**컴퓨터 공학과**

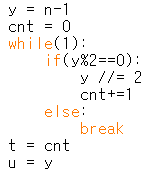
**컴퓨터 보안**

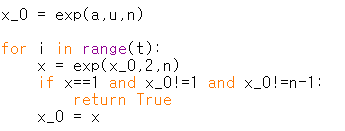
**2차 실습 과제**

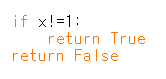
**12161558**

**김혜윤**

**20.10.05**

* Test 함수 구현 방법 및 부연 설명
*  n-1 = 2^t\*u
  + 변수 y에 n-1을 넣고 while문으로 2로 나눈 나머지가 0일 때 나눠주고 cnt를 증가시켜준다. 그리고 더 이상 2로 나눈 나머지가 0이 아닐 때, while문을 break 시킨다. Cnt의 값은 t로 y의 값은 u로 하여 n-1 = 2^t\*u 를 구해주었다.





* + X\_0 값에 미리 구현 되어 있던 exp(a,b,n) 함수를 이용하여 a^u mod n 값을 구해주고 t번 동안 x = exp(x\_0,2,n)을 하고, x==1이고 x\_0 != 1 그리고 x\_0!=n-1이 동시에 만족된다면 NSR test로 인해 prime number가 아니기 때문에 True를 return 한다. 하나라도 만족되지 않으면 다시 x를 x\_0에 넣어주고 반복한다. T번을 모두 반복한 후, x가 1이 아니라면 Fermat Test에 의해 prime number가 아니기 때문에 True를 return하고 그 외의 경우에는 prime number 이기 때문에 False를 return 하여 준다.