|  |
| --- |
| **2021 국민대학교 정보보안암호수학과 동아리 연합 암호경진대회** |
| 2번 문제 답안 |
| 정보보안암호수학과 20192243 이용진 |
| <소스 코드는 Visual Studio Code, Window10에서 작성되었습니다>  2-1. 소스 코드 제출  2-2. 소스 코드 제출  <Table1>    <Table2>      <Ttable3>    <Ttable4>    2-3. 소스 코드 제출  2-4.    2-5.  T-table 하나는 (256 x 4)-byte의 크기를 가진다.  T-table은 총 4개 임으로 메모리는 (256 x 4 x 4)-byte = 4096-byte 가 필요하다.  T-table을 최소로 사용하는 경우는 필요할 때 마다 즉석에서 생성하는 방식을 사용하면 된다.  즉, T-table을 연산하는 함수만 만들어 두고 AES구현시 필요한 값을 즉석으로 T-table함수로 계산한다.  즉석에서 T-table 값을 생성하면, 미리 T-table을 저장할 필요가 없음으로 T-table이 차지하는 메모리 사용량은 0이다. |