보안SW구현 - 과제 2

제출 마감: 2022년 11월 18일

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

   (a) ECB모드로 파일을 암호화, 복호화하는 프로그램

   (b) CBC모드로 파일을 암호화, 복호화하는 프로그램

   (c) "AESAVS"의 테스트 벡터를 찾아 만족함을 보여라.

   (d) 두 모드의 암호화 차이를 잘 나타낼 수 있는 샘플 파일을 만들고 암호화 결과를 설명하라.

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

   (a) ECB모드로 암호호한 경우

   (b) CBC모드로 암호호한 경우

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

□ 실행 화면과 결과에 대한 보고서와 별도로 실행 가능한 소스코드를 제출해야 함.