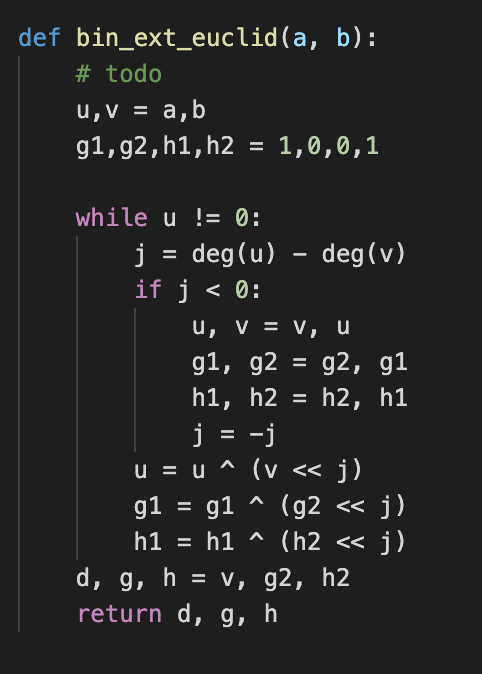
**REPORT**



|  |  |
| --- | --- |
| **과목명** | 컴퓨터보안 |
| **학과** | 컴퓨터공학과 |
| **학번** | 12161658 |
| **이름** | 조재민 |
| **제출일자** | 20.10.23 |



구현 된 bin\_ext\_euclid 함수 입니다.

d는 gcd(a, b)이고, g와 h는 ag + bh = d 를 만족하는 binary polynomials입니다.

Extended Euclid algorithm을 사용하기위해, 우선적으로 u,v, g1, g2,h1,h2를 초기화합니다. u,v 는 각각 loop invariant의 우변에 해당하는 값 입니다. 반복문을 수행하며 u가 0이 되면 종료합니다. J라는 변수에 u와 v의 최고차항의 차를 값을 넣어줍니다. J가 음수라면 측 u의 최고차 항보다 v의 최고차 항이 더 크다면 양수로 만들며 u, v, g1, g2, h1, h2 모두를 swap 합니다. V << j는 즉 j만큼 왼쪽으로 shift 하는 효과가 z^j를 곱해주는 값과 같은 연사을 해줍니다. XOR 연산을 통해 원하는 값을 얻어냅니다. 아래는 실행결과 입니다.텍스트이(가) 표시된 사진

자동 생성된 설명