**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 |

**한림대학교**

1. OW-CCA에 대해 설명하시오.

* OW
  + 평문 복구 (breaking **o**ne-**w**ayness)
* CCA
  + 선택 암호문 공격(**C**hosen **C**iphertext **A**ttack)
* OW-CCA
  + 복호화 기계를 쓸 수 있는 상황이어도, 목표 암호문 하나의 평문은 못 알아내야 한다.

1. 강의자료의 RSA 기법이 OW-CCA에 안전하지 않음을 보이시오.

**텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.**