컴퓨터 보안

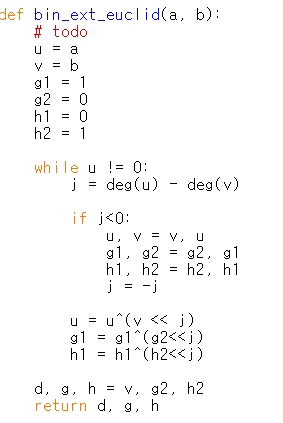
실습 3차 과제

컴퓨터공학과

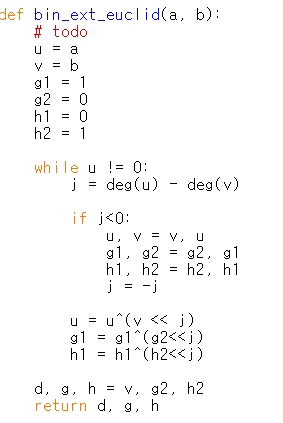
12161558

김혜윤

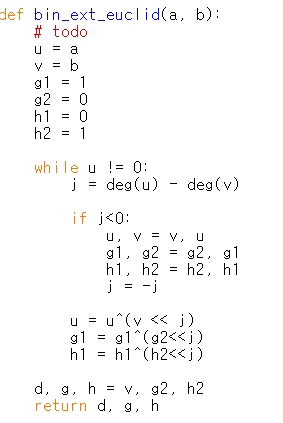
* Extended Euclid for binary polynomials



* 처음 변수 초기화를 해준다 u는 a로 v는 b, g1 =1, g2=0, h1=0,h2로 한다.

`

* u의 차수가 v의 차수보다 커야 하기 때문에, 작다면 둘을 바꿔주고 g1,g2,h1,h2 또한 서로 바꿔주고 j는 -를 붙여서 양수로 바꿔준다.



* 그 다음 u와 j만큼 (둘의 차수 차) 왼쪽으로 shift해준 v를 xor 연산 (u+v mod 2의 의미) 을 하여 준다. U가 0이 되면 반복을 멈추고 return 을 해준다.