정보보호론 0401

4월 22일 중간고사 시험 수업시간

시험 범위 : 공개키 암호까지

DES bit ?

AES bit Key bit ?

AES 분석\_안전성

복호화 할 때 패딩도 알아야 한다.

단점 : 원본 메시지가 완전할 때, 패딩 페이지를 만들어 주어야한다. (비효율적)

원본 메세지를 지우는 일은 없다.