REPORT

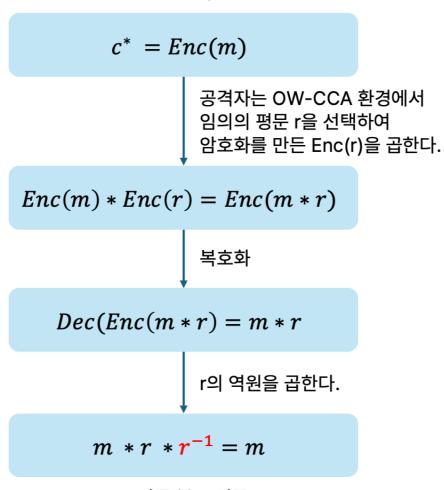
[Assignment 3 : RSA 암호 기법 분석]



과 목 명	정보보호론
교 수 명	김 효 승
학 번	20237107
작 성 자	하 태 영
제 출 일	2025.04.11

- 1. OW-CCA에 대해 설명하시오.
- ⇒ OW
 - 평문 복구 (breaking one-wayness)
- ⇒ CCA
 - 선택 암호문 공격(Chosen Ciphertext Attack)
- ⇒ OW-CCA
 - 복호화 기계를 쓸 수 있는 상황이어도, 목표 암호문 하나의 평문은 못 알아내야 한다.
- 2. 강의자료의 RSA 기법이 OW-CCA에 안전하지 않음을 보이시오.

RSA 암호화: c*, 평문: m



m 평문 복구 성공