**REPORT**



|  |  |
| --- | --- |
| **과목명** | 컴퓨터 보안 |
| **학과** | 컴퓨터공학과 |
| **학번** | 12161658 |
| **이름** | 조재민 |
| **제출일자** | 2020.10.15 |

Miller-Rabin Algorithm

이번 실습 과제로는 미리 구현된 Exponential 함수를 활용하여 유명한 소수 판별 법 알고리즘인 Miller-Rabin 함수를 구현하는 과제였습니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

구현된 Miller Rabin 함수입니다. 함수에 넘겨진 인자 값 n과 s는 각각 검사하여야 하는 수와 Miller Rabin 함수의 잘못된 판단 가능성 () 의 값 s 입니다.

검사하여야 하는 수가 2면 소수, 2로 나누어 떨어지면 합성수 임을 첫 두 If 문에서 확인해준 뒤, s 번 만큼 반복문을 돌며 test 함수에 n보다 작은 양의 정수 a와 함께 test 함수에 넘겨줍니다. 해당 Test 함수에서 값이 True로 리턴된다면 이는 합성수임을 알리며 종료됩니다. 통과하였다면 소수일 가능성이 큼으로 소수로 반환합니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

구현된 test 함수 입니다. 이 함수에서는 NSR Test와 Fermet Test로 구성되어 있습니다. t 라는 값을 0으로 두고 u를 넘겨온 수 n의 n – 1이라는 값을 둔 뒤, while문을 조건에 맞게 돌리며 t와 u를 올바른 값으로 설정합니다.

그다음 t번만큼 반복문을 돌며 NSR test를 위해 값을 조정합니다. X\_0에는 값을 설정 한 뒤 X\_0의 값이 1 이라면 False를 리턴합니다. 그다음 반복문을 돌며 x\_0값을 페르마의 소정리를 이용하기 위해 값을 계속해서 비교하며 해당 값이 n – 1과 일치하면 False를 리턴해줍니다. 이러한 과정을 모두 거쳐서 True로 리턴되면 해당 수는 합성수임을 반환하고, False로 리턴되면 해당 수를 Prime으로 리턴해줍니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

예제로 들어온 소수 집합 배열을 검사한 결과입니다. 정상적으로 모두 소수임을 판별해 냈습니다.