이(가) 표시된 사진

자동 생성된 설명

=패딩된 마지막 블록을 제외하면, 테스트 벡터와 동일함

-파일을 복호화한 cbc\_test\_decipher.txt의 바이너리 코드

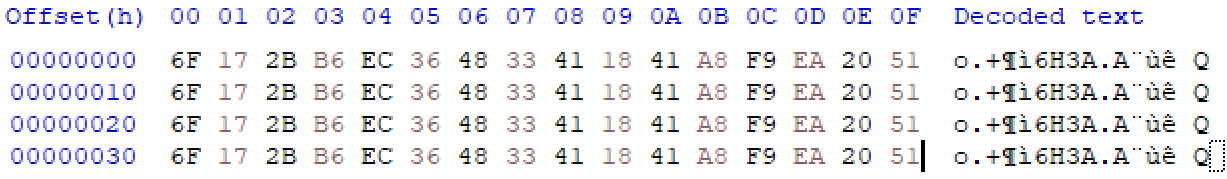
텍스트, 전자기기, 키보드이(가) 표시된 사진

자동 생성된 설명

=패딩된 부분도 잘 지워져 원래 평문파일과 동일해짐

**(d) 두 모드의 암호화 차이를 잘 나타낼 수 있는 샘플 파일을 만들고 암호화 결과를 설명하라.**동일한 블록이 존재할 경우, EBC모드는 같은꼴의 암호화블럭이 나오지만, CBC모드는 그렇지 않음

-다음과 같이 블록이 동일한 평문을 ECB 모드에서 수행



-ECB모드로 수행할 경우, 아래와 같이 동일한 블록들이 만들어짐

텍스트이(가) 표시된 사진

자동 생성된 설명

-그러나, CBC모드로 수행할 경우, 아래와 같이 동일한 블록이 나올 가능성은 낮음

텍스트이(가) 표시된 사진

자동 생성된 설명

**2. 운영모드(Mode of Operation): 암호화한 파일의 한바이트를 변경하고 복호화한 결과를 비교하라.**

**(a) ECB모드로 암호화한 경우**

1-(c)에서 사용한 테스트 벡터와 비교하여 진행

-28위치에 있던 49를 5F로 변경

텍스트이(가) 표시된 사진

자동 생성된 설명

-1바이트 바뀐 파일로 복호화 실행

-1-(c)의 평문파일과 복호화된 파일을 비교

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

=>한블록만 바뀌었으며, 다른블록에는 영향을 끼치지 않음

**(b) CBC모드로 암호화한 경우**

1-(c)에서 사용한 테스트 벡터와 비교하여 진행

-28위치에 있던 45를 29으로 변경

테이블이(가) 표시된 사진

자동 생성된 설명

-1바이트 바뀐 파일로 복호화 실행

-1-(c)의 평문파일과 복호화된 파일을 비교

테이블이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

=>3번째 블록과 38위치의 바이트가 바뀌었음

**(c) 한바이트의 변경이 복호화 결과에 미치는 영향은 어떠한가 분석하라.**

암호문에서 한바이트가 변경되었을 경우, EBC모드는 한바이트의 변경이 다른 블록에 영향을 주지 않지만, CBC모드는 한바이트의 변경이 두 블록에 영향을 미친다.